www.zte.com.cn/magazine/English

ISSN 1673-5188
CODEN ZCTOAK

ZTE COMMUNICATIONS

An International ICT R&D Journal Sponsored by ZTE Corporation

September 2015, Vol. 13 No. 3

SPECIAL TOPIC:
Recent Advances in Smart Grid

ZTE中兴 ZTE COMMUNICATIONS

VOLUME 13 NUMBER 3 SEPTEMBER 2015

ZTE Communications Editorial Board

Chairman

Houlin Zhao: International Telecommunication Union (Switzerland)

Vice Chairmen

Lirong Shi: ZTE Corporation (China) **Chengzhong Xu**: Wayne State University (USA)

Members (in Alphabetical Order):

Chang Wen Chen	The State University of New York at Buffalo (USA)
Chengzhong Xu	Wayne State University (USA)
Connie Chang–Hasnain	University of California, Berkeley (USA)
Fa–Long Luo	Element CXI (USA)
Fuji Ren	The University of Tokushima (Japan)
Guifang Li	University of Central Florida (USA)
Honggang Zhang	Université Européenne de Bretagne (France)
Houlin Zhao	International Telecommunication Union (Switzerland)
Huifang Sun	Mitsubishi Electric Research Laboratories (USA)
Jianhua Ma	Hosei University (Japan)
Jiannong Cao	Hong Kong Polytechnic University (Hong Kong, China)
Jinhong Yuan	University of New South Wales (Australia)
Keli Wu	The Chinese University of Hong Kong (Hong Kong, China)
Kun Yang	University of Essex (UK)
Lirong Shi	ZTE Corporation (China)
Shigang Chen	University of Florida (USA)
Shuguang Cui	Texas A&M University (USA)
Victor C. M. Leung	The University of British Columbia (Canada)
Wanlei Zhou	Deakin University (Australia)
Weihua Zhuang	University of Waterloo (Canada)
Wen Gao	Peking University (China)
Wenjun (Kevin) Zeng	University of Missouri (USA)
Xiaodong Wang	Columbia University (USA)
Yi Pan	Georgia State University (USA)
Yingfei Dong	University of Hawaii (USA)
Yueping Zhang	Nanyang Technological University (Singapore)
Zhenge (George) Sun	ZTE Corporation (China)
Zhili Sun	University of Surrey (UK)

CONTENTS

Submission of a manuscript implies that the submitted work has not been published before (except as part of a thesis or lecture note or report or in the form of an abstract); that it is not under consideration for publication elsewhere; that its publication has been approved by all co-authors as well as by the authorities at the institute where the work has been carried out; that, if and when the manuscript is accepted for publication, the authors hand over the transferable copyrights of the accepted manuscript to *ZTE Communications*; and that the manuscript or parts thereof will not be published elsewhere in any language without the consent of the copyright holder. Copyrights include, without spatial or timely limitation, the mechanical, electronic and visual reproduction and distribution; electronic storage and retrieval; and all other forms of electronic publication or any other types of publication including all subsidiary rights.

Responsibility for content rests on authors of signed articles and not on the editorial board of *ZTE Communications* or its sponsors.

All rights reserved.

Special Topic: Recent Advances in Smart Grid

Review

CONTENTS

ZTE COMMUNICATIONS
Vol. 13 No. 3 (Issue 47)
Quarterly
First English Issue Published in 2003

Supervised by:
Anhui Science and Technology Department

Sponsored by:
Anhui Science and Technology Information Research Institute and ZTE Corporation

Staff Members:
Editor-in-Chief: Sun Zhenge
Executive Associate Editor-in-Chief: Huang Xinming
Editor-in-Charge: Zhu Li
Editors: Paul Sleswick, Xu Ye, Yang Qinyi, Lu Dan
Producer: Yu Gang
Circulation Executive: Wang Pingping
Assistant: Wang Kun

Editorial Correspondence:
Add: 12F Kaixuan Building,
329 Jinzhai Road,
Hefei 230061, P. R. China
Tel: +86-551-65533356
Fax: +86-551-65850139
Email: magazine@zte.com.cn

Published and Circulated (Home and Abroad) by:
Editorial Office of
ZTE Communications

Printed by:
Hefei Tiancai Color Printing Company

Publication Date:
September 25, 2015

Publication Licenses:

ISSN 1673-5188
CN 34-1294/ TN

Advertising License:
皖合工商广字0058号

Annual Subscription:
RMB 80

Research Papers

Roundup

Guest Editorial
Kun Yang and Yingfei Dong

Recent Advances in Smart Grid

▶ Kun Yang

Professor Kun Yang received his PhD degree from University College London (UCL). He received his MSc and BSc degrees from Jilin University, China. He is currently a chair professor in the School of Computer Science and Electronic Engineering, University of Essex, and leads the Network Convergence Laboratory there. Before joining the University of Essex in 2003, he worked for several years at University College London on EU research projects. His main research interests include heterogeneous wireless networks, fixed-mobile convergence, future Internet technology and network virtualization, and cloud computing and networking. He manages research projects funded by sources such as UK EPSRC, EU FP7/H2020, and industries. He has published more than 60 journal papers. He serves on the editorial boards of both IEEE and non-IEEE journals. He is a senior member of the IEEE and a fellow of IET.

▶ Yingfei Dong

Professor Yingfei Dong received his B.S. degree and M.S. degree in computer science at Harbin Institute of Technology, China, in 1989 and 1992, his PhD degree in engineering at Tsinghua University in 1996, and his PhD degree in computer and information science at the University of Minnesota in 2003. He is an Associated Professor at the Department of Electrical Engineering of the University of Hawaii at Manoa. His research mostly focuses on computer and network security and privacy, especially in security and privacy issues in network design and protocols, cloud computing, smart grid, unmanned aerial vehicles, real-time networks, distributed systems and applications. He has published about 90 refereed research papers in various international journals and conferences. He has also served as associated editors for three international journals, and as organizer and program committee member for many IEEE/ACM/IFIP conferences. His research has been supported by US National Science Foundation.

A smart grid is the next-generation electric grid that enables efficient, intelligent, and economical power generation as well as reliable, safe, robust transmission and distribution. It uses modern information and communications technologies, such as advanced sensing, monitoring and processing technology, and high-speed bi-directional communications and networking. In recent years, the smart grid has attracted significant attentions from academics, industry, equipment manufacturers, and service providers. Developing the smart grid has become a global trend due to the immense potential benefits including enhanced reliability and resilience, higher operational efficiency, more efficient energy consumption, and better power quality.

We received strong responses to this call for papers on Recent Advances in Smart Grid from universities, research institutes, and industry. Following a peer-review process, we have selected five papers for inclusion in this special issue.

The first paper, "Theory Study and Application of the BP-ANN Method for Power Grid Short-Term Load Forecasting," aims at improving the accuracy of short-term load forecasting in a power system. To this end, the authors propose a new predictive model using the BP-ANN-based method from a neural network. A theoretical background and numerical results are also given in this paper.

The second paper, "A Solution-Based Analysis of Attack Vectors on Smart Home Systems," first presents a short survey of privacy and security in the broader smart-world context and then analyzes and ranks attack vectors or entry points into a smart home system and propose solutions to remedy or diminish the risk of compromised security or privacy.

In the third paper, "Secure Communication Networks in the Advanced Metering Infrastructure of Smart Grid," the authors propose a security protocol for the advanced metering infrastructure (AMI) with two-way communication in a smart grid. The work proposes a security protocol specifically for the AMI to meet the security requirements.

The methods for efficient network resource management are proposed in the fourth paper, "Reliable Remote Relay Protection in Smart Grid." The authors discuss simple backup solutions in the previous work. They also focus on improving the system reliability by exploring known power system information and minimizing the chances of false trips of important remote relays. Moreover, in order to further improve the system reliability, the authors investigate the peer-to-peer protection approaches to address the single point of failure of centralized control center.

The authors of the final paper, "Experimental Study on Cloud-Computing-Based Electric Power SCADA System," discuss the main issues in applying private cloud architecture to power system control and propose a professional private cloud solution to integrate the electric power SCADA system. In particular, experimental study has been conducted.

We would also take this opportunity to thank all the authors, reviewers, and editors in ZTE involved in this special issue.

DOI: 10.3969/j.issn.1673-5188.2015.03.001
http:http://www.cnki.net/kcms/detail/34.1294.TN.20150909.1043.004.html,published online September 9, 2015

Theory Study and Application of the BP-ANN Method for Power Grid Short-Term Load Forecasting

Xia Hua[1], Gang Zhang[2], Jiawei Yang[3], and Zhengyuan Li[1]
(1. Gansu Electric Power Research Institute, State Grid Gansu Electric Power Company, Lanzhou 730050, China;
2. Institute of Water Resources and Hydro-Electric Engineering, Xi'an University of Technology Xi'an 710048, China;
3. College of International Communications, China Three Gorges University, Yichang 443000, China)

Abstract

Aiming at the low accuracy problem of power system short-term load forecasting by traditional methods, a back-propagation artificial neural network (BP-ANN) based method for short-term load forecasting is presented in this paper. The forecast points are related to prophase adjacent data as well as the periodical long-term historical load data. Then the short-term load forecasting model of Shanxi Power Grid (China) based on BP-ANN method and correlation analysis is established. The simulation model matches well with practical power system load, indicating the BP-ANN method is simple and with higher precision and practicality.

Keywords

BP-ANN; short-term load forecasting of power grid; multiscale entropy; correlation analysis

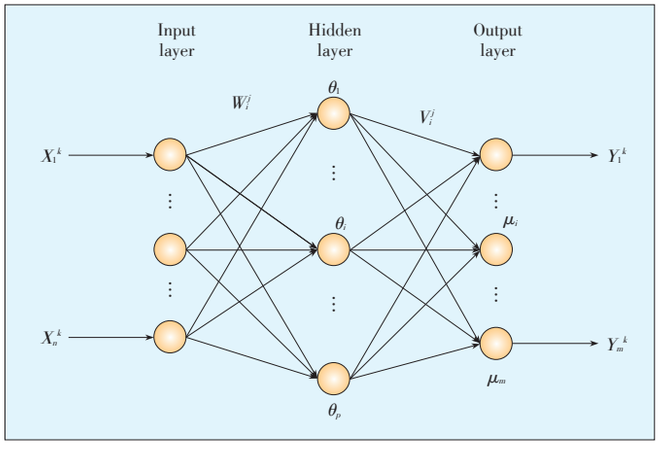
1 Introduction

The short-term load forecasting is an important component of the power system generation projects, which supports the economic and stable power system operation [1]. Increasing the forecasting precision of power grid load has been a major concern all over the world. Recently, many short-term load forecasting methods have been studied, such as regression analysis method [2], exponential smoothing model [3], random time series model, grey forecasting model, support vector machine and its improved model [4]–[6], neural network and its improved model and combination forecasting model [7], [8]. Most of these methods can be divided into two types according to the utilized data, one takes the weather factors into account, while the other does not involve weather data. The two types both have advantages and apply to different situations. The type without weather impact mainly uses historical data, which has easy model and calculation, but the precision is relatively low. The other type includes weather and many impact factors, but most of these impact factors are predictive data, which introduce bigger errors in load forecasting model, not to mention that some weather factors are difficult to obtain. Therefore, it is significant to find a precise load forecasting method with few impact factors.

In this paper a back-propagation artificial neural network (BP-ANN) based load forecasting method is presented, to balance the problem of precision and impact factors. Firstly we pick historical load data and employ multiscale entropy analysis. Then we build the BP-ANN load forecasting model based on the screened historical data. The load forecasting model is applied to practical load prediction and compares with two literature forecasting methods, in order to verify its superiority and high precision.

2 BP-ANN Basic Principles

BP network is one of the most commonly used neural network modes, which owns several advantages: 1) has simple structures and operability; 2) can realize any complicated nonlinear mapping since basically it is nonlinear mapping from input to output; 3) has self-study ability for further improvement and development. Based on these advantages of BP network, we employ the 3-layer BP network to dynamically evaluate the Muskingum model parameters. **Fig. 1** gives out the topological structure of the 3-layer BP network. We divide the 3-layer BP network into input layer, hidden layer and output layer, the point numbers of each layer are n, p, m, respectively. W_i^j (i = 1, 2, ... , n; j = 1, 2, ... , p) represents the weight between the input layer and hidden layer, while V_i^j (i = 1, 2, ... , p; j = 1, 2, ... , m) represents the weight between the hidden layer and output layer. The threshold values of the hidden and output layers are θ_i (i = 1, 2, ... , p) and μ_i (i = 1, 2, ... , m), respectively. The self-study processes of the BP network have been thoroughly discussed in literatures [1].



▲**Figure 1. The structure of BP-ANN.**

According to the basic principles of BP-ANN method, the precondition of BP network forecasting is determining the input and hidden layers. As for the power load forecasting, i.e., use historical data to forecast the load of a future moment, the input layer plays the key role, since yet there is few effective method to determine the hidden layer parameters.

3 Multiscale Entropy of Load Data

3.1 Basic Principles of Multiscale Entropy

The entropy has been widely used to characterize the complexity of information, and is the measurement of the system randomness. The Kolmogorov-Sinai (KS) entropy can characterize the complexity of the signals by calculating the average generation rate of new information. The approximate entropy (ApEn) originates from KS entropy, and applies well in the complexity analysis of short-term time series. The sample entropy (sampEn) is the further modification of the ApEn.

3.1.1 Sample Entropy

The similar data comparison of the ApEn calculation contains the comparison with its own data part, which causes result errors. The sampEn is the precise value of the average natural logarithm of conditional probability, and avoids the comparison with its own data. Thus the sampEn calculation does not depend on the data length, showing better consistence than ApEn.

Set the initial time series as $x(1), x(2), \dots, x(N)$, the sampEn of the series is calculated as follows:

1) Construct a m-dimension vector $X(i) = [x(i), x(i+1), \dots, x(i+m-1)]$, $i = 1, 2, \dots, N-m+1$;
2) Define the distance between $X(i)$ and $X(j)$ as $d[X(i), X(j)] = \max[\,|x(i+k)-x(j+k)|\,]$, $k = 0, 1, \dots, m-1$;
3) Give the number of threshold values r and obtain the ratio $C_i^m(r) = [\textit{the number of all } d[X(i), X(j)]<r]/(N-m)$, $i = 1, 2, \dots, N-m+1$;
4) Calculate the average value of $C_i^m(r)$ for all i, $C^m(r) = C_i^m(r)/(N-m+1)$, $i = 1, 2, \dots, N-m+1$;
5) Add the dimension to $m+1$, then repeat processes 1–4 to get $C^{m+1}(r)$;
6) SampEn of this series $\text{sampEn}(m, r, N) = -\ln C_i^m(r)/C_i^m(r)$.

Apparently the values of m, r are very important to the sampEn results. Generally we choose $m = 2$, $r = 0.1$-0.2 SD, where SD is the standard deviation of the initial data $x(i)$, $i = 1, 2, \cdots, N$, and the series length N is required to be larger than 1000.

3.1.2 Multiscale Entropy

The parameters of ApEn, sampEn are determined by the system step finite difference $(H_{n+1}-H_n)$, which is based on the single scale analysis and does not contain the system characters of high scale >1. The multiscale entropy analysis is calculated as following processes, in which τ is the scale index, when $\tau = 1$ the time series $y_j(\tau)$ is the initial time series.

Set the initial data as $\{x(1), x(2), \dots, x(N)\}$, now we construct the coarse-graining series $\{y(\tau)\}$:

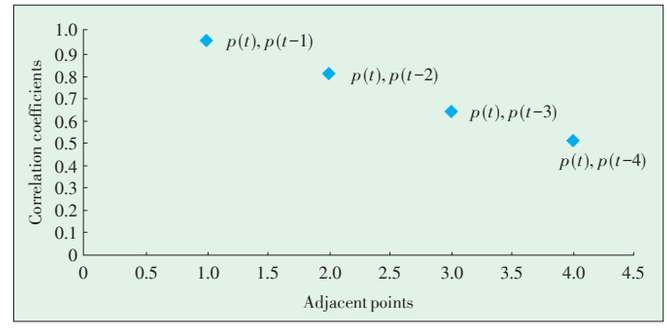
1) $y_j(\tau) = x(i)/\tau$, $i = (j-1)(\tau+1), \dots, j\tau$, $j = 1, 2, \dots, N/\tau$. The length of each time series equals the ratio of the initial time series length to scale index τ.
2) Calculate the sampEn of the coarse-grained series for different τ.

3.2 Load Analysis by Multiscale Entropy

Researchers generally use the adjacent data points before the predictive data point as the input data in the BP-ANN model for load forecasting [9], [10], because it is usually believed that the predictive points only relate to the changing trend of recent and adjacent data. In this paper we calculate the correlation coefficients of predictive points and adjacent points, which are illustrated in **Fig. 2** All data come from the daily load of Shanxi Grid in 2004.

Fig. 2. shows the changing trend of the predictive points and 4 adjacent points. The $p(t)$ represents the predictive load point value, and $p(t-1)$ represents the previous load point value before the predictive load point, and so on. Clearly, it is found that the correlation coefficients between predictive points and adjacent points gradually descend.

Then we utilize the multiscale entropy to evaluate the calcu-

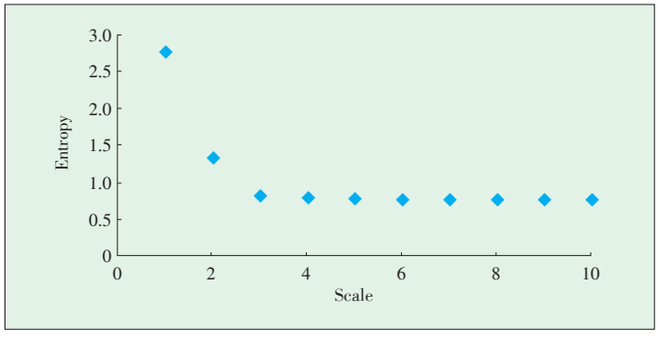


▲**Figure 2. Correlation coefficient of calculating point and adjacent point.**

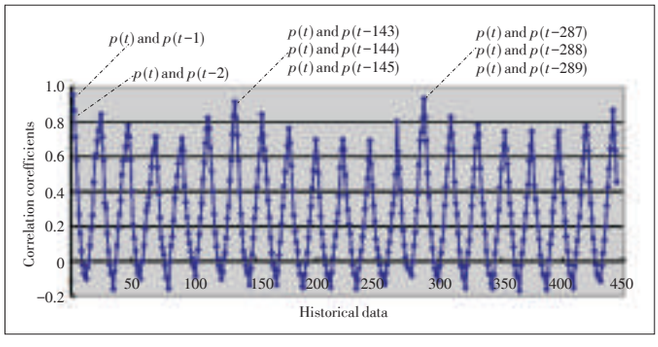
lation error introduced by adjacent data points in BP-ANN model. We pick the daily load data of Shanxi Grid (from 2003.1.1 to 2009.12.31) as the database, and calculate the entropy of load data through the above method in chapter 2.1, with parameters m = 3, r = 0.1 SD. The calculating results are demonstrated in **Fig. 3**. The entropy of load data decreases with the increment of scale index. Note that the entropy changes rapidly between scale 1 and scale 2, indicating that adjacent points introduce strong chaos. Combining with Fig. 2, it is clear that adjacent data points definitely affect the forecasting precision in BP-ANN load forecasting model. As a result, the forecasting model should be established based on nonadjacent data points to increase precision.

4 Building BP-ANN Model for Short-Term Load Forecasting

Start from the correlation coefficients discussed above, we set up the BP-ANN model for short-term load forecasting. Firstly we pick the most relevant load data series with the predictive data series, as the input of the BP-ANN model. The correlation coefficients between the predictive point $p(t)$ and historical data is illustrated in **Fig. 4**. We find that the predictive load point $p(t)$ not only shows strong correlation with the adjacent two load points $p(t-1)$ and $p(t-2)$, also periodically correlates to long-term historical data. Thus these periodically correlated historical data can also be used to build the forecasting model as well. We choose 8 historical data points with the strongest correlation with $p(t)$ in Fig. 4 as the input of neural network. The parameter of hidden layer is 4, and the output is the predictive load data $p(t)$ of next hour. As a result, we build the 8-4-1 BP-ANN load forecasting model, which is schematically shown in **Fig. 5**.



▲Figure 3. Entropy of load data under different scale.

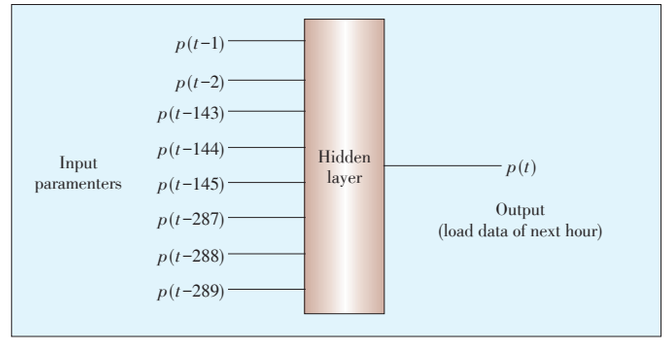


▲Figure 4. Correlation coefficient of prediction set and history set.

5 Application Examples of Shanxi Grid

Shanxi Grid mainly serves Shanxi Province and includes both hydropower and thermal power. The short-term load forecasting is of great significance for Shanxi Grid, which directly determines the operation mode of hydropower and thermal power. In this paper we use 24 short-term load data points from the year of 2003 to 2008 as the database, and employ the presented BP-ANN model for prediction. The results are verified with the load data of 2009. Also, we use the methods of literatures [10], (named as Method 1 and Method 2, respectively) to obtain predictive results, and compare the results of three methods through mean absolute error, error quadratic sum, and average relative error. The results are shown in **Table 1**. The result of the presented BP-ANN method in this paper has the lowest errors for all three evaluation index, which indicates its superiority and high precision.

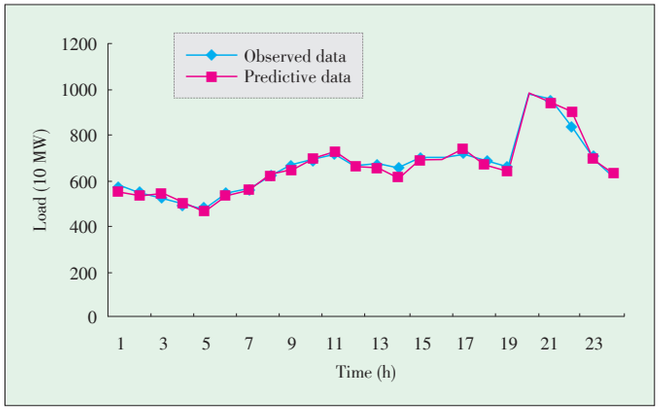
The presented BP-ANN method applies well to the short-term load forecasting of Shanxi Grid for its operability and stability. We predict one day load of Shanxi Grid in 2009 through the BP-ANN method, and give out the result in **Fig. 6**. We find that the predictive load data is in good accordance with the observed load data. The highly matched results imply that the simple presented BP-ANN method is with high precision and practical for short-term load forecasting in Shanxi Grid. This method opens another simple and accurate way to forecast short-term grid load, which owns great prospects for its feasibility



▲Figure 5. BP-ANN model for load prediction.

▼Table 1. Comparison of 3 prediction methods

Evaluation index	Mean absolute error (10 MW)	Error quadratic sum (10 MW^2)	Average relative error (%)
Method 1	0.12	4280	0.21
Method 2	0.08	3750	0.17
Presented BP-ANN method	0.03	2270	0.11



▲**Figure 6. Load prediction result of 2009.**

and precision.

6 Conclusion

This paper presents a simple and accurate BP-ANN method for the short-term load forecasting. We use the multiscale entropy to analyze the load data. The BP-ANN model using adjacent data points greatly affect forecasting precision. And the predictive load data not only shows strong correlation with the adjacent load data, also with periodic long-term data points. Therefore, we employ adjacent data correlation method to screen the input layer parameters of BP-ANN model, and establish the short-term load forecasting BP-ANN method. We apply the model and method to the short-term load forecasting of Shanxi Grid, and compare it with other two forecasting methods in previous literatures. The predictive results of the presented BP-ANN method owns the lowest average relative error 0.11% among three methods, and matches very well with the observed load data, which indicates the extremely high precision. Thus this method serves as a simple and feasible approach to realize precise short-term grid load forecasting.

References

[1] I. Drezga and S. Rahman, "Short-term load forecasting with local ANN predictors," *IEEE Transaction Power System*, vol. 14, no. 3, pp. 844–850, 2002. doi: 10.1109/59.780894.
[2] CH Hsien, "Grey neural network and its application to short term load forecasting problem," *IEICE Transaction Information System*, no. 3, pp. 897–902, 2002.
[3] X. Yao, M. Fischer, and G. Brown, "Neural network ensembles and their application to traffic flow rediction in telecommunications networks," *International Joint Conference on Neural Networks*, Washington, USA, 2001, pp. 693–698.
[4] L. C. Ying and M. C. Pan, "Using adaptive network based fuzzy inference system to forecast regional electricity loads," *Energy Conversion and Management*, vol. 49, no. 2, pp. 205–211, 2008.
[5] P. J. Santos, A. G. Martins, and A. J. Pires, "Designing the input vector to ANN-based models for short-term load forecast in electricity distribution systems," *Electrical Power and Energy Systems*, vol. 29, no. 4, pp. 338–347, 2007.
[6] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences*, vol. 1, no. 8, pp. 2297–2301, 1991.
[7] S. M. Pincus, "Approximate entropy as a complexity measure," *Chaos*, vol. 5, no. 1, pp. 110–117, 1995.
[8] J. S. Richman, and J. R. Moorman, "Physiological time-series analysis using approximate entropy and sample entropy ," *American Journal of Physiolog Heart*, vol. 1, no. 23, pp. 2039–2040, 2000.
[9] H. S. Hippert, C. E. Pereira, and S. R. Castro, "Neural networks for short-term load forecasting: a review and evaluation," *IEEE Transaction Power System*, vol. 16, no. 4, pp. 44–45, 2001. doi: 10.1109/59.910780.
[10] I. Dreaga, and S. Rhaman, "Input variable selection for ANN-based short-term load forecasting," *IEEE Transaction Power System*, vol. 13, no. 11, pp. 1238–1344, 1998. doi: 10.1109/59.736244.

Manuscript received: 2015-04-13

Biographies

Xia Hua (kevinxhua@163.com) received the bachelor degree in physics from Shanghai Jiao Tong University in 2009. He received his PhD degree in semiconductor physics from the Department of Physics and Astronomy, Shanghai Jiao Tong University from the Department of Physics and Astronomy, Shanghai Jiao Tong University in 2014. He is currently working in the Gansu Electric Power Research Institute, Lanzhou, China. His research interest focuses on new energy and photovoltaic systems.

Gang Zhang (zhanggang3463003@xaut.edu.cn) received his PhD degree in water resources and hydrology from Xi'an University of Technology in 2013. He is currently working in the Institute of Water Resources and Hydro-electric Engineering, Xi'an University of Technology. His research interest focuses on new energy and power saving.

Jiawei Yang is currently pursuing the bachelor's degree in Electrical Engineering and automation. His current interests include smart grid systems.

Zhengyuan Li is currently working in the Gansu Electric Power Research Institute, Lanzhou, China. His research interest focuses on power system protection.

DOI: 10.3969/j.issn.1673-5188.2015.03.002
http://www.cnki.net/kcms/detail/34.1294.TN.20150908.0928.002.html, published online August 12, 2015

A Solution-Based Analysis of Attack Vectors on Smart Home Systems

Andreas Brauchli and Depeng Li
(Department of Information and Computer Sciences, University of Hawaii at Manoa, HI 96822, USA)

Abstract

The development and wider adoption of smart home technology also created an increased requirement for safe and secure smart home environments with guaranteed privacy constraints. In this paper, a short survey of privacy and security in the more broad smart-world context is first presented. The main contribution is then to analyze and rank attack vectors or entry points into a smart home system and propose solutions to remedy or diminish the risk of compromised security or privacy. Further, the usability impacts resulting from the proposed solutions are evaluated. The smart home system used for the analysis in this paper is a digitalSTROM installation, a home-automation solution that is quickly gaining popularity in central Europe, the findings, however, aim to be as solution independent as possible.

Keywords

digitalSTROM; smart home systems (SHS); digitalSTROM server (dSS)

1 Introduction

As welfare increases and technological gadgets become ubiquitous, we lighten our daily lives by automating trivial and common tasks. A clear trend of automation technology usage within both personal homes and commercial buildings has been shown over the past few years. The increasing adoption of Smart Home Systems (SHS) leads to the need for not only more functionality but also for a safe, secure and function environment. The ongoing battle for smart grid security [1] includes smart homes [2]. When one technology becomes particularly wide spread it automatically creates a high-reward target type. Several companies offer products on the market to automate lighting, shades, heating, cooling etc. Among the many systems which feature different wired or wireless topologies is digitalSTROM (dS) with its powerline based bus and embedded central server. This research is dedicated to finding security and privacy weaknesses in SHS on the example of a dS system. Wherever possible we try to approach the problem in a generic way that can also be applied to other systems [3].

This works is organized as follows: We begin with this introduction and proceed with a review of how smart homes fit into the broader smart world context and present related work. In the fourth section the dS environment is covered before listing possible attack vectors on SHS in the fifth section along with two example attacks on the dS infrastructure. In section six, solutions to prevent or diminish those attack vectors are proposed and discussed. In section seven, we analyze the proposed solutions which are followed by the conclusions.

2 Smart World

With our world growing "smarter" than ever, there are different ways of integrating smart homes into the broader context of smart services, smart grids or even smart cities. Researchers of different fields have amply been studying this ongoing trend and come up with interesting and useful applications. We briefly present some of those to emphasize the security and privacy needs of a modern SHS, especially in the light of a majority of consumers being agnostic of technology and not necessarily trained in computer and network security. They may thus not be fully aware of what privacy invasions must be expected when certain sensory data is leaked or revealed from their smart environment.

In [4], the authors define smart communities as interconnected sets of co-located homes that share certain common processing infrastructure. The authors give an example of a distributed intrusion detection/aversion scheme based on surveilance data from multiple homes that is processed centrally in the community and an example of smart health care where neighbors are alerted when a critical health situation is detected. A call center responsible for multiple smart communities for emergencies or further assistance is introduced in this paper. While the au-

thors propose a centralized processing of data for privacy reasons, it is likely that not every smart community will want to maintain a data center on its premises. In [6], the authors predict a trend towards more artificial intelligence and thus processing power in future smart homes. The paper foresees that with the increasing number of sensors and readings, a single smart home might not be able to process all data and thus processes them in a cloud environment. Privacy is listed as a potential issue. In a similar light, a framework [5] is proposed to integrate smart homes into Platform as a Service clouds. Data privacy is supposedly managed by the user but the decision on which data to use and process seems to take place post transmission in the cloud. The cloud interface provides additional services or virtual smart home devices provided by third parties. Further improvements in the broad context of lifestyle are presented in [7] where Ambient Intelligence is mentioned. In this paper, we predicts how smart devices will carry an individual's preferences who will then experience personalized results in places like museums and other public places.

Overall, the trend is clearly geared towards a highly interconnected smart world where data is processed in a distributed fashion and the line between private data sharing, such as highly sensitive and individual medical records, and beneficial services is at risk of becoming increasingly blurred. In fact, both might not even remain separable due to design, marketing or infrastructural decisions. The problem is further amplified when individuals may not have a choice anymore in what part of the collected bulk sensor data is shared or even transmitted over a potentially insecure network. It is thus crucial to set the bar high for both security and privacy. Even when individuals do explicitly consent to data sharing the actual transmission protocol must always be open and reviewable for potential leaks (Ideally, the protocols are independently audited and published with unredacted raw data to the general public). Accountability is the key to gain the user's trust and, once obtained, can only be beneficial to the product's success. Since smart home installations have a comparatively long life time of several years or decades and process sensitive sensory information, interested parties will likely take their time to evaluate and research their options. Open source approaches are, in general, very favorable towards trustworthiness and, possibly, also towards the longevity of a product when the modifications and extensions can be installed by the owner/user without requiring specific tools or requiring digital signatures. Unfortunately the shift towards more open protocols is slow and customers might not always see the benefits of open solutions. A change is only expected to happen when demanded by a majority of customers or with comparably successful open solutions.

3 Related Work

This section lists related security research in the smart home context and explains the differences to this work. We conclude that there has been no previous security assessment of this kind on smart home environments with a wired power line bus type and, particularly, not for the dS architecture. The journal article [8] surveys available SHS technology but only briefly lists potential attack vectors on the SHS control infrastructure (DDoS). It also details personal security, i.e. not software system related security, automation logic proposals such as notifying emergency services when a fire is detected, unusual user behavior detection using neural networks and a privacy guard to protect against sensitive information leakage. The paper [9] covers the detect and prevent approach to several security issues in Wireless Sensor Networks in the SHS context. Several attack vectors that compromise confidentiality, integrity and availability are shared in this paper. In contrast, we analyze security issues on the example of dS products which uses a wired bus system with non-factory-default and optional wireless connectivity.

A meter reporting system [10] based on public key encryption that doesn't reveal specific power usage to the utility company is proposed. The system is based on signed readings by a trusted reader. The processing then directly applies the matching price tariff to those readings resulting in a fully verifiable bill without specific usage information. In this paper, we create a good solution to verifiably aggregate metering data but requires a trusted meter by the utility company, which the dS environment does not target or provide. A framework [11] for evaluating security risks associated with technologies used at home is proposed. The paper also associates high level attacker goals such as extortion or blackmail to low-level attacks compromising the infrastructure. We focus solely on low-level security issues and leave out inferring the potential consequences. In [3], the authors present a deep literature review of smart homes and provide a prediction of future development going towards integrated health care systems. Due to the amount of time that people spend in their homes, there is a large economic potential for integrated services. Additionally, the paper includes a section of papers dedicated to security. dS does not appear in any of the papers, however, some wired systems such as KNX are listed.

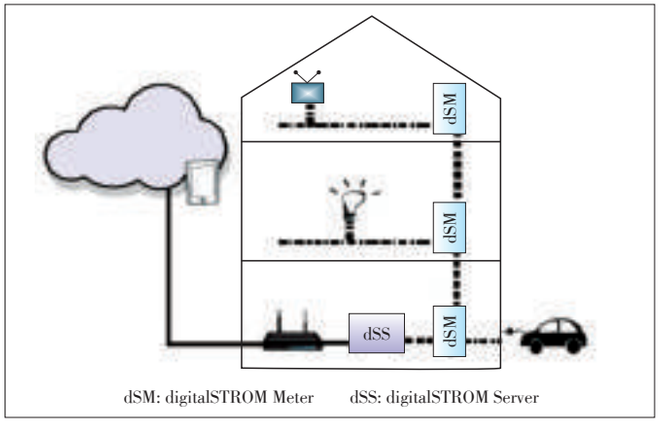
4 The digitalSTROM Environment

The digitalSTROM environment is a SHS designed primarily for personal home use. It can also be simultaneously used in multiple apartments of a building, whereas each apartment has its own installation. The installation consists of one (optional) digitalSTROM Server (dSS), usually one digitalSTROM Meter (dSM) and one digitalSTROM Filter (dSF) per circuit and numerous terminal blocks (small clamps) with a digitalSTROM chip (dSC) for each device. The dSF is responsible for filtering out dS messages on the power bus from and prevent them from reaching the outside world. It is technically required when multiple dS installations are present nearby to prevent crosstalk.

Each dSM can handle up to 128 clamps and communicates with the other dSM and the dSS by use of the ds485 (is an analogy to the serial RS485 bus protocol.) two-wire protocol. The ds485 bus can span up to 100 m but is usually confined within the cabinet (dashed line in **Fig. 1**). DSC are conventionally integrated in a terminal block ("clamp") that, in turn, is connected directly to a power switch or an appliance. The DSC can also be integrated directly into an appliance, into a power socket or a socket list by a licensed manufacturer. The appliances communicate over the power wire by use of a proprietary closed protocol (dash-dotted line in Fig. 1). The bandwidth available to dS devices is very limited with100 bauds (dSM→dSC) / 400 bauds (dSC→dSM) [12]. The reaction time for events is between 250 and 750 ms. Fig. 1 shows a simplified SHS consisting of three separate power circuits (one per floor), two dS appliances (TV, light on the dash-dotted line) and a non-dS charging electric vehicle on an outdoor plug. The dSM are interconnected (dashed lines) with the dSS by the 2 wire bus. The dSS is connected to the home network, symbolized by the wireless router, by a Cat.5 cable or, optionally, by a supported wireless USB dongle. A control device (typically a smart phone or tablet) is connected to the home network with the wireless network. The dSS provides a web interface for configuration and an AJAX/JSON Application Programmable Interface (API) for control.

5 Attack Vectors on SHS

We grouped the possible SHS attack vectors into five vulnerability categories which are detailed in this section: Wired SHS commonly use (1) a server for state management and to provide a control interface or API, (2) a bus for communication with the appliances and (3) a small clamp or control-device for switching individual appliances. This system is ultimately controlled by the user with (4) a control-device such as a smart phone. Additionally, (5) remote third party services may be contracted to extend the system's core functionality. The categories and their communicative interaction are visualized in **Fig. 2**.

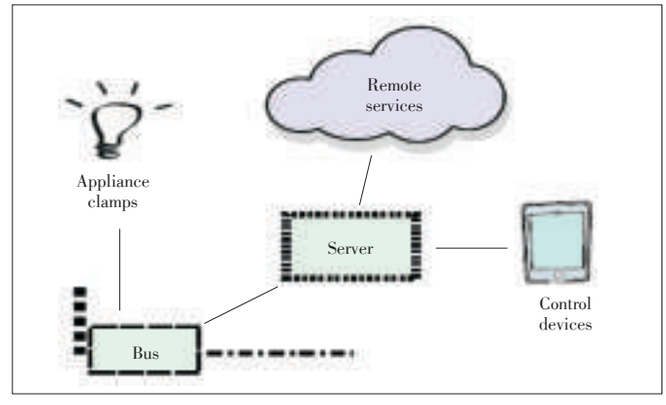


▲**Figure 1. A sample digitalSTROM SHS.**

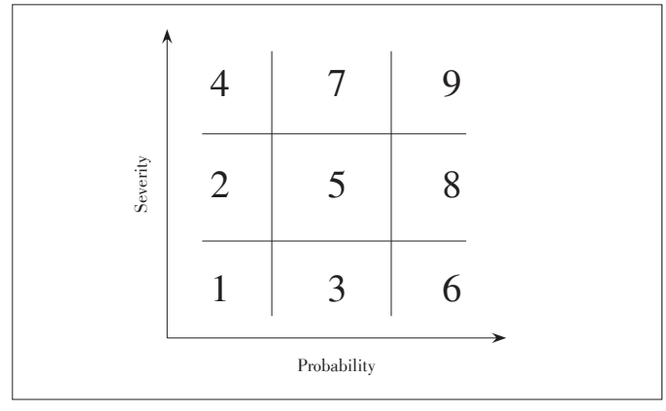
We divided the attacks into the nine relative and perceived risk categories: low, medium and high in each of the two dimensions severity and probability shown in **Fig. 3**. The risk is based on how likely and severe a given attack is. We note that more probable attacks are assigned higher risk ratings than more severe ones.

5.1 Central digitalSTROM Server

This first subsection elaborates on the possibilities to gain access to the central dS server as a mean to compromise the entire SHS. The central server has total access privileges to the SHS: It can switch appliances, read out metering values, manages API connections on the home network and runs virtually permanently. The server is thus the most crucial component to secure within the SHS. Due to the many interfaces it is also the most exposed part. This server role is assumed by the dSS component and is located in the cabinet. In dS systems, the location is dictated by the proximity to the dSM circuit meters. The dSS is an embedded Linux platform with 400 Mhz ARM9 CPU, 64 Mb ram, 1 Gb flash memory, two USB ports and an RJ45 100 Mbit Ethernet port. It features an on-board RS-232 serial port for recovery purposes [13]. The first possibility to attack the dSS is to gain physical access and compromising the root



▲**Figure 2. The risk categories.**



▲**Figure 3. The nine risk categories.**

system password. This can be done using the debug ports to gain access to the serial console and thus the (uBoot) boot-loader. Earlier versions of the dSS featured only 256 Mb flash storage but used an SD card as main storage drive which adds the possibility of maliciously switching SD cards to one with added or modified credentials. Due to the high impact but local constraint (physical access required), this attack is rated at risk level four. The second possibility is to gain access to the local wired or, if available, wireless network and (1) exploit a system vulnerability (e.g. TCP/IP vulnerability in the

Linux IP stack or network driver both LAN or WLAN if a WLAN dongle is plugged to the dSS), or (2) exploit a service vulnerability of a service running with system privileges, e.g. ssh server (Dropbear), if enabled. We note at this point that the dss process handling dS events does not run with elevated privileges. Alternatively an attacker can (3) exploit an API vulnerability within the dSS process. This attack is generally locally bound to the home network and wireless range but weak router/firewall rules may directly expose the dSS to the Internet and thus pose a major potential flaw. Since home automation systems are long-term systems with expected run times of 10–15 years, the software is highly likely to become outdated and unmaintained during its life cycle thus greatly increasing the risk. Due to the high potential severity we assign these two vectors the risk rating seven. Third, an attacker may target the server via the dS485 bus interconnecting the dSM by (1) directly gaining wire access, (2) indirectly by a rogue dSC that injects events that trigger a given message by the dSM on this bus. This attack is judged as having a medium-impact due to the ability to control the whole static SHS, i.e. the functionality of the SHS available when no dSS is installed, with low probability. Besides the impact on the powerline bus, it is questionable whether such an attack would be able to compromise the dSS integrity and would have to be determined by a code analysis of the dS485 bus handler process. We thus assign this attack vector the risk level two. The fourth attack possibility is to redirect or abuse the app store to (1) inject rogue updates with open backdoors, this is possible because updates are not digitally verified, or (2) rogue apps may be installed either by mistake or by misguiding the user into installing them. As dS apps do not have system privileges because they are run from within the dss process and are restricted to a JavaScript sandbox, the main threat is to privacy, as all events can be triggered and registered. Both rogue updates and apps can be installed when the attacker has control over the local network and can intercept and modify the home network traffic from and to the dSS as the updates are served through an unencrypted HTTP connection. Without local access, it is very hard to manipulate network traffic, however, due to the high impact of a compromised update, this attack vector is assigned the risk level four. When considering rogue apps, we increase the risk to level five due to the higher probability of such an attack but lower severity: tricking a user into installing a rogue app is possible but depends highly on the victim.

5.2 Smart Control Devices

This subsection describes how a compromised Smart Control Device (SCD) such as a smart phone or control station leads to a compromised SHS.

Besides the wall switches in rooms, control of the SHS is generally delegated to trusted and/or authenticated control devices such as smart phones or control terminals. In the dS case, the JSON-API is only accessible by a secure HTTPS connection and requires a token that is obtained after successful authentication. However, if a control device such as an Android or iPhone smart phone is compromised, the control of the whole system, as far as API support reaches, is consequently compromised until the token is revoked or expires, in case the device doesn't store the actual credentials. DS does not currently feature specific (usually wall-mounted) control terminals, thus this scenario is omitted. DS published both an iOS and Android app. Since smart phones are mostly connected to the Internet they are exposed to many third party apps and, possibly, viruses or worms. Additionally the device usually has full access to the home network. These facts lead to a high-risk attack vector with risk category nine.

5.3 Smart Home Communication Bus

In this subsection we analyze the risks of a compromised communication bus. The implications of which directly lead to a largely compromised SHS. DS uses an proprietary but unencrypted protocol for its communication on the power wiring (powerline) [12]. As the protocol uses neither encryption nor authentication, any received messages are assumed to be valid. This opens the possibility for (1) injecting control signals to directly control appliances or disrupt the system, or (2) inject invalid power readings to falsify the report system power consumption. When falsifying consumption readings, this only falsifies the reading of individual single devices as the dSM is aware of the total sub-circuit consumption independently of any attached dSC. Having access to the communication bus allows easy jamming of the SHS thus creating a Denial of Service (DoS) type attack. The low bus bandwidth makes this attack particularly effective. The attacker has the choice of jamming only the sub-circuit with the attached rogue sender device or the whole system by continuously sending systemwide events, such as alarms, that are then broadcast by the dSM into the adjacent sub-circuits. As all dS appliances have access to the powerline bus and thus have full control of the bus within its sub-circuit, an attacker may attach a rogue appliance anywhere in the system. If the attacker does not have physical access, he may still trick someone who does into plugging in an appliance for him, for instance by gifting or lending such a prepared appliance. DS appliances can be anything from a lamp to a TV or computer. As dSC clamps are relatively small and only draw minimal power, they are easily hidden inside an ap-

pliance case. An alternative and limited attack consists of connecting unmodified original dS clamps to the system which automatically registers and adds the device, an automatic Plug-n-Play (PnP) procedure which takes less than 10 minutes. Once registered, the device is ready for use: e.g. a clamp with a yellow color code4 switches all room lights in the room it's plugged in. A generic panic button will trigger the panic procedure which defaults to turning on all lights and opening all shades and blinds in the entire installation. With the locally limited exposure of the powerline bus, generally secure premises (except for outdoor plugs) but with high control level, this attack vector is rated a risk category four (private home without outdoor plugs) or seven (with easily reachable outdoor plug or when the SHS is a semi-public environment such as an office space.) An alternative point of entry is the ds485 bus interconnecting the dSM and dSS. The implications are the same as compromising the powerline bus with an additional small but unverified possibility of exploiting the dSS's process by buffer overflow. This attack does not seem very likely or attractive as dSM are usually located next to the more rewarding dSS. We thus assign the risk category four.

5.4 Remote Third Party Services

This subsection analyzes the trust implications of connecting third party services with the SHS. A third party service provides additional functionality to the SHS. Those services can be classified into two categories: (1) monitoring services and (2) control delegation services. A service can also be classified in both categories simultaneously. The monitoring services accept consumption statistics, system events or other collected data and provide a suggestive or analytical service based on the data interpretation. As such this type of service imposes purely a privacy risk as identifying events such as home presence and activities may be leaked [18]. We rank this attack vector at risk level three but the actual danger could highly vary depending on the nature of the leaked information and the danger that such a leak could go unnoticed for a very long time. The second category of services requires control permissions and thus API access by token which may be revoked individually [18]. Such services may for instance provide an alternative Internet-based user interface. By consequence, a compromised third-party service directly implicates a compromised SHS and carries an elevated risk rated at seven or nine, depending on how secure and trustworthy the third party service is. DS offers such a service called "mein.digitalSTROM" [19] using a dS app which allows remotely controlling the installation. It also allows temporary control delegation with a time expiring link and backs up local configuration and metering data. It is inevitable that all third-party services be trusted with private data and system control respectively.

5.5 Two Attack Scenarios

In this sub-section, we elaborate on two theoretical attack scenarios based on our previous analysis. The first attack uses the dS Android smart-phone app [14] as entry vector and switches lights on at night when the home owners are sleeping. The second attack uploads power readings to a remote server, allowing the attacker to know when the home is empty or will likely be. The first attack is created by installing a rogue app on the home owner's Android smart phone. This app poses as totally unrelated app to the SHS. Once the app is installed on the SHS owner's smart-phone, it launches a background service that sends an Android intent [16], a cross app message using the dS app's public interface, to the dS app sometime during the night. The unmodified and unknowing dS app then performs the action using the stored credentials. The malicious apps does not need to know any connection details or the API token. While the attack may sound banal, more frightening scenarios can be envisaged. In the second attack, the dS app is user-installed on the dSS using the official dS app-store. Once installed, the app collects consumption data from all connected dSM and periodically uploads them to a remote location. The attacker uses this collected data to establish when the residence is likely to be empty. We do note that third party apps will likely have to pass a code review before being entered into the dS app-store. There are enough legitimate uses for sending private data and the app should thus pass a code inspection based on different expectations by the reviewer and the app's user, especially if the documentation is ambiguous, suggestive or simply missing.

6 SHS Hardening

This section is modeled after the previous chapter: It is organized into central dS Server, Smart Control devices, Smart Home Communication Bus and Third Party Services. In an effort to harden SHS against the attacks described in the previous section, we recommend adopting proven strategies from other domains. In addition to providing security-enhancing suggestions, we reflect on the usability impact of the proposed solutions.

6.1 Central digitalSTROM Server

This subsection reiterates the crucial role of the central dS Server in the overall system security. Because of its central role and exposure to different interfaces in the SHS, a physical server breach is rated at both the highest severity and highest probability. To protect against physical server breaches, the easiest and, at the same time, most effective method is, arguably, to lock the cabinet if it is located in a (semi-) public space. This should be recommended to every customer through the installation documentation. This solution

has a low usability impact and leaves the choice and risk assessment to the customer. Within private spaces the risk of a physically compromised dSS is rated low. If additional security is desired, one could make use of a tamper-evident case which

may avert certain attackers. This change requires a customer to be aware of how to check the integrity seal, which could possibly be done remotely, but does still require a lock secured cabinet. A tamper-evident case incurs a high usability impact due to needed additional training. To protect against network-based attacks on the dSS it is important to make the user change the default access password, preferably during the initial setup. A default access password together with an open network results in a very high probability and high severity risk. Usability is only minimally impacted by requesting the user to set a password on setup. The initial setup could be streamlined by a setup wizard which would cover this step. To prevent Man-in-the-Middle (MitM) attacks such as modifying system or app updates, dS update servers should default to an encrypted HTTPS connection with a valid SSL certificate. Such a secure connection is transparent to the user and does thus not incur any usability changes. To reduce the risk of a totally compromised SHS the introduction of a permission based access control system for the API is suggested. Possible permissions include reading out meter values, controllable dSMs/rooms such that an application may be restricted to controlling appliances in one sub-circuit or even individual appliances, the events that can be triggered and the events that one can register with. This list is not exhaustive and further permissions may be applicable. There is a certain trade-off between usability and permission-configurability as analyzed by [15], however, the impact could be lessened by allowing full permissions by default and leaving the specific constraining to knowledgeable users within the "advanced settings" menu option.

6.2 Smart Control Devices

SCD have full control over the SHS. Thus it is crucial to educate all users that a compromised SCD implies a compromised SHS. The dS app for Android provides other apps on the smart phone with the possibility to send intents (Android control messages) that the app will then react upon. Thus any app on such a smart-phone can control the SHS. We propose adding a white-list of registered apps, managed by the user, to the Android dS app to verify that a certain app is allowed to control the SHS. The list would be updated on the fly upon first request as to incur usability only minimally. Users may also feel more secure when they know which apps can, or are trying to, control their SHS.

6.3 Smart Home Communication Bus

DS uses a proprietary protocol for communication between dSC and dSM. The technology does not permit inter-dSC communication without going through a dSM first due to separate up and downstream channels. If one were to reverse engineer the communication protocol and implement a device speaking the protocol or a reverse engineering a dSC's interface/firmware, an attacker could easily inject messages or jam the circuit and installation and create a DoS attack. We thus strongly recommend investigating adding an encryption layer such as [17] targeting low power and very low overhead settings. An encryption layer may incur a moderate overhead in usability if keys have to be set up by the user. We further suggest adding an option to disable the PnP functionality for automatically registering new devices. Especially in semiprivate environments such as offices where power plugs are readily available to everyone having physical access. For ease of use we do not suggest disabling PnP by default, but when the auto-registration function has been disabled, we suggest adding a timer-based enable function—analogous to how bluetooth pairing works that allows auto-registering appliances that are plugged in during a short time frame. The usability impact of such a feature is minimal resulting in only one more option which could be placed within the advance configuration mode.

6.4 Remote Third Party Services

Remote services provide additional functionality to the SHS by either providing remote access to the dSS or by analyzing and reporting on collected data. To harden the system against privacy leaks, we suggest implementing configurable time-resolution limit permissions to the already proposed permission system. Such a resolution limit would e.g. not allow access to resolutions below a 15 minute-aggregation in order to maximize privacy. As such a restriction is optional, the usability impact remains small while giving the user a much greater sense of privacy. To harden against compromised third party services, a restricted set of permissions should be applied to remote controlled API accesses, additionally all API accesses and transactions should be logged for a future audit. As the user is responsible for checking the logs, he does incur a great usability impairment unless combined with a method of automatically checking logs for irregularities. A Third party app should only be accepted into the dS appstore when sufficient, clear and unambiguous documentation is available as to what data is being processed, sent off remotely and what control events are raised by the app. The code reviewers are responsible for checking the code paths against the documentation and ask for corrections before accepting it. Before installing an app, a user should have the possibility to accept or reject the requested functionality. There is a minimal usability overhead to display the app documentation which have to be manually accepted or rejected by the user.

7 Solution Analysis

We now look back on the sample attacks in the light of the suggested improvements and find that the attacks would not be possible anymore. We do note that all proposed solutions are

theoretical improvements based on the research and experience in related fields. The physical experimentation of the suggested solutions in this exact context is left as future work item. The first attack scenario uses the dS Android app to

stealthily inject control events into the SHS. With a whitelist of apps that are allowed to send control events through the dS Android app, any app on the smart phone would have to request permission before being granted access, thus thwarting a stealthy attack. A visual clue should make it apparent that

said app, which has nothing to do with SHS, pursues a malicious purpose when it seeks access to the SHS via the exposed Android intent.

The second app that sends consumption events to a remote server would have to declare the intent to send readings to a remote service in the documentation and request those specific permissions during the installation. If this is against the purpose of the app, the user should recognize the threat and choose not to install the app. After an implementation of our proposed solutions, both sample attacks would thus not be possible anymore.

8 Conclusion

We conclude this paper by reiterating that homes are very intimate places where people expect and deserve a high level of privacy and security at a level that is currently not

satisfyingly offered by the feature-driven industry. We have elaborated different attack vectors on a dS SHS which range from physical breaches, over networked attacks all the way to third party remote issues. We demonstrated actual abuse of two of those attack vectors and suggested various improvements to all of the pointed out attack vectors along with possible usability impairments resulting from the solutions. We hope that this research will lead to an increase of openness and security awareness from the early development process on in both generic SHS products and particularly to an improved digitalSTROM system.

References

[1] European Union Agency for Network and Information Security ENISA. *Smart grid security recommendations* [Online]. Available: http://www.enisa.europa.eu 2012

[2] National Institute of Standards and Technology NIST. *NISTIR 7628 guidelines for smart grid cyber security* [Online]. Available: http:www.nist.gov/index.html

[3] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes-past, present, and future," *IEEE Transactions on System, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 42, no. 6, pp. 1190–1203, Nov. 2012. doi: 10.1109/TSMCC.2012.2189204.

[4] X. Li, R. X. Lu, X. H. Liang, X. M. Shen, J. M. Chen, and X. D. Lin, "Smart community: an Internet of Things Application", *IEEE Communications Magazine*, no. 49, pp. 68–75, 2011.

[5] B. Eom , C. Lee, C. Yoon, H. Lee, and W. Ryu, "A platform as a service for smart home", *IJFCC*, vol. 2, no. 3, pp.253–257, 2013.

[6] D. Cook, "How smart is your home?" *Science* , vol. 335, no. 6076, pp.1579-1581, March 2012.

[7] M. O'Grady and G. O'Hare, "How smart is your city?" *Science*, vol. 335, no. 6076, pp. 1581–1582, March 2012.

[8] R. Robles and T. Kim. *A Review on Security in Smart Home Development* [Online]. Available: http://www.sersc.org/journals/IJAST/vol15/2.pdf

[9] K. Islam, W. Sheng, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," *2012 IEEE 16th International Conference* on *Computer Supported Cooperative Work in Design (CSCWD)*, Wuhan, China, 2012, pp.626-633.doi: 10.1109/CSCWD.2012.6221884.

[10] A. Rial and G. Danezis, "Privacy-preserving smart metering," *Proceedings of the 10th annual ACM Workshop on Privacy in the Electronic Society (ACM WPES11)*, NJ, USA, pp. 49–60. 2011.

[11] T. Denning, H. M. Kohno, and T. Leving, "Computer security and the modern home," *Communications of the ACM*, vol. 56, no. 1, pp. 94–103, 2013.

[12] Aizo AG. *digitalSTROM FAQ* [Online]. Available: http://www.aizo.com/de/support/documents/A0818D044V004 FAQ.pdf

[13] Aizo AG. *dSS 11 Produktinformation* [Online]. Available: http://www.aizo.com/de/support/documents/ digitalSTROMServerdSS11ProduktinformationV1.0.pdf

[14] Google Playstore, Aizo AG. *dS Home Control* [Online]. Available: https://play.google.com/store/apps/details?id=com.aizo.digitalstrom.control

[15] T. H. -J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. *Challenges in access right assignment for secure home networks* [Online]. Available: https://sparrow.ece.cmu.edu/group/pub/kim_bauer_newsome_perrig_walker_hotsec10.pdf

[16] Google Ltd. *Android API Reference* [Online]. Available: http://developer.android.com/reference/android/content/Intent.html

[17] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," *Proceeding in Sensor Network (IPSN07)*, Massachusetts, USA, 2007, pp. 479-488.

[18] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser. *Neighborhood watch: security and privacy analysis of automatic meter reading systems* [Online]. Available: http://www.winlab.rutgers.edu/~gruteser/papers/fp023-roufPS.pdf

[19] Aizo AG. *digitalSTROM Installation Manual* [Online]. Available: http://www.aizo.com/de/support/documents/html/digitalSTROM Installationshandbuch A1121D002V010 EN 2013-11-12/ index.html#page/digitalSTROM% 2520Installationshandbuch/digitalSTROM% 2520Installationshandbuch A1121D002V010 EN 12-11-2013 Final.1.56.html

Manuscript received: 2015-04-26

Biographies

Andreas Brauchli (andreasb@hawaii.edu) received his MS in Computer Sciences from the University of Hawaii at Manoa, USA (UHM) and his B.Sc. C. S. from the Federal Institute of Technology in Zurich, Switzerland (ETHZ). He is employed as Mobile Software Engineer at Sensirion and previously interned at AIZO where he worked on digitalSTROM smart home applications. His research position at the University of Hawaii focused on privacy and security in multiple domains, amongst others, he worked on the AllNet delay tolerant secure networking protocol. His interests lay in the fields of Open Source Software and the vast areas of security and privacy around the digitally connected life.

Depeng Li (depengli@hawaii.edu) obtained his PhD in computer science from Dalhousie University, Canada. He received his BS and Master Degree in Computer Science from Shandong University, Jinan, China. He is currently an Assistant Professor in Department of Information and Computer Sciences (ICS) at University of Hawaii at Manoa (UHM). Before that, he had been worked in RIM (Blackberry) in Ottawa, Canada and Microsoft, Redmond, US to release Blackberry smart phone and Windows 7, respectively. He had also been worked as Post-Doc researcher for MIT and Masdar Institute cyber security project. His research interests are in security, privacy, and applied cryptography. His research projects span across areas such as Internet of Things, smart grids, mobile Health-tech, aerospace safety and physical-human-cyber triad. He had published around 40 papers at some famous journals and conferences.

DOI: 10.3969/j.issn.1673-5188.2015.03.003
http://www.cnki.net/kcms/detail/34.1294.TN.20150909.0929.002.html, published online September 9, 2015

Secure Communication Networks in the Advanced Metering Infrastructure of Smart Grid

Feng Ye and Yi Qian
(Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE 68124, USA)

Abstract

In this paper, a security protocol for the advanced metering infrastructure (AMI) in smart grid is proposed. Through the AMI, customers and the service provider achieve two-way communication. Real-time monitoring and demand response can be applied because of the information exchanged. Since the information contains much privacy of the customer, and the control messages need to be authenticated, security needs to be ensured for the communication in the AMI. Due to the complicated network structure of the AMI, the asymmetric communications, and various security requirements, existing security protocols for other networks can hardly be applied into the AMI directly. Therefore, a security protocol specifically for the AMI to meet the security requirements is proposed. Our proposed security protocol includes initial authentication, secure uplink data aggregation, secure downlink data transmission, and domain secrets update. Compared with existing researches in related areas, our proposed security protocol takes the asymmetric communications of the AMI and various security requirements in smart grid into consideration.

Keywords

smart grid; advanced metering infrastructure; network security; privacy

1 Introduction

In smart grid, the communication networks have been updated to more complicated and bidirectional ones. Data transmitted more frequently over the networks in much larger quantity. Therefore, compared with the communication in traditional power grid, network security issues are more important [1]-[3]. The advanced metering infrastructure (AMI) is a system that collects and analyzes data from smart meters, and giving intelligent management of various power-related applications and services based on that data. An AMI has a hierarchical network structure. It consists of home area networks (HANs), neighborhood area networks (NANs), and a wide area network (WAN). In each HAN, there is a smart meter which monitors the energy consumption of the appliances and other power line status in that household. Metering data (data that is generated by smart meters) is uploaded to the metering data management system (MDMS) at the service provider side. Based on the metering data and other monitoring data from sensors, the service provider is able to have precise real-time monitor over the power grid. Moreover, demand response [4]-[7] can be applied with timely information exchange between the customers and the service provider. As a result of the modern control system, smart grid is more efficient and eco-friendly compared with the traditional power grid. However, in order to achieve optimal control and demand response through the AMI, the data in uplink transmissions from smart meters to the MDMS includes secret information. For example, power usage of a household is included in metering data. Those data will be collected by the MDMS and be further applied to determine the power generation and the usage of renewable energy. Nonetheless, power usage pattern may reveal lifestyle of the corresponding customers. The controlling data in downlink transmissions involve the price/tariff information. Forgery or manipulation of such information may let the demand response be astray from being efficient.

In this paper, we propose a network security protocol for the AMI. The WAN in AMI is a high speed backhaul network, which has robust security mechanisms from fiber optic networks or ethernet. Therefore, the security issues in AMI. Thus, our focus is on the wireless portion of the AMI, including smart meters from HANs and data aggregate points (DAPs) from NANs. Specifically, the proposed network security protocol includes four parts: initial authentication, secure uplink data aggregation, secure downlink data transmission, and domain secrets update. Initial authentication is for the nodes such as smart meters and DAPs to join the AMI. Security schemes for

The work was supported by the National Science Fourdation under Grant No. CNS-1423408.

uplink and downlink transmissions are independently designed because of the asymmetric communications. Data in the uplink is more in quantity and higher in frequency. It features a many to-one communication. Moreover, aggregated data is enough, for instance, the aggregated power consumption for the service provider. Nonetheless, confidentiality of the controlling data in downlink may not be an issue. For instance, pricing/tariff is supposed to be public for the customers. Data integrity and sender authentication are more important for such controlling data. In addition, domain secrets such as session keys, public/private keys, and other secrets need to get refreshed once in a while. In the proposed domain secret update process, the communications remain uninterrupted.

The rest of the paper is organized as follows. In Section 2, related work is discussed. In Section 3, the studied AMI is illustrated. In Section 4, the security schemes for the AMI are proposed. In Section 5, the conclusion and the future work are given.

2 Related Work

Although HANs and NANs in the AMI have structures of wireless mesh networks (WMNs) [8], [9], difference can be addressed in three holds. First, each smart meter must be available and be treated equally in the network since fairness must be applied to each of the customers while traditional WMN does not emphasize availability for each wireless node let alone fairness. Second, the deployment of smart meters are fixed and in specific orders since they are deployed in each household and the houses are in fixed position in most cases, while the wireless nodes in traditional WMN are usually deployed randomly and redundantly. Third, the uplink transmission and downlink transmission in AMI are asymmetric where the uplink transmission consists of different data from each smart meter to the MDMS and the most of the downlink transmissions are in broadcast mode, while in traditional WMN, the uplink or downlink can even barely be distinguished. Our proposed network security protocol is designed to match the uniqueness of AMI.

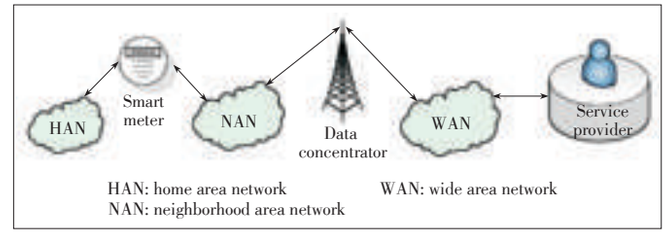
There are several researches for the security issues in AMI [10]–[13], however, there are very few comprehensive security protocols for AMI. In [12], the authors proposed a protocol called integrated authentication and confidentiality (IAC) which involves the initial authentication of a smart meter, and the security in both uplink and downlink transmissions. However, IAC has several problems to be addressed. 1) The smart meters are not treated equally where some of them are chosen to be the backbone nodes and proceed with security protocol, while the others must go through the backbone nodes, however the backbone nodes selection does not have any security concern. 2) The initial authentication process cannot prevent replay attack or even forgery if the initial request is overheard by the attacker. 3) The security protocol in uplink transmission cannot handle multiple incoming data at an intermediate node. 4) Compromise of a node will at least endangers another node since they share the same secret key for message encryption. 5) The security protocol for downlink transmission is too complicated since IAC did not consider broadcast scenario as the main transmission mode for downlink. 6) Once a node malfunctions in the network, IAC cannot function any longer. An improved security protocol for the AMI was proposed in [13]. However, it applied many digital signatures for uplink transmissions which may not be practical. As a preliminary work, the protocol was not comprehensive enough. For instance, some of the messages may suffer from replay attack, and domain secret update mechanism was not mentioned. In this paper, an enhanced security protocol which addresses those shortages is proposed.

3 Advanced Metering Infrastructure

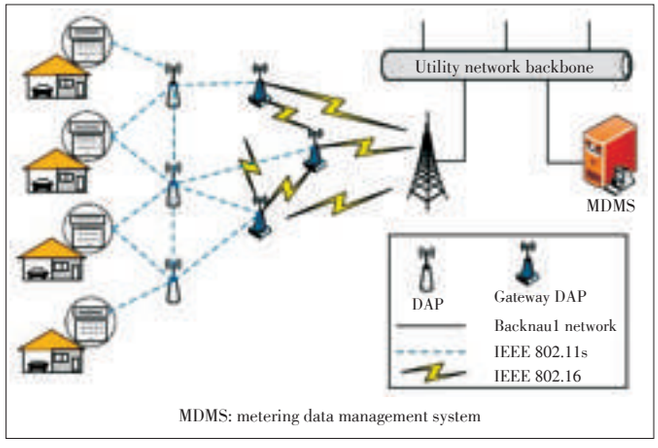
The communication networks of the AMI have a hierarchical structure, including HANs, NANs, and WAN. This structure is shown in **Fig. 1**. A HAN consists of several smart appliances and a smart meter (Some may suggest that a gas meter is also involved. However, for simplicity, we restrict the discussion to electricity power grid and rule out gas meters.) . The sensing/measuring of the power grid status inside households and apartments (e.g., energy-consumption, damage to power equipment, voltage-fluctuation, etc.) is gathered by smart meters. A NAN consists of many DAPs. Each DAP covers a few smart meters. The gathered data from smart meters is uploaded to the MDMS through DAPs. The gateway of a NAN is the data concentrator, which has fast and reliable network connection to the MDMS. Such fast and reliable network is the WAN. It covers a much larger area compared with a NAN.

Because the AMI has a complicated structure, there is no single communication technology that can perfectly fulfill all the needs in the AMI. For example, the optical fiber used in backhaul networks is reliable (0:99999 reliability) and fast (in the order of Gbps). However, it will be too expensive to use it in HAN where data is usually in the order of KB. Therefore, researchers have proposed to use different types of technologies so that communication requirements can be met while the deployment cost and the maintenance cost can be reasonably low.

In the studied AMI as shown in **Fig. 2**, various communication technologies are applied. A HAN is connected by local ar-



▲**Figure 1. Two-way communication networks in smart grid.**



▲Figure 2. Studied advanced metering infrastructure.

ea networks, e.g., IEEE 802.11 (Wi-Fi) and/or IEEE 802.15.4 (Zigbee). In a NAN, the DAPs form a wireless mesh network based on IEEE 802.11s (Wi-Fi based). Compared with Zigbee applied in HANs, Wi-Fi can achieve much higher transmission data rate. It is necessary because local NAN transmissions among DAPs introduce multi-hop wireless mesh networking and it requires higher data rate for the transmissions. Some of the DAPs are chosen as gateway DAPs which have direct communication with the concentrator. It is not necessary for the gateway DAPs to be close to the concentrator. In fact, multiple gateways need to be deployed sparsely in a NAN for its wide ranged latency requirement (3 ms to 5 min) [14], [15]. If a customer has too many hops to reach a gateway, it may not be able to successfully deliver the data with most critical latency requirements. Therefore, gateway DAPs are equipped with IEEE 802.16 (WiMAX) interface for longer distance transmission. Adopting WiMAX has a bonus compared with similar technology (e.g., LTE) that it can be deployed using unlicensed band (e.g., 5:8 GHz) in order to lower the service cost by not paying license band accessing fee. However, using unlicensed bandwidth must follow certain restrictions by the FCC [16]. Without loss of generality, the concentrator can be deployed in the center of the neighborhood. It is the gateway of the NAN to the wired backhaul network which connects to the MDMS (or the service provider) in a fast and reliable way.

In the uplink of AMI, information such as energy consumption and monitoring data is transmitted from the customer side to the service provider. In the downlink of AMI, information such as control message and pricing/tariff is transmitted from the service provider to the customer.

The data from customers (metering data) contains much privacy. For example, from the pattern of the energy consumption, it is possible to have a sketch of the lifestyle of that customer. Therefore, it is a must to provide confidentiality to metering data. In addition, integrity is also important to metering data. Manipulation of energy consumption (e.g., energy theft) may cause loss to the service provider. More importantly, manipulated energy consumption will deviate the service provider from optimal control of the power grid, in turn will lead to unnecessary fuel waste and pollution. However, non-repudiation may not be as critical as the other two security requirements for two reasons. 1) Providing non-repudiation which usually is achieved by digital signature may compromise the identity of the customer, and thus jeopardize the privacy. 2) Data in the uplink is frequently transmitted by simple devices such as smart meters, DAPs, sensor nodes. They are equipped with limited computational capability. Therefore, applying public key cryptograph frequently is not practical. The monitoring data of power grid status is gathered by low profile sensors (e.g., phasor measurement unit). Obviously, data integrity needs to be provided so that the service provider can monitor the grid correctly. However, with limited computational power and real-time transmission requirement, it is not necessary to provide confidentiality and non-repudiation to monitoring data.

In the downlink transmission of the AMI, the service provider sends control messages to customers or some components in the power grid. Since control messages usually have real-time transmission requirement and the privacy of control message may not be very important, confidentiality is not required for control messages. Nonetheless, data integrity is critical. Non-repudiation is supposed to be important since the control messages need to be verified from a legitimate sender (i.e., the service provider). However, due to the low-latency requirement and limited computational power at the receiver side, it varies from case to case. Pricing/tariff is also sent from the service provider to customers in downlink transmissions. Confidentiality of such information is not needed because it is for the public. Data integrity and non-repudiation is nonetheless critical.

4 Proposed Security Protocol for AMI

The proposed security protocol consists of four schemes, initial authentication scheme, secure uplink transmission scheme, secure downlink transmission scheme, and domain secret update scheme.

For simplicity, the notations of the keys used in the proposed security protocol are listed in **Table 1**.

4.1 Initial Authentication

An uninitialized node that does not function in the AMI

▼Table 1. Notations of the keys

K_i	Pre-shared secret key of n_i
k_i	Active secret key of n_i
Pu_i	Public key of n_i
Pr_i	Private key of n_i
$k_{i,j}$	Session key between n_i and n_j
Pu_{AS}	Public key of the AS
Pr_{AS}	Private key of the AS

properly must be authenticated through the initialization process. Generally speaking, if a node is closer to the AS, it will be authenticated before the others that are further away. Therefore, before smart meters join the AMI, gateway DAPs and normal DAPs are initialized. Note that gateway DAPs are initialized before normal DAPs since they have direct communication to the concentrator. For simplicity, gateway DAPs are not specified in the rest of the discussion.

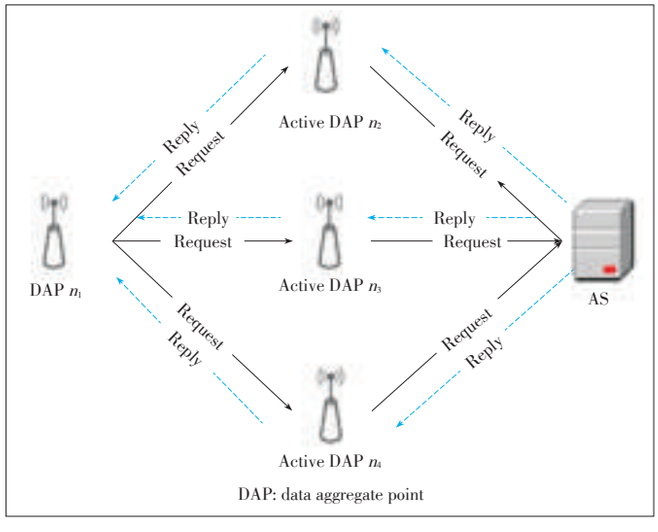
Let the DAPs be divided into two groups, one is active and the other is uninitialized. An active node has been authenticated by the AS to join the AMI communication and is functioning in a healthy status. An uninitialized node can be one of the four types shown in the following:

1) A newly installed node
2) A node which is recovered from malfunctioning status
3) A node which is updated with new pre-shared keys
4) A node which is reinstalled to another location.

For example, if DAP n_1 wants to join the AMI, the initialization process goes through all of its active neighbors (e.g., n_2, n_3 and n_4). As illustrated in **Fig. 3**, n_1 sends requests to all of its active neighbors, which will relay the request to the AS through established secure links. After being authenticated by the AS, n_1 will receive different reply messages from the AS through its active neighbors. Through this initial authentication process, there are mainly three tasks accomplished,

- n_1 is authenticated to be an active node and join the AMI
- n_2 establishes secure connection to the AS through one of its active neighbors which has the shortest distance to the AS
- n_1 establishes backup secure connections to the AS through the rest of its active neighbors.

Without loss of generality, n_2 is chosen to illustrate the detailed initialization process. The processes through n_3 and n_4 are similar. n_1, a secure link between n_2 and the AS, and the AS are involved. Note that the nodes in the secure link do not get useful information from the process. Therefore, we focus on

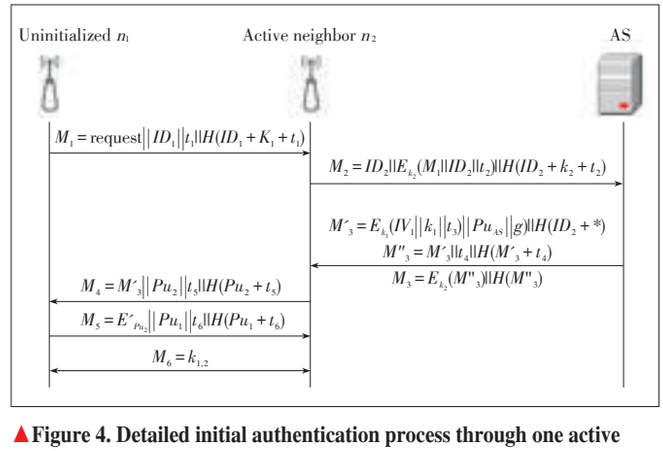


▲Figure 3. Initial authentication process for DAP n_1.

n_1, n_2, and the AS. The initialization process has three mutual authentications. One is between n_1 and the AS, one is between n_2 and the AS, and the other one is between n_1 and n_2. The mutual authentication between n_1 and the AS is obvious since the legitimate nodes are allowed to join the AMI by AS and the nodes also only trust the AS. The mutual authentication between n_2 and the AS is to ensure n_2 is active and is trusted to relay the request from n_1. The mutual authentication between n_1 and n_2 is to help further establish secure communications from n_1 to n_2. Assuming that each node has a pre-shared secret key (i.e., K_i for node n_i) with the AS before initialization. Each active node has been assigned with an active secret key (i.e., K_i for n_i) mainly for uplink data encryption. This active secret key is also used to verify if this node is active or not. Similar to K_2, k_2 is only known to n_2 and the AS. In order to establish a secure connection from n_1 to the AS, an active secret key k_1 must be generated by the AS and assigned to n_1 during the initialization process. Note that n_1 does not bare k_1 before initialization process, only K_1 is known to n_1.

As shown in **Fig. 4**, the whole initialization process involves 6 messages.

1) $M_1 = request||ID_1||t_1||H(ID_1 + K_1 + t_1)$: n_1 sends M_1 to the AS through n_2, where $H(\cdot)$ is a hash function, ' + ' is *XOR* function, and t_1 is a time stamp. The authentication is achieved by K_1 since with given ID_1 and t_1, the AS is the only entity other than n_1 to be able to compute $H(ID_1 + K_1 + t_1)$.
2) $M_2 = ID_2||E_{k_1}(M_1||ID_2||t_2)||H(ID_2 + k_2 + t_2)$: n_2 sends M_2 to the AS, where $E_k(\cdot)$ is a symmetric encryption function with key k. Once n_2 receives M_1, it generates another time stamp t_2 and appends $H(ID_2 + k_2 + t_2)$ to M_1. The extra information is used for the AS to authenticate n_2 as a genuine node and validates the integrity of time stamp. n_2 then encrypts the entire message and appended its own identification with k_2. This is used to protect its identity verification code $H(ID_2 + k_2 + t_2)$ and also let the AS authenticate its a-



▲Figure 4. Detailed initial authentication process through one active neighbor.

ctive status.

3) $M_3 = E_{k_2}(M_3' || H(M_3''))$: Once the AS receives M_2, it authenticates n_2 by decrypting M_2 using k_2. Time stamp t_2 is validated by computing $H(ID_2 + k_2 + t_2)$. The AS then authenticate n_1 by computing $H(ID_1 + K_1)$. Once n_1 is authenticated, the AS generates a message $M_3' = E_{K_1}(IV_1 || k_1 || t_3 || PU_{AS} || g) H(ID_2 + *)$ for n_1. In M_3', IV_1 is the initial vector for further uplink transmission. k_1 is the active key for uplink transmission. Pu_{AS} is the public key of the AS for downlink transmission protocols. Moreover, g is the generating parameter for public key cryptography in the communication domain. It can be a set of parameters depending on chosen public key cryptography schemes. For instance, g stands for two primes numbers if RSA is applied [17], and for more parameters if identity-based cryptography [18]–[20] is applied. Nonetheless, g remains the same in the communication domain. Although the AS generates g, it does not generate public/private keys for each node. It is safer to keep the nodes as independent as possible to other nodes and the AS. Those data for n_1 is encrypted with the pre-shared secret key K_1. Moreover, in M_3', $H(ID_2 + *) = H(ID_2 + IV_s + k_1 + t_3 + PU_{AS} + g)$ is the integrity checksum. Note that ID_2 is also part of the input and thus n_1 is able to authenticate n_2 through the AS. Then, the AS generates another time stamp t_4 (it is possible that $t_4 = t_3$) and $M_3'' = M_3' || t_4 || H(M_3' + t_4)$. Finally, the message sent back to n_2 is $M_3 = E_{k_2}(M_3'' || H(M_3''))$.

4) $M_4 = M_3' || Pu_2 || t_5 || H(Pu_2 + t_5)$: After n_2 receiving M_3, it verifies the message and recovers M_3'. So far, n_2 has authenticated n_1 from the AS, then n_2 relay M_3' to n_1 along with its public key Pu_2. A time stamp t_5 is generated for message freshness. Hash function is applied to $Pu_2 + t_5$ for data integrity.

5) $M_5 = E^*_{Pu_2}(Pu_1) || t_6 || H(Pu_1 + t_6)$: Once n_1 receives M_4, it reveals IV_1, k_1, Pu_{AS} and g. After verifying the integrity of the received information, n_1 computes a pair of public/private keys based on given g. The public key Pu_1 is encrypted with the public key of n_2 s.t. $E^*_{Pu_2}(Pu_1)$, where E^* is the encryption function of the adopted public key cryptograph. A time stamp t_6 is generated and $M_5 = E^*_{Pu2}(Pu_1 || t_6 || H(Pu_1 + t_6)$: is computed to keep the integrity of the message.

6) $M_6 = k_{1,2}$: After exchange public keys, n_1 and n_2 can work out a way to generate a session key $k_{1,2}$ for communication. Session key $k_{1,2}$ is only shared between n_1 and n_2. It is subject to get refreshed frequently.

After exchanging these 6 messages, n_1 is fully initialized and it is able to join uplink communications through n_2. The initial authentication processes through other active neighbors are similar. The AS sends back the same IV_1, k_1, Pu_{AS}, and g. In the final hand-shake, n_1 will send the same Pu_1 to its active neighboring node n_x encrypted with Pu_x. By doing so, n_1 shares the same public key to all of its active neighbors. Therefore, n_1 is able to join the uplink transmission through any of the active neighbors, in other words, both operating and backup secure communication channels are established through the initial authentication process.

When the DAPs are initialized by the AS, the NAN is formed. Smart meters will then be initialized through active DAPs. Unlike DAPs, smart meters do not have many neighbor nodes because of two reasons. First, smart meters have limited transmission range. They are unlikely to have direct connection with more than one DAPs. Second, it is not a good idea to let smart meters communicate with each other since the data contains much privacy and smart meters are easier to get access to than DAPs. A smart meter sends an initialization request to an active DAP, and the DAP will relay the request to the AS through a secure communication link. The detailed process is similar to that shown in Fig. 4 and thus is not repeated.

Security Analysis:

- Confidentiality: Confidentiality of the authentication request is unnecessary, therefore it is not provided. Much information is transmitted in plain text.
- Data integrity: All the messages (except for M_6) are provided a hash value for integrity check. Moreover, the input is not the original message which can be captured easily by an eavesdropper. The input is the XORed messages of the useful information, which cannot be captured or forged. Therefore, the messages in this protocol is unforgettable. Moreover, with time stamps being applied in each message, replay attack is unlikely to succeed in the process. The detailed process of M_6 is not given in this protocol, because the real application may vary based on different public key schemes. With a given public key scheme, data integrity can be provided in a similar way for session key $k_{i,j}$.
- Non-repudiation: The idolization process does not use a digital signature for sender authentication except for M_5. However, secret pre-shared keys are applied for message encryption. With the sender and the receiver being the only ones that can encrypt and decrypt the message, nonrepudiation is achieved for all messages (except for M_5). Non-repudiation of M_5 is indeed provided by a digital signature.

4.2 Security Protocol in Uplink Transmission

In the uplink transmission, data from each node is aggregated in a chain topology and is finally delivered to the service provider (assuming that the AS and the service provider share the same entity). As discussed before, data confidentiality and data integrity are important security requirements for metering data since the wrong data may cause unnecessary loss of the power generation. Sender authentication or non-repudiation may be considered in certain situation if there is enough computational resources. To achieve all those requirements mentioned above, we propose the security protocol for data aggregation in uplink transmission as shown in **Fig. 5**. Suppose in one path there are N nodes with an order of $(n_1, n_2, \cdots, n_N)$. As the

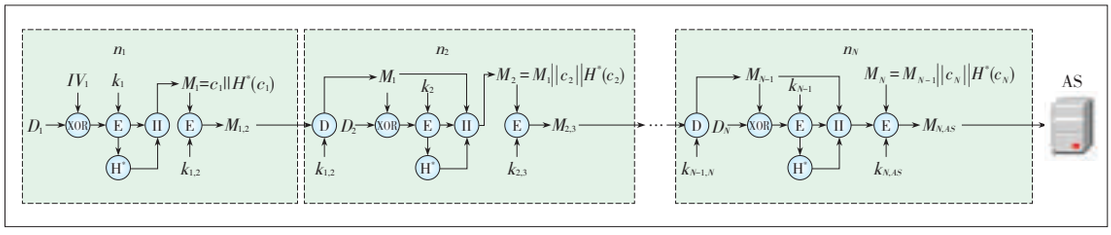


Figure 5.
Data aggregation process in uplink transmission.

first one of the aggregation, n_1 mixes its raw data D_1 with IV_1 and encrypts it with k_1 so that confidentiality can be achieved. $H^*(\cdot)$ is a hashed message authentication code function which provides data integrity. Different hash functions can be used for initialization process and uplink transmission, therefore we use $H^*(\cdot)$ for clearer illustration. Finally, n_1 encrypts the entire message with $k_{1,2}$ so that n_2 can verify that the data is from n_1 which is an active node. The intermediate nodes first decrypt the incoming data with the session key of the previous node. Then, they mix their raw data with the previous data. After that, they follow the same steps as the first node.

If an intermediate node has multiple incoming nodes, it treats each of them as a separate chain and aggregates its own data to one of the incoming data while simply padding the data from the other incoming nodes to it with flags. The details are shown in **Fig. 6**. Assume n_p has two incoming nodes n_i and n_j, and n_p chooses to aggregate incoming data from n_i. Then n_p follows the usual steps dealing with D_p and $M_{i,p}$. For $M_{j,p}$, n_p authenticates the sender by getting M_j, and simply flags M_j such that $f_0||M_j||f_1$ to the original M_p, thus $M_p=f_0||M_j||f_1||C_p||H^*(C_p)$.

Once the AS receives the aggregated data, it starts the recovery process of the data. The AS first authenticates the incoming node by decrypting the receiving data with the pre-shared public key $Pu_{N,AS}$. Before recovering the raw data, the AS needs to verify the data integrity by checking the hashed value. Since the data of each node are not further processed by nodes after it, if some of the data corrupt, the AS will simply discard them instead of wasting the whole message from that transmission path. The detailed raw data recovery process (without integrity check) is shown in **Fig. 7**. Message $M_i=M_{i-1}||C_i||H^*(C_i)$, after verifying the data integrity, the AS decrypts C_i and XOR the result with M_{i-1} to recover D_N. Note that D_1 is recovered by XORing IV_1. If the message includes data from multiple chains, the AS extracts the message between f_0 and f_1 first and recovers the data following the same process as shown in Fig. 7 without verifying the sender authentication (the decryption process with $Pu_{N,AS}$).

Security Analysis:

- Confidentiality: The confidentiality is achieved by two steps in this protocol. For each node n_i, its raw data is mixed with the incoming data from the previous node.
- The first node achieves this step by mixing its data with the initial vector given by the AS. Moreover, mixed data is encrypted with the active key k_i.
- Data integrity: The message cannot be manipulated since message integrity is verified using a hash value. The message of n_i is unforgeable unless an active key k_i is compromised.
- Non-repudiation: On one hand, since each message is encrypted by an active key from the corresponding node, sender authentication is provided. On the other hand, no digital signature is used in the proposed protocol for non-repudia-

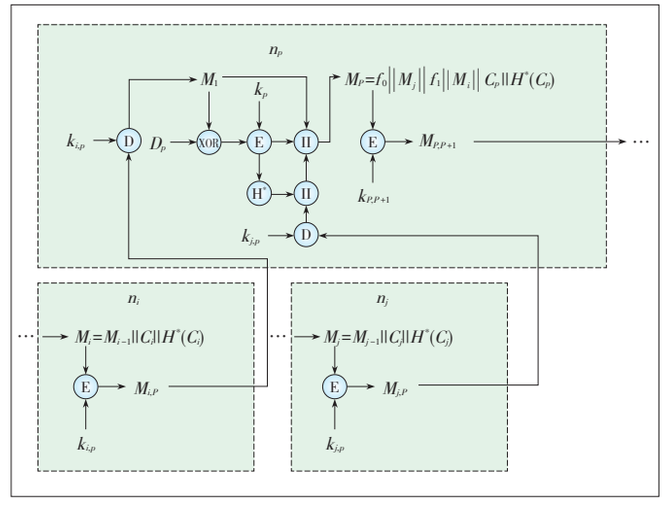


Figure 6. Multi-flow data aggregation process.

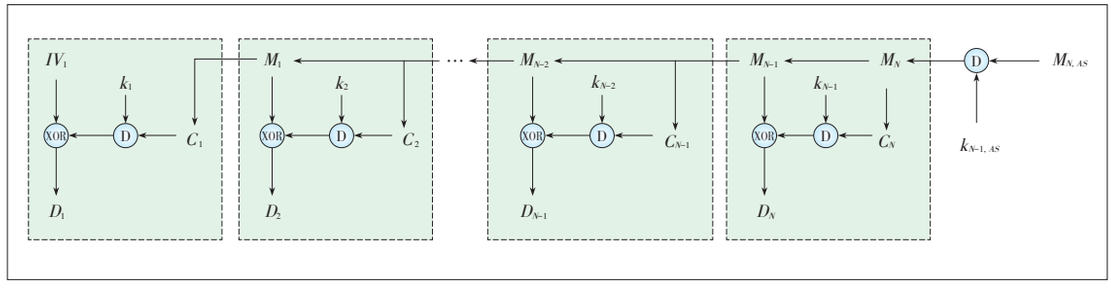


Figure 7.
Data recovery process in uplink transmission.

tion. In fact, if a message is susceptible or invalid, the service provider will simply discard it without wasting resources on it.

4.3 Security Protocol in Downlink Transmission

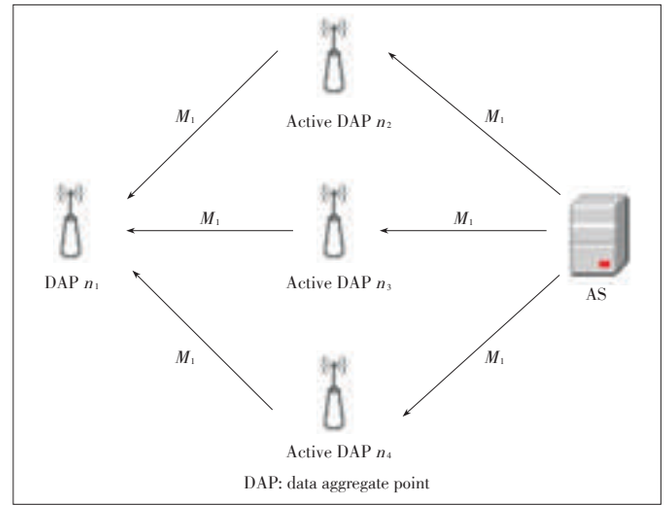
The downlink transmission involves control messages from the service provider to the nodes. Most of the control messages (e.g., price and tariff information) are for all the smart meters in the neighborhood, where the confidentiality is not as important as that of the uplink data. Nonetheless, as discussed before, data integrity is important. Message manipulation will cause further responding in power usage and will finally result in unnecessary fuel waste due to excess power generation. Moreover, non-repudiation is critical for such control messages so that the customers can trust the sender.

Let C_B be the control message to be broadcast. To provide message integrity, a hash value (achieved by hash function $H^*(\cdot)$) is appended to the original message, the entire message is then signed with Pu_{AS} as a digital signature to provide non-repudiation and sender authentication. $E^*_{\Pr_{AS}}(\cdot)$ is an encryption function using public key cryptography, the encryption key is $\Pr_{AS}$. In all, $M_B = E^*_{\Pr_{AS}}\left(C_B \| t \| H^*(C_B + t)\right)$, where t is a time stamp for data freshness. At the receiver side, the original information (i.e., C_B and t) is revealed by performing $D^*_{Pu_{AS}}(M_B)$, where $D^*_{Pu_{AS}}(\cdot)$ is a decryption function using public key cryptography with decryption key Pu_{AS}. An integrity check will be performed to verify both the hash value and the time stamp. If the integrity check is not passed, the receiver will request a retransmission from the AS through its secure uplink transmission tunnel. This rarely happens unless the message is not legitimate. Because each node will receive multiple copies of the control message from all of its active neighbors. If one of the message is valid, then a retransmission will not be necessary.

Some of the control messages (e.g., request for update) are for a specific node (e.g., n_i). Let such control message be C_i. Apparently, message integrity, nonrepudiation and sender authentication shall still be provided, moreover, confidentiality of the message is also important, therefore the message is encrypted with k_i such that $M_i = E^*_{\Pr_{AS}}\left(E_{k_i}\left(C_i \| t \| H^*(C_i + t)\right)\right)$. Unlike M_B, broadcasting M_i is a waste of resource and is unnecessary. However, sending M_i through the corresponding uplink path may reduce the availability of the message. Therefore, we propose to send such specific control message to n_i through all of its active neighbors, as illustrated in **Fig. 8**.

Security Analysis:

- Confidentiality: For downlink broadcasting messages, confidentiality is not provided. For downlink messages to a specific node (e.g., n_i), confidentiality is provided by encrypting the message with the active key k_i.
- Integrity: First of all, both the broadcasting and unicasting control messages are unforgeable since they signed by the AS using its private key. Secondly, any manipulated control messages will be recovered since their hash values cannot pass the data integrity check.
- Non-repudiation: Since each control message is signed by the AS, the control message is non-repudiable.



▲**Figure 8. Example of Control message M_1 to n_1.**

4.4 Domain Secrets Update

In order to keep the AMI secure in the long run, domain secrets need to be refreshed once in a while (e.g., daily or even hourly). For the AS, its public and private key needs to be refreshed. After the AS generates a new pair of public/private keys (i.e., $Pu'_{AS}/\Pr'_{AS}$), it transmits the public key to all the active nodes in a broadcasting way (signed by current private key of the AS), s.t., $M_B = E^*_{\Pr_{AS}}\left(Pu'_{AS} \| t \| H^*(Pu'_{AS} + t)\right)$, where t is a time stamp which keeps the freshness of the message. The update of Pu'_{AS} is for all the active nodes in the same time slot. In the meantime, separate control messages signed by $\Pr_{AS}$ and $\Pr'_{AS}$ will be sent so that the downlink transmission is not interrupted.

For an active node (e.g., n_i), its active secret key k_i needs to be refreshed. To do so, the AS picks a new active secret key k'_i for n_i, and sends $M_i = E^*_{\Pr_{AS}}\left(E_{k_i}\left(k'_i \| t \| H^*(k'_i + t)\right)\right)$ to n_i, where t is a time stamp which keeps the freshness of the message. However, it is not necessary to refresh the active secret keys for all the nodes at the same time. The AS can do a batch at a time when the network is not heavily loaded, for example, after mid night. Moreover, as mentioned before, the session key (e.g., $k_{i,j}$) between two active nodes (i.e., n_i and n_j) needs to be refreshed more frequently. To do so, n_i and n_j simply run the 6-th step from the initialization process again.

The pre-shared key of a node is not refreshed as frequently as the other keys since it is used much less frequently. Therefore, the pre-shared key can last longer before it wears out. However, it is reasonable to refresh the pre-shared key in some

cases. For example, if a DAP is compromised and recovered, or if a DAP is redeployed to another NAN, or if a house has been sold and thus its smart meter has a new owner. An on-site firmware update will be recommended in this case. A customer can also request a firmware update and then load it to his/her smart meter. Automatic update can also be achieved. For example, if DAP n_i needs a pre-shared key update, the AS picks a new $K_i^{'}$, and sends $M_i = E^*_{\mathrm{Pr}_{AS}}\left(E_{k_i}\left(K_i^{'} \| t \| H^*\left(K_i^{'} + t\right)\right)\right)$. It is also reasonable to encrypt this message with K_i if k_i has been compromised. However, if both K_i and k_i are compromised, then a physical update will be inevitable.

5 Conclusions

In this paper, we propose a security protocol for the AMI in smart grid. In order to meet various security requirements for the asymmetric communication of the AMI, the proposed security protocol consists of initial authentication scheme, independent security schemes for uplink and downlink transmissions, and a domain secrete update scheme. The security scheme in uplink scheme provides confidentiality, data integrity to metering data and other monitoring data. The security scheme in downlink provides data integrity and non-repudiation to controlling data and pricing/tariff information. In the future work, we will extend the network security protocol so that cloud computing and various external information sources can be involved in the modern control of smart grid.

References

[1] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012. doi: 10.1109/surv.2012.010912.00035.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 5– 20, 2013. doi: 10.1109/SURV.2012.021312.00034.

[3] F. Ye, Y. Qian, and R. Hu, "Energy efficient self-sustaining wireless neighborhood area network design for smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 220–229, 2015. doi: 10.1109/TSG.2014.2344659.

[4] J. Ma, J. Deng, L. Song, and Z. Han, "Incentive mechanism for demand side management in smart grid using auction," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1379–1388, 2014. doi: 10.1109/TSG.2014.2302915.

[5] H. Soliman and A. Leon-Garcia, "Game-theoretic demand-side management with storage devices for the future smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1475–1485, 2014.

[6] Z. Fadlullah, D. M. Quan, N. Kato, and I. Stojmenovic, "Gtes: An optimized game-theoretic demand-side management scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 588–597, 2014. doi: 10.1109/JSYST.2013.2260934.

[7] F. Ye, Y. Qian, and R. Hu, "A real-time information based demand-side management system in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, no. 99, pp. 1, 2015.

[8] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Peace: A novel privacy enhanced yet accountable security framework for metropolitan wireless mesh networks," *IEEE Transactions on* Parallel and Distributed Systems, vol. 21, no. 2, pp. 203–215, 2010.

[9] E. Witzke, J. Brenkosh, K. Green, L. Riblett, and J. Wiseman, "Encryption in mobile wireless mesh networks," in *2012 IEEE International Carnahan Conference on* Security Technology (ICCST), Boston, Massachusetts, USA, 2012, pp. 251–256.

[10] M. Thomas, I. Ali, and N. Gupta, "A secure way of exchanging the secret keys in advanced metering infrastructure," in *2012 IEEE International Conference on Power System Technology (POWERCON)*, Auckland, New Zealand, Oct 2012, pp. 1–7.

[11] B. Vaidya, D. Makrakis, and H. Mouftah, "Secure multipath routing for ami network in smart grid," in *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)*, Austin, USA, Dec 2012, pp. 408–415.

[12] Y. Yan, R. Hu, S. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Network*, vol. 27, no. 4, pp. 64–71, 2013. doi: 10.1109/MNET.2013.6574667.

[13] F. Ye, Y. Qian, and R. Hu, "A security protocol for advanced metering infrastructure in smart grid," in *2014 IEEE Global Communications Conference (GLOBECOM)*, Austin, USA, Dec 2014, pp. 649–654.

[14] G. Rajalingham, Q.-D. Ho, and T. Le-Ngoc, "Attainable throughput, delay and scalability for geographic routing on smart grid neighbor area networks," in *Wireless Communications and Networking Conference (WCNC 2013)*, Shanghai, China, 2013, pp. 1121–1126.

[15] *Communication Networks and Systems in Substations–Part 5: Communication Requirements for Functions and Device Models*, P-IEC 61850-5ed1.0, 2003.

[16] *FCC Rules for Unlicensed Wireless Equipment operating in the ISM Bands* [Online]. Available: http://www.afar.net/tutorials/fcc-rules

[17] S. Burnett and S. Paine, *The RSA Security's Official Guide to Cryptography*, McGraw-Hill, Inc., 2001.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[19] B. Libert and J. -J. Quisquater, "The exact security of an identity based signature and its applications," *IACR Cryptology ePrint Archive*, vol. 2004, pp. 102–104, 2004.

[20] F. Ye, Y. Qian, and R. Q. Hu. *Hibass: hierarchical identity-based signature scheme for ami downlink transmission* [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/sec.1217/abstract

Manuscript received: 2015-04-21

Biographies

Feng Ye received his BS degree from the Department of Electronics Engineering, Shanghai Jiaotong University, Shanghai, China, in 2011. Currently he is pursuing his PhD degree at the Department of Electrical and Computer Engineering in University of Nebraska-Lincoln, NE, USA. His current research interests include smart grid communications and energy optimization, big data analytics and applications, cyber security and communication network security, wireless communications and networks.

Yi Qian (yi.qian@unl.edu) received his PhD degree in electrical engineering from Clemson University. He is an associate professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln (UNL). Before joining UNL, he worked in the telecommunications industry, academia, and the government. His research interests include information assurance and network security, computer networks, mobile wireless ad-hoc and sensor networks, wireless and multimedia communications and networks, and smart grid communications. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Digital Library.

DOI: 10.3969/j.issn.1673-5188.2015.03.004
http://www.cnki.net/kcms/detail/34.1294.TN.20150916.1553.002.html, published online September 16, 2015

Reliable Remote Relay Protection in Smart Grid

Jiapeng Zhang and Yingfei Dong
(Department of Electrical Engineering University of Hawaii, Honolulu, HI 96822, USA)

Abstract

As the false trips of remote protection relays are among the main reasons behind cascading blackouts, it is critical to design reliable relay protection. Even though common protection schemes on traditional power systems have been investigated for a few decades, cascading failures in recent years indicate more research needed in this area. Consequently, researchers have proposed agent-based methods on the Smart Grid (SG) to address this issue. However, these existing agent-based methods simply use TCP protocol without considering real-time communication requirements (such as bandwidth and delay). To deal with this issue, several methods for efficient network resource management are proposed. Furthermore, these existing methods do not consider the potential issues in practical communication networks, which may result in delay violation and trigger relay false trips. We have discussed simple backup solutions in the previous work. In this paper, in addition to network efficiency, we focus on improving the system reliability by exploring known power system information and minimizing the chances of false trips of important remote relays, e.g., defining power line priorities based on their importance. Moreover, to further improve the system reliability, we also investigate the peer-to-peer protection approaches to address the single point of failure of centralized control center.

Keywords

zone 3 relay; cascading failure; real-time communications; smart grid protection; power-aware resource management

1 Introduction

To deal with device failures, prevent damages to power sys-tem components, and avoid broad-spread disturbances, modern power transmission systems use different types of local and remote relays to isolate such issues and stop disturbances from spreading. In the protection system, directional relays (especially remote zone 3 relays) are critical in protecting transmission lines as backup protection, and they are universally deployed in protection systems [1], [2]. However, some over-sensitive remote relays may trip due to various reasons and generated cascading failures in recent large scale blackouts [3], [4]. While researchers have developed many methods to prevent such failures on the traditional power systems [5]–[7], these existing methods failed to solve the problem and could not stop the spread of cascading failures due to the false trips of remote relays. We will focus on this critical issue in this paper.

In the emerging Smart Grid (SG), many intelligent devices are employed to monitor and control power system components, which allow us to achieve more effective protection for dealing with the false trips of remote relays. These de-vices communicate with power control systems on real-time networks, provide instant system status, and conduct precise control. In this research direction, agent-based protection systems [8], [9] have been designed to utilize SG real-time communications to prevent the false trips of remote relays. However, the existing methods simply use TCP/UDP transport protocols to deliver monitor and control messages without band-width and delay guarantees, and simply assumed ideal dedicated communication network paths; they did not address practical network issues due to many potential errors such as simple traffic congestion, routers/links errors/misconfigurations, or malicious attacks that cause bandwidth and delay violation on communication paths. Meanwhile, more and more SG applications and services are being developed for reliability, efficiency, and system protection [10]–[13]. Many of these applications require high bandwidth and short latency (e.g., emerging PMU operations [12]), and may cause temporary congestion (e.g., in a diagnostic mode). Therefore, we cannot simply assume a dedicated network for each application and have to carefully manage real-time communication network resources to support the operations of these applications.

The previously-proposed agent-based schemes assume ideal dedicated network paths between protection relays and their master agent for real-time monitoring and control [8], [9], without considering the details of network resource management and potential link errors. To fill this gap, our previous work focused on methods for basic network resource management for ensuring bandwidth and delay guarantees. We also designed a

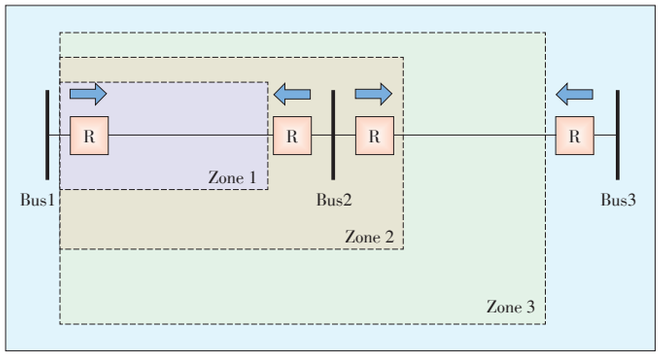
simple backup method presented in [14].

In this paper, in addition to address network management, we focus on system reliability, because the reliability of power system become extremely critical and today's information-focused world is highly dependent on the availability of power systems. To enhance the system reliability of agent-based solutions, we will first introduce a master-based static reservation scheme for delay and bandwidth guarantees, and then discuss different backup methods to address potential communication errors in practical networks. We further propose a power-ware protection approach by exploiting known information about power systems in order to define power line priorities based on their importance. Furthermore, as the master-based solution is highly dependent on the availability of the master agent, to address this issue, we further present a Peer-to-Peer (P2P) based scheme as an alternative to the master-based scheme to address the single point of failure of centralized control center. Although the path failures are low probability events, when they occur, they do cause serious issues in remote relay protection schemes and damage the entire power system. The proposed ideas in this paper are not limited to only relay protections and can be employed for many other real-time control and monitoring systems.

We organize the remainder of this paper as follows. In Section 2, we will discuss related work. In Section 3, we will present the enhanced primary path construction method, different backup methods, and the proposed power-ware scheme. In Section 4, we will focus on the proposed P2P-based scheme. In Section 5, we will evaluate the proposed solutions and discuss their pros and cons. In Section 6, we will summarize this work and elaborate our future research in this direction.

2 Related Work

Distance protection relays are one of the most common relays used for power transmission lines [1]. The operation of a distance relay is determined by the impedance measured by the relay, which is used to estimate the distance from the relay to a fault. We usually have three protection zones as shown in **Fig. 1** [9]. Protection zone 1 is the basic protection of a distance relay, which covers about 80% of the length of a transmission line. The protection zone 2 covers a little more than zone 1, usually about 120% of the length of a transmission line. Protection zone 3 covers the first transmission line and also about 80% of the second line. We can adjust the relay settings for zone 1, zone 2, and zone 3 protection, and construct both primary protection and backup protection with different delays. Normally, we use zone 1 as the primary protection, which is almost immediately triggered when a fault is detected, e.g., with a delay of a few milliseconds. We use zone 2 and zone 3 protection as backup mechanisms, which are triggered after given tripping delays when a fault is detected. These tripping delays are often determined by the protection distance, e.g., a zone 2 protection may waits for 0.3 second, and a zone 3 protection may wait up to 1 second [8], [9].



▲**Figure 1. Distance protection relays: zone 1, zone 2, and zone 3.**

Hidden failures have been considered one of the main sources of large scale disturbances [3], [5], [15]. A hidden failure occurs when incorrect system states or control actions are triggered by another system event. It may induce widespread cascading failures such as the Northeastern blackout in 2003, which is initialized by a false relay trip [16]. Although solutions to hidden failures on traditional power systems have been extensively investigated [4], [7], [9], it is still extremely challenging to completely prevent such failures on large-scale complicated power systems.

The false trips of zone 3 relays are often associated with hidden failures [7], as shown in the past events. Such false trips have been identified among the main causes of blackouts (about 70% [3], [6]). In the meantime, zone 3 protection is also considered essential to power systems and we really rely on such protection in many cases [1], [2]. To deal with such false trips, new agent-based solutions have been proposed by utilizing smart grid communication networks [8], [9].

SG is in rapid development due to its salient features such as improving efficiency and reliability, better utilizing renewable energy, etc [10], [11], [17]–[19]. One key difference between the SG and the traditional power systems is that SG enables two-way power transmission with intelligent devices that exploit the rapid increase of computing power and the ubiquitous network communication systems. Many SG technologies have developed and many more new SG applications are still in development, e.g., Phasor Measurement Unit (PMU) technology [12].

Agent-based protection methods use a query-response model to avoid zone 3 false trips. A software agent is deployed at each relay. When a zone 3 relay r detects a remote disturbance from a line l, it will send a query to a master agent (MA) to verify if such a disturbance has been seen by other relays associated with the same transmission line. The MA then queries all related relays to pull their readings. After the MA receives all responses from these relays, it can determine if the disturbance on line l is a real fault or simply a temporary error. The MA sends a response to relay r to tell it how to react. Ideally, such

a solution can eliminate all over-sensitive tripping of zone 3 relays, assuming that there is only one transmission line error in the system and the query-response process can be completed before relay r is tripped based on its setting. However, the network delay requirement may be violated in real networks. Therefore, we have to consider practical network issues to further improve the reliability of zone 3 protection.

As we focus on the issues on SG communication network, the proposed solution in the following section will also help many other real-time SG applications depending on the same communication network.

3 Proposed Power-Aware Reliable Scheme

In this section, before we discuss the power-aware approach, we will first present an improved two-step network resource management scheme to ensure the message can be exchanged between a relay and its MA in time. We will first introduce the enhanced primary path construction in section 3.1, and present different backup methods in section 3.2 to further improve the communication reliability, in the case that the primary path fails due to unexpected network errors. Then, we will present a power-aware resource management frame-work to improve system reliability and resource management efficiency.

3.1 Enhanced Primary Path Selection with Reliability

To ensure a message is delivered on time between a MA and a relay, we first need deal with network delays for the agent-based protection scheme. Assume the MA is placed on a network topology based on certain criteria (which are out of scope of this paper). Our first task is to build a path for each remote protection relay to communicate with the MA. We name such a path as a Primary Path, and assume no links on this path fails. In our previous work, we proposed to use a shortest path based on the network topology as a primary path [14], which is more efficient in bandwidth use. In this paper, we further improve this process using the most reliable path, which emphasizes the path reliability. The shortest-path method minimizes the distance of a relay/bus to the MA so that a packet may have less resource requirement on each communication link; the most-reliable-path method minimizes the failure probability of a primary path by considering the reliability of its links.

Note that each bus may be associated with multiple relays. In general, only one relay at the bus will experience disturbances at a time and need to contact with the MA for guidance. So we usually only need one path from a bus to the MA.

As a single link failure is one of the most common cases in a network, the failure probability of a primary path is defined as:

$$P_f(path_i) = \sum_{j \in path_i} \left[P_f(link_j) \cdot \prod_{n \notin j} (1 - P_f(link_n)) \right] \quad (1)$$

where $path_i$ is a primary path from bus i to the MA, and $P_f(link_n)$ is the failure probability of link n. The enhanced primary path selection process is shown in **Algorithm 1**.

Algorithm 1 Primary path selection algorithm for buses

Input: Bus Set B, MA info, and Link Set L_e.
Output: A primary path for each bus.
Method:
1: **for** each bus $u_i \in B$ **do**
2: Find all path set P_{pr} from u_i to the MA
3: For each path in P_{pr}, assign its weight based on its path length (or path failure probability)
4: Select the path $path_{pr}(u_i)$ with the minimum weight as the primary path for u_i
5: **end for**

After finding a primary path for a remote relay, we need to determine its path delay requirement. The agent-based method has four main steps introducing delays: 1) A query is sent from a remote relay r to the MA, when it sees a temporary issue (e.g., a voltage surge or an impedance drop); 2) After the MA receives the query from r, the MA queries other related relays, where Rl is the set of relays $\{ r' : r' \in R_l \text{ and } r' \neq r \}$, where R_l is the set of relays protecting the same power line; 3) A response is sent from each r' to the MA; 4) the MA makes a decision based on the responses and sends its decision to r. The maximum allowable delay for a remote relay between sending a query and receiving a decision from MA can not exceed a given amount [8], [9]; otherwise, the relay will automatically trip a power line.

We determine the path delay requirement from a relay to the MA based on the following procedure. Denote the set of power transmission lines as L_p. For a power line $l \in L_p$, we find two relays r_1 and r_2 in R_l, which have the largest and the second-largest hop count h_{r1} and h_{r2} to the MA, respectively. The delay requirement of a remote relay is initialized to a default value D_0. (For ease of illustration, we assume that all remote relays have the same delay requirement. In real systems, the requirement of each relay may be different; we can represent them as $D_0(r_i)$ for relay r_i.) To ensure the delay requirement in the remote protection procedure, we proportionally divide the total delay requirement between these two relays: in case that one is the remote relay starting the query process and another is among the relays that respond to the MA. That is, the delay requirement between r_1 and the MA is set to $d_1 = h_{r1} \cdot D_0 / 2(h_{r1} + h_{r2})$; the $d$elay requirement between r_2 and the MA is set to $d_2 = h_{r2} \cdot D_0 / 2(h_{r1} + h_{r2})$. For other remote relays of l, their round trip delay requirements are set as no larger than d_2, because their path lengths to the MA are equal or smaller than the length from r_2 to the MA. There is no need to make the other relays to respond faster than r_1 and r_2. (As a relay may be used to protect multiple different lines, it may have different settings. In general, we use the minimal setting of a relay as its preset delay for remote protection.) The delay requirement of a relay is then equally divided along links of its

primary path and we then reserve resources on each link, as shown in **Algorithm 2**.

Algorithm 2 Primary path bandwidth reservation algorithm

Input: Remote Relay Set R, their Delay Assignment D_0 and Relay Inquiry Packet Size L_0.
Output: Primary Path Reservations on Link Set L_c.
Method:
1: **for** each relay $r \in R$ **do**
2: Equally divide its delay requirement $D_0(r)$ to links on its primary path $path_{pr}(r)$, i.e., assign delay on link i as $d(i)$
3: **for** each network link $l \in path_{pr}(r)$ **do**
4: Current reservation on link l is $b_{rsv}(l)$
5: Required capacity by r at l is $C_{pr}(l,r) = L_0/d(l)$
6: **if** $b_{rsv}(l) + C_{pr}(l,r) \leqslant C(l)$, where $C(l)$ is the total capacity of l **then**,
7: $b_{rsv}(l) = b_{rsv}(l) + C_{pr}(l,r)$;
8: **end if**
9: **end for**
10: **end for**

3.2 Enhancing Backup Path for More Reliability

Without network link failures, a primary path is able to handle the query process. However, in practical networks, links may fail. We need to deal with such failures for remote relay protection. As a single link failure is the most common case, we can handle it by using a backup path that is completely not overlapping with the primary path. However, there are several limitations in this scheme: 1) the network topology may not have another path that is a completely not overlapping with the primary path of some buses. 2) the length of a non-overlap backup path is often relatively long: for a fixed path delay, a longer path means a short delay and more bandwidth use at each link on the path, which is inefficient and may create unnecessary hot spots in the network. 3) a link on a non-overlap backup paths may not have enough capacity to support the backup requirement.

The first and the second limitation can only be fixed by changing network topology, which is out of scope of this paper. Here we focus on the third limitation and we propose to utilize power system information to select backup paths and manage resources more effectively. Assume we have historical data about a power network. Therefore, we know which power line carries more load and how likely it may fail, and we can assign a priority to each power line. Using such information, we can then decide how to allocate the limited network resources to maximize the system reliability. In this paper, we do not have such information available. We then use PowerWorld Simulator to generate such information as presented in the evaluation section.

Based on such known information of power systems, we use $P_f(S|line_i)$ to denote the probability that tripping a power line leads to a system failure in simulation. As such data give us the importance of power lines, we can prioritize them in protection. Assume there are N_l lines that may result in system failures. We equally divide the total system requirement P_f^S to these N_l lines. In this way, we expect the probability $P_f(S \bigcap line_i)$ does not exceed P_f^S/N_l for each of them. From (2)

$$P_f(S \bigcap line_i) = P_f(S|line_i) \cdot P_f(line_i) \tag{2}$$

we have:

$$P_f(line_i) = \frac{P_f(S \bigcap line_i)}{P_f(S|line_i)} \tag{3}$$

Consider that the failure of a line is usually due to the false trip of a relay at one of the two ends of the line. Then we can equally divide the requirement of $P_f(line_i)$ to the relays at two ends of the line. For a remote protection relay, when it sees a temporary issue, it sends an query to the MA and waits for the MA's response. If the query cannot reach the MA or the decision from the MA cannot be received by the relay within the required time, a false trip may happen. This case occurs if both a primary path and its backup path of a relay fail at the same time. Under the single link failure assumption, this only happens if the failed link is used by both path. We can define the probability as:

$$P^{relay\ false\ trip} = P_f^{the\ overlap\ links} = \sum_{j \in N_{ol}} [P_f(link_j) \cdot \prod_{n \neq j} (1 - P_f(link_n))] \tag{4}$$

where N_{ol} is the set of overlap links between the primary and backup path of the relay. Thus our goal is to find a backup path that has $P_f^{the\ overlap\ links}$ and can meet the minimum requirement of $P^{relay\ false\ trip}$. (Similar to finding a primary path, we find a backup path for a bus, instead for its relays.) The backup path selection procedure is presented in **Algorithm 3**. After a backup path is selected, resources are also reserved on the path, as shown in **Algorithm 4**. In case that a link does not have enough capacity to support all backup paths on it, the reservations are carried out with a specified order. For power

Algorithm 3 Backup path selection algorithm for buses

Input: Bus Set B and Communications Link Set L_c.
Output: Backup path for each bus.
Method:
1: **for** each bus $u_i \in B$ **do**
2: Find the smallest false trip probability $P_{\min}^{relay\ false\ trip}$ for relays on u_i
3: Calculate the minimum required failure probability for a backup path of u_i as:
4: **if** u_i does not have critical relays **then**
5: Set $P_{f,req}(u_i) = 1$
6: **else**

7: $P_{f,req}(u_i) = P_{\min}^{relay\ false\ trip}$
8: **end if**
9: Find all backup paths set P_{bp} to MA that are different from the primary path
10: Sort paths in P_{bp} based on hop count in an ascending order
11: Start from the first path in P_{bp}
12: **for** each backup path $p \in P_{bp}$ **do**
13: Compute the overlap link set N_{ol} between u_i 's primary path and p, then Calculate $P_f^{the\ overlap\ links}$
14: **if** $P_f^{the\ overlap\ links} \leqslant P_{f,req}(u_i)$ **then**
15: Select path p as the backup path
16: **end if**
17: **end for**
18: **end for**

Algorithm 4 Backup path bandwidth reservation algorithm for remote protection relays

Input: Zone-3 Relay Set R, their Delay Assignment D and Relay Inquiry Packet Size L_0.
Output: Backup path bandwidth reservations on Link Set L_e.
Method:
1: For each relay $r \in R$, find the powerline l_p it is located on and assign the probability $P_f(system|l_p)$ as the weight of relay r
2: Sort the set R using the weight assigned in the above step In a descending order
3: Start from the first relay in R
4: **for** each relay $r \in R$ **do**
5: Devide its delay requirement D on each link of its backup path $P_{bp}(r)$, for link i, its assigned delay is $d(i)$
6: **for** each network link $l \in P_{bp}(r)$ **do**
7: Current reservation on l is $b_{rsv}(l)$, total capacity of l is $C(l)$
8: Required capacity by relay r at link l is $C_{bp}(l,r) = L_0/d(l)$
9: **if** l is also used in the primary path of relay r **then**
10: Reservation of primary path on l is $C_{pr}(l,r)$
11: **if** $C_{pr}(l,r) \leqslant C_{bp}(l,r)$ **then**
12: $C_{bp}(l,r) = C_{bp}(l,r) - C_{pr}(l,r)$
13: **else**
14: $C_{bp}(l,r) = 0$
15: **end if**
16: **end if**
17: **if** $b_{rsv}(l) + C_{bp}(l,r) \leqslant C(l)$ **then**
18: $b_{rsv}(l) = b_{rsv}(l) + C_{bp}(l,r)$;
19: **end if**
20: **end for**
21: **end for**

lines that may blackout the system, their remote relays are "critical" and will be first considered. If a line is not expected to crash the system, we consider the consequence of tripping this line less important. The goal is to ensure that we can fulfill "critical" relays' requirement as much as possible.

Usually a bus contains more than one remote protection relays. We observe that many of the relays are used to protect different power lines. From this observation, we notice that it is possible to further reduce the required network resources, and we will discuss this issue in the evaluation section.

4 Peer-to-Peer (P2P) Protection Scheme for More Reliability

4.1 Motivation: MA is a Single Point of Failure

In the master-based relay protection, the MA receives a query from a substation relay and makes a decision based on system states whether the relay should trip or not, and then sends the decision back to the inquiry relay. Under normal network conditions, this mechanism works properly. However, as the MA is the only node responsible for making decisions, if it is shut down due to cyber-attacks or physical damages, the entire power system will lose the centralized protection, and relays may trip and cause unforeseen instability in the system.

As modern relays are powerful devices, we propose to use a P2P mechanism to deal with the potential unavailability of MA. The key observation is that a relay usually only need to check with a small group of related relays to protect a line. In this scheme, a relay at a substation communicates with other related relays about the state of local and remote power lines. With these responses, the relay can make a justified decision by itself whether to trip or not. An obvious advantage of this scheme is that the average response delay is much shorter than the master-based scheme, because a relay usually only asks other relays nearby, much closer than the MA. (This advantage may be elaborated when a relay need to make a very quick decision for special cases, even when the MA is still available.)

4.2 Proposed P2P Protection Procedure

Identify related relays and form a peer group. For each transmission line, we need first identify the set of related primary and remote relays for a power line and form a relay peer group for the line, shown in **Algorithm 5**.

Algorithm 5 Identify relay protection set for power lines

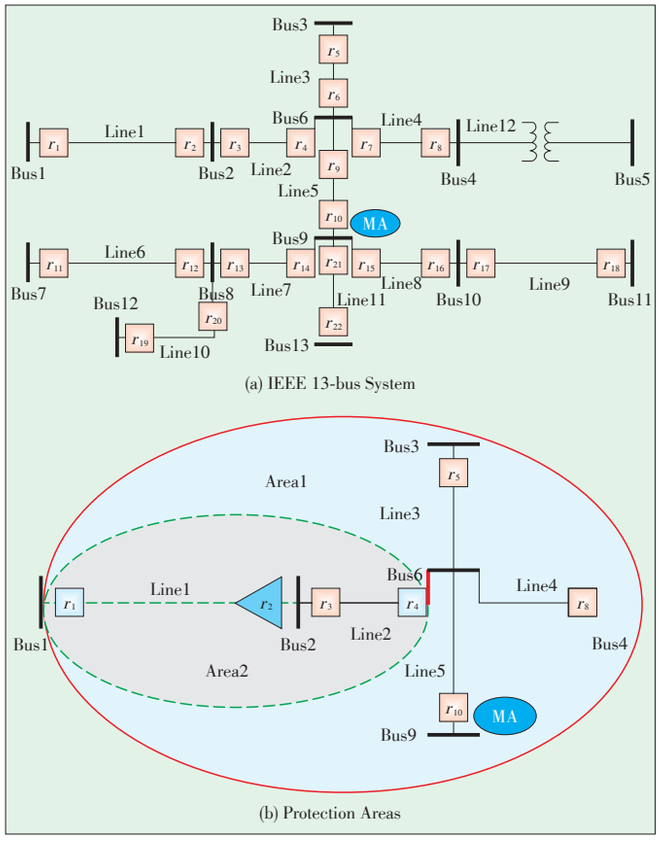
Input: Bus Set B, Power Line Set L_p and Relay Set R.
Output: Protection relays for each power line.
Method:
1: For each relay $r \in R$, we know which bus it is located and which line it serves as primary relay
2: **for** each power line $l_n \in L_p$ **do**

3: Assume the two buses at each end of l_n are u and v
4: For two relays r_u, r_v located at u, v and protect l_n, they are the primary relays of l_n
5: Identify all buses X that directly connected to u or v, while $u \notin X$ and $v \notin X$
6: **for** each bus $x' \notin X$ **do**
7: Denote the power line between (x', u) or (x',v) as l'_n
8: Identify the relay r_b that is located at x' and protects l'_n as primary relay, then r_b is the remote backup relay for line l_n
9: **end for**
10: **end for**

We give an example in **Fig. 2**, for $Line_2$, r_3 and r_4 are the primary relays and (r_1, r_5, r_8, r_{10}) are the remote protection relays. If any remote relay of this set sees a disturbance, it will check with one or more other relays within this set.

When the inquiry relay receives replies from other peers, it uses a voting scheme to decide the action.

For example, if relays with positive confirmations outnumber relays that do not see the fault, the inquiry relay will assume that there is a "real-fault" in the transmission line, and will trip the line when its primary relay fails to do so; otherwise, it assume no fault.



▲**Figure 2. The power system can be divided into different protection areas with the corresponding sets of relays.**

The primary path selection and resource reservation on each link of a path is shown in **Algorithm 6**. We have the following assumptions here. 1) A relay will communicate with all other related peers. 2) At one moment, there is only one hidden failure exposed [9], e.g., one relay has abnormal reading. Moreover, if there is only one hidden failure in the system, a single response from a peer is sufficient to make the decision. 3) At this step, the effect of link failure to the protection is not considered; and we will discuss backup schemes in the following. With the proposed P2P scheme, even if the master agent is shutdown unexpectedly, relays in the system are still able to make correct decisions to prevent the false trips of power lines.

Algorithm 6 Primary path selection and bandwidth reservation algorithm for P2P scheme

Input: Relay Zone 3 Delay Assignment D_0, Power Line Set L_p and Communications Link Set L_C.
Output: Bandwidth Reservations on Links L_C.
Method:
1: For each communication link $l \in L_c$, initialize reservation $b_{rsv}(l)$ to 0
2: **for** each power line $l_n \in L_P$ **do**
3: Find all zone-3 remote backup protection relays R_b and primary protection relays R_p
4: **for** each relay $r_i \in R_b$ **do**
5: **for** each relay $r_j \in (R_b \bigcap R_p)$ and $r_i \neq r_j$ **do**
6: **if** path is not set between r_i and r_j **then**
7: Find a shortest hop count path p from r_i to r_j, which is different from the primary path
8: Assume path p has H hops, then on each link l of p, the reservation of r_i is $Crsv(r_i,l) = \frac{L_0}{D_0/H}$ ▷ L_0 is the packet size
9: **for** each link $l \in p$ **do**
10: $C(l)$ is capacity of l
11: **if** $b_{rsv}(l) + C_{rsv}(r_i,l) \leq C(l)$ **then**
12: $b_{rsv}(l) = b_{rsv}(l) + C_{rsv}(r_i,l)$
13: **end if**
14: **end for**
15: **end if**
16: **end for**
17: **end for**
18: **end for**

In the P2P scheme, we have two types of delays: 1) the (maximum) delay to send a query to other related relays, and 2) the (maximum) delay for other relays to send their responses back to the inquiry relay. The round trip delay should not exceed a pre-defined time period D_0 to avoid false trips. To make sure the decision can be made within the required time period D_0,

we need to reserve network resources for a path from a relay to another relay. The relay delay requirement to and from a peer relay can be set to $D_0/2$. Assume the path consists of H hops and each inquiry has size L_0, the required resource on each link is $L_0/((D_0/2)/H)$.

As in the master-based scheme, the P2P scheme can also use backup paths to deal with communication link failures. Unlike the master-based scheme where the reservation is required between each bus and the master agent, in the P2P scheme, we can reduce the network usage by answering the following questions: 1) Does the P2P scheme need to backup for all of its primary paths between relays? 2) For the backup path used in the P2P scheme, whether to use overlapped or non-overlapped paths? For the first question, we consider that a minimum of two replies may be enough for the inquiry relay to make a majority decision, given the fact that two relays have hidden failures simultaneously is very low [9]. In addition, in [20], it is considered that, if the system is not in a "stressed state", which means the system is not close to unstable operational condition, a relay can even make decision without the responses from other relays. For the second question, due to the specific topology of a system, non-overlap paths can be much longer than the normal paths, especially for the P2P scheme in which primary paths are mostly just a few hops. As an alternative, overlapping backup paths may be used if we can still meet the system requirement. The advantage is obvious: overlapping paths are shorter, thus consume less network resources at each link. The backup path selection process and the resource reservation process are shown in **Algorithm 7** and **Algorithm 8**. Note that since some relays are protecting multiple lines, for example, r_i and r_j protect $line_k$ and $line_l$ simultaneously, then they can both be used as a backup protection relay pair for the two lines. In this way, when we protect $line_k$ with r_i and r_j, we only need to find one additional backup path for protecting linel, which save resources instead of using two different backup paths.

Algorithm 7 Backup path selection algorithm for P2P scheme

Input: Power Line Set L_p, Communication Link Set L_c and required backup path number N_u.
Output: Backup path between a relay and its peer relays.
Method:

Initially there is no backup path for any relay in the system
for each power line $l_n \in L_p$ **do**
  Find all zone-3 remote backup protection relays R_b and primary protection relays R_p
  For each relay, set the number of required backup peers as $N' = N_u$ ▷ For each relay, we hope it has backup paths to N_u peers
  for each relay $r_i \in R_b$ **do**
    Denote peer relays of r_i as $R'_i = (R_b \cap R_p) \not\ni r_i$
    Denote the current backup peers of r_i, whose backup paths already found, as R_x, its size is N_x
    if $N_x \geqslant N_u$ **then**
      Continue to next relay in R_b
    else
      We still need to find $N'_i = N_u - N_x$ number of backup peers
    end if
    for relay r_j in R_x **do**
      Exclude r_j from R'_i ▷ We already have backup path to r_j
    end for
    Find N'_i number of peers from R'_i, which have the shortest hop count paths as the backup peers of r_i ▷ The paths between each of the found relay and r_i should be different from their primary paths, they can have overlapped links with the primary paths or be totally non-overlapped
  end for
end for

Algorithm 8 Backup path bandwidth reservation algorithm for P2P scheme

Input: Relay Zone 3 Delay Assignment D_o, Power Line Set L_p, Communication Link Set L_c.
Output: Backup path reservation for each relay and its backup peers.
Method:

For each communication link $l \in L_c$, its reservation is $b_{rsv}(l)$
for each power $l_n \in L_p$ **do**
  Find all zone-3 remote backup protection relays R_b and primary protection relays R_p
  for each relay $r_i \in R_b$ **do**
    for each relay $r_j \in (R_b \cap R_p)$ and $r_i \neq r_j$ **do**
      if r_j is not a backup peer of r_i OR path between r_j and r_i is already reserved **then**
        Continue to next relay
      end if
      Denote the path from r_i to r_i as *path*
      Assume *path* has H hops, then on each link l of path, the reservation of r_i is $C_{bp,rsv}(r_i,l) = \frac{L_o}{D_o/H}$ ▷ L_o is the packet size
      for each link $l \in path$ **do**
        $C(l)$ is capacity of l
        if l is also used in the primary path of r_i and r_j **then**
          The primary path reservation on l is $C_{pr,rsv}(r_i,l)$
          $C_{bp,rsv}(r_i,l) = \max(C_{bp}, rsv(r_i,l)) -$

$C_{bp,rsv}(r_i,l),0)$
16: **end if**
17: **if** $b_{rsv}(l)+C_{bp,rsv}(r_i,l)\leqslant C(l)$ **then**
18: $b_{rsv}(l)=brsv(l)+C_{bp,rsv}(r_i,l)$
19: **end if**
20: **end for**
21: **end for**
22: **end for**
23: **end for**

We can compute the failure probability of a power system, $P_f(S)$, as shown in (5) to (7). We assume that the false trips of one critical line will result in a system failure, and there are different critical lines under different system load states. The total failure probability of the system is the sum of probability {*system fails and line$_i$ fails*}. Then, based on the known historical information of a power system, we use $P_f(S|line_i)$ to denote the conditional probability that tripping a power line leads to a system failure in simulation. With the above data given, the $P_f(S\cap line_i)$ will be determined by the probability that a power line is falsely tripped, denoted as $P_f(line_i)$. As we have mentioned before, the malfunction of zone 3 remote relay is a common reason for false trips. With the deployment of agent-based protection, under normal conditions, we can deal with such potential malfunctions. However, the failure still exists if either of the primary relays on a power line cannot obtain correct responses from the MA or other peers. Thus, the probability directly relates to the false trip probability of a relay, $P^{relay\ false\ trip}$, as in (7), where $relay_{i,1}$ and $relay_{i,2}$ are the two relays at each end of $line_i$ (assume each time only one relay is exposed to a hidden failure). We will see that different primary and backup paths selection will affect the false trip probability of a relay as shown in the evaluation section.

$$P_f(S)=\sum_{line_i\in S}P_f(S\cap line_i) \tag{5}$$

$$P_f(S\cap line_i)=P_f(S|line_i)\cdot P_f(line_i) \tag{6}$$

$$P_f(line_i)=P^{relay_i,1\ false\ trip}+P^{relay_i,2\ false\ trip} \tag{7}$$

5 Performance Evaluation

5.1 Evaluation System Setting

We evaluate the proposed schemes on the IEEE 39-bus system [9]. We simply assign the MA at bus 16 because the maximum hop count from bus 16 to other buses is the minimum among all buses, and it also has the highest connection degree in the system. (More sophisticated MA assignment schemes need detailed power system and communication network information, which is out of the scope of this paper.) For testing purposes, to make every bus have a non-overlap path for comparison, we modify the topology slightly by adding a communication link between bus 19 and bus 21. Assume bus 21 is the closest bus for bus 19. Assume all query and response packets have the same size of 80 bytes, e.g., a simple PMU packet. We set the system failure requirement to 10^{-5}, which is a higher requirement than current power grid [24], and set the communication link capacity to 1.5 Mbps (one T1 line) [25] with a failure probability no more than $P_f(link)=10^{-5}$ [26]. In this case, the probability of two or more links fail simultaneously is about 10^{-8}, which is much smaller than the system requirement. Thus, in this paper, we only consider a single link failure.

To build power system knowledge, we use the PowerWorld simulator [21] to obtain the conditional probability $P_f(S|line_i)$. As we know, more reactive loads cause more system losses, and result in various instability issues which may lead to system failures. We follow the methods used in [22], [23], and gradually increase the reactive loads of all PQ buses that have nonzero reactive loads, by setting $load_{new}=load_{base}\cdot(1+x)$. The increase step of x is 10% of the base load each time. At each system load setting, we examine system contingency by tripping power transmission lines one by one to check if the system fails (shown as a blackout in PowerWorld). We vary x in a range of (0; 3.3), because a blackout usually happens when $x\geqslant 3.4$, even if we do not trip any line. As a result, we have $P_f(S|line_i)=\sum_{k=0}^{3.3}P(x=k)\cdot I_{failure}(line_i)$, where $I_{failure}(line_i)$ equals to 1 if a system failure happens; otherwise, it is 0. For $line_i$ whose tripping may cause system failures, we obtain its $P_f(S|line_i)$ based on the above procedure, associated with 15 lines ranging from 0.8% to 4.2%. We use these data for optimizing backup path selection later.

5.2 Performance of Primary Selections and Backup Paths without/with Power Knowledge

To evaluate the two primary path schemes and corresponding backup path schemes, we assign the failure probability of a communication link according to the amount of transmitted power on the corresponding power line. (Assume each communication link connects the same buses as its power line.) For lines with more than 200 MW power (in 39-bus system, under normal condition, we have 17 lines with real power more than 200 MW, which is about 50% of all power lines), we set their corresponding links with $P_f(link)=10^{-6}$; otherwise, $P_f(link)=10^{-5}$. As shown in **Table 1**, when using primary paths only, neither primary selection scheme alone can achieve the system requirement (10^{-6}), as shown in the first row. The reliability-based primary-path selection does a little better than the shortest path selection. After adding backup paths, both schemes can fulfill the system requirement and achieve similar system reliability, as shown in the second row.

Using power knowledge can improve system reliability. As discussed in Section 3, we can handle a single link failure on a primary path by using a completely non-overlap backup path

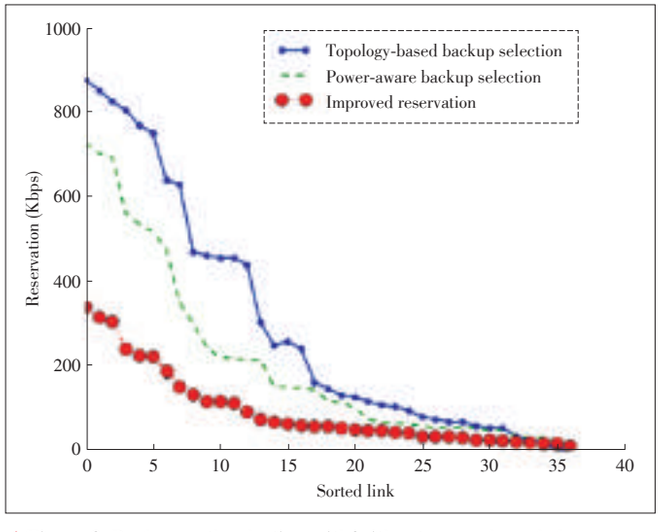
▼Table 1. Comparison of system reliability

Failure probability	Shortest hop count based	Reliability
Primary path only	1.58×10^{-6}	1.32×10^{-6}
With backup path	1.18×10^{-7}	1.22×10^{-7}

for each relay as a topology-based backup selection. However, this method consumes more resources. We utilize power system knowledge to address this issue. As mentioned before, we observe 15 lines that may lead to system failures under different load settings. Therefore, we prioritize these lines and their protection relays to better use network resources. Here we set $P_f(link)=10^{-5}$ for all links. Compared with using complete non-overlap backup paths, such a power-aware backup path selection significantly reduces the bandwidth reservation on almost every link, and the average bandwidth saving across all links is about 18%. The upper two curves in **Fig. 3** show the comparison of reservations on links. We sort them from high to low for easy illustration. In the above, we compare the maximum required link reservation on the 39-bus system for using non-overlap backup paths and partially overlapped backup paths with the system failure requirement $RS=10^{-6}$. To further show how the proposed power aware scheme can reduce link reservations, we also test it with system failure requirement $RS=10^{-5}$.

Assume the single link fails with $P_f(link)=10^{-5}$. As shown in **Table 2**, compared with the non-overlap path scheme, the power-aware scheme can significantly reduce bandwidth reservation (29% less) while still meeting the system reliability requirement. In the second row, we set the value of non-overlap path scheme as the "base" of 100%.

When some links do not have enough capacity, we assign higher priorities to the protection relays of important lines based on the power knowledge to further improve the system reliability. We compare three simple resource reservation orders in the following. The first order is to start to allocate bandwidth from the most important relay to least important one; the second order use the opposite order for comparison; the third order is to allocate bandwidth using random bus orders (here we compute the average of 20 random orders). To show the case that some relays may not obtain the required bandwidth on a link, we make link 19 as the bottleneck and reduce its capacity from 1.5 Mbps to 550 Kbps. We set the system requirement as 10^{-6}, and the failure probability of links as 10^{-5}. We observed that the relays without enough reservation vary in the different orders. For the latter two orders, some relays do not obtain enough bandwidth for their paths, for example, relays protecting Line {3, 5, 6, 15, 19, 21, 31}. However, these lines have higher probabilities in causing system failures if improperly tripped. The system failure probabilities for different orders are 1×10^{-7}, 1.5×10^{-6}, and 6.7×10^{-7} respectively.



▲Figure 3. Backup path selection with/without power knowledge and improved reservation scheme.

▼Table 2. Comparison of maximum link reservation for different backup path schemes and requirements

	Topology-only $R_S=10^{-6}$	Power-aware $R_S=10^{-6}$	Power-aware $R_S=10^{-5}$
Max reservation	878	725	625
Percentage(%)	100	82	71
Failure probability	0	1.0×10^{-7}	5.7×10^{-7}

Smart Reservation. A bus may have multiple remote relays for protecting different power lines. In common cases, they will not simultaneously communicate with the MA. This provides us another opportunity to further reduce the required bandwidth on communication links. Assume only one relay experiences a hidden failure or only one power line has disturbances. For example, in the IEEE 39-bus system, only bus 26, 28, and 29 have two remote relays protecting the same line; remote relays on other buses all protect different power lines. In this case, we only need to reserve bandwidth for relay r_i with the most strict delay requirement on a bus. Because other relays on that bus do not have delay requirement as high as r_i, the reserved capacity is sufficient for them to communicate with the MA. Again, we set the system requirement as 10^{-6} and $P_f(link)=10^{-5}$. The maximum required capacity on a link decreases from 725 Kbps to 366 Kbps, a nearly 50% saving. As shown in Fig. 3, comparing the lower two curves, on average, we save about 39% capacity on each communication link. The overall system failure probability is 1×10^{-7}, still meeting the system reliability requirement.

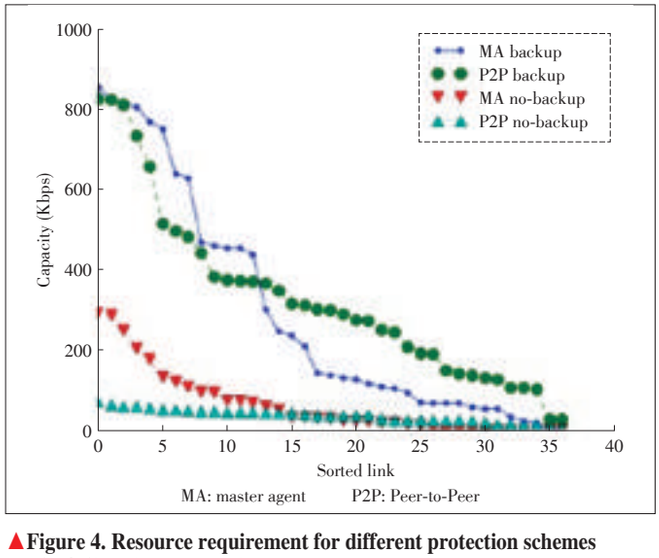
5.3 Comparing Master-Agent-Based and P2P Schemes

We follow the method in [9], assume at a single moment, there is only one hidden failure exposed in the system: a disturbance is applied to a power line that the relay with a hidden failure will sense the disturbance, and the communication network has a single link failure at most. We compare the resource requirement for the protection and the false trip proba-

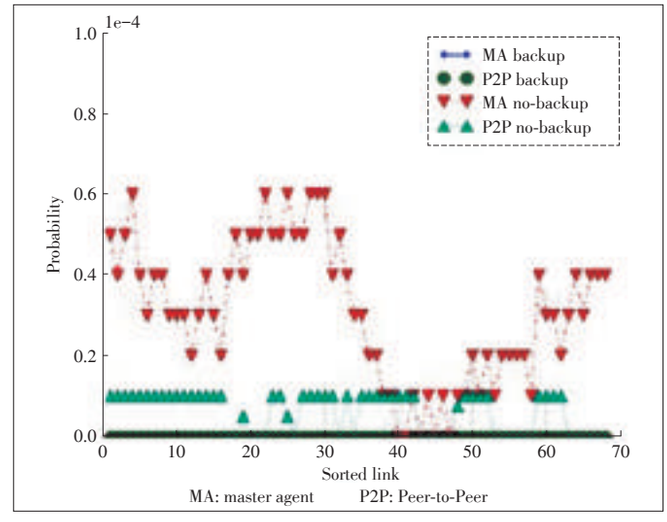
bility of each relay, under four schemes: the MA scheme without backup paths, the P2P scheme without backup paths, the MA scheme with backup paths, and the P2P with backup paths. For the primary path selection, both the MA scheme and the P2P scheme use the shortest path to the master node or peers. For the backup path selection, both schemes use non-overlap backup paths.

The result for resource requirement is shown in **Fig. 4**. Without backup paths, the P2P scheme consumes the minimum resources since the distance to peers are shorter than in the MA scheme. However, adding backup paths to both schemes significantly increases the resource usage. **Fig. 5** shows the false trip probability of each relay in the system. Under the single link failure condition, in the MA scheme without backup paths, if the primary path of a relay fails, it cannot communicate with the MA and will result in a false trip. As we can see, more relays in the MA scheme are affected than in the P2P scheme, For the P2P scheme, since each peer can send its response to the inquiry relay, the false trip occurs if all paths to the relay's peers fail, which means the failed link is shared by all paths to the peers. Intuitively, this probability is much lower than the failure of a primary path in the MA scheme. With non-overlap backup paths, both the MA scheme and the P2P scheme can handle a single link failure, in which all relays have zero failure probability. Combining the relay false trip probability with the power data ($P_f(S|line_i)$), the system failure probability can be computed.

Without backup paths, the system reliability $P_f(S)$ in the P2P scheme is 0.55×10^{-6}, which is about 4-time better than that of the MA scheme (2.62×10^{-6}). Note that the P2P scheme can meet the 10^{-6} requirement but the MA scheme cannot. This matches the results from Fig. 5 that the failure of a primary path of a relay has more influence in the MA scheme, because all relays must first contact the MA and then receive a



▲**Figure 4. Resource requirement for different protection schemes with/without backup path.**



▲**Figure 5. False trip probability of each relay, assume a single link failure.**

decision from the MA. While we can protect relays from false trips using non-overlap backup paths, judging from the resource requirement from Fig. 4, the cost of non-overlap backup path in the two schemes do not have much difference. The potential difference between the two is the response delay.

The response delay counts from the time when the query is sent until a decision reaches the inquiry relay. This delay is closely related to the path distance (hop count), especially when the traffic load is light most of the time. We compute the maximum, minimum and average hop counts for both the MA scheme and the P2P scheme. For the MA scheme, the primary/backup path distance is between a bus and the MA bus. The result for the MA scheme with non-overlap backup paths is shown in Table. 3. As a comparison, the result of the P2P scheme with non-overlap backup paths is also given. In the P2P scheme, paths exist between each pair of "corresponding relays". Note that in both the MA and P2P schemes, the minimum hop count is 0. The reason is that, in the MA scheme, there are a few relays locating at the same bus with the MA; for the P2P scheme, in the 39-bus system, relays (64,67) and relays (66,68) are located at bus 28 and 29, respectively, and they are protecting the same lines. Thus the communication between these relays are within a substation. (We assume the indexes of relays for a power transmission line with index i are $2\cdot i$ and $2\cdot i-1$.). In addition, although the average path length between (the MA and a non-MA bus) or (P2P peers) are similar, in the MA scheme the query process takes two round-trip delays. While in the P2P scheme, there is only one round-trip delay (as shown in the "Actual" column of **Table 3**). As link loads are not heavy most of the time, a shorter path benefits the protection with faster response delays.

Compare the effect of full backup vs. partial backup paths and the effect of overlap backup vs. non-overlap backup paths. The above case is the worst case resource requirement for the

▼Table 3. Path hop count in the MA scheme

	Max	Min	Average	Actual
MA primary path	6	0	3.2	6.4
MA backup path	10	0	6.2	12.4
P2P primary path	3	0	2.0	2.0
P2P backup path	12	0	5.7	5.7

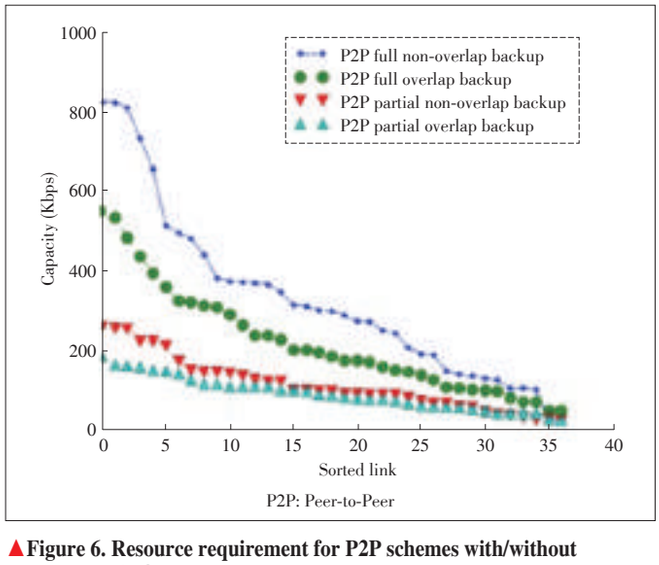
P2P scheme since a non-overlap path between each pair of "corresponding relays" are reserved. As a comparison, the shortest-hop-count overlap backup path is tested in the P2P scheme. Similar to the non-overlap scheme, resources for each "corresponding relay pair" is reserved as well. We exam the "stressed case" and assume two replies returning from peers will enable the inquiry relay to make correct decision.

Fig. 6 shows network resource requirements for each protection scheme.

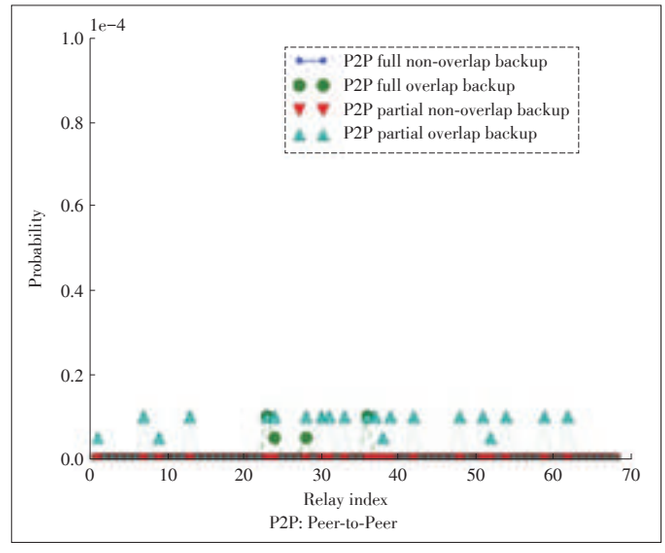
Fig. 7 shows the false trip probability of relays. We see that only four out of about 68 relays are affected when using overlapping paths. Fig. 6 and Fig. 7 also show that the resource requirement further decreases because now each relay only reserves for two backup paths.

When using non-overlap backup paths, all relays can handle the single link failure; while using overlapping backup path uses less resources at the cost of a few more potential false trips. **Table 4** shows how the total resource requirement and the changes of system reliability for different backup schemes.

Compare the effect of the number of overlapping backup paths in the P2P scheme. We try to identify how many overlapping backup paths should be used in the P2P scheme by varying the number of backup paths for each relay from two to five. We choose the shortest hop count path as a backup path, and allow this path to have overlapping links with its primary P2P path. The results are summarized in **Table. 5**, including the total resource requirement, the overall failure probability of the system, number of potential relay failure, and average relay failure probability. As we can see, the more backup path we use, the less number of relays that will have false trips. The resource requirement is as expected: the more backup paths we use, the more resources we consume. Comparing the first two lines of Table 5, a significant point is that, when we increase the number of overlap backup paths from two to five, the resource cost doubles, but the reliability is improved by ten-folds. While the trends of improvement are different in in the second and forth lines, the reason is that power lines are not of the same importance: for some lines, the false trip may lead to severe system failure, while others are not.



▲Figure 6. Resource requirement for P2P schemes with/without backup path for each relay.



▲Figure 7. Relay false trip probability for P2P schemes with/without backup path for each relay, assume a single link failure.

▼Table 4. Total resource requirement and system failure probability with/without backup path for each relay

	Full non-overlap	Full overlap	Two BP non-overlap	Two BP overlap
Resource	12140	8140	4131	3372
$P_f(S)(\times 10^{-7})$	0	0.2	0	2.76

6 Conclusions and Future Work

In this paper, we have developed more reliable remote relay protection schemes by exploring both network link reliability and power systems knowledge on SG. Furthermore, to address the single point of failure of common centralized control center, we have also investigated P2P protection approaches. The simulation results show that the proposed method can significantly improve power system reliability while utilizing network resource more effectively.

In this paper, as most existing research, we assume that a

Table 5. Total resource requirement, System failure probability, and Number of potential failure relay and their average failure probability under different P2P schemes

	2 Overlap backup	3 Overlap backup	4 Overlap backup	5 Overlap backup
Resource(Kbps)	3372	5122	6646	7638
$P_f(S)(\times 10^{-7})$	2.76	2.5	1.0	0.29
Number	21	16	9	6
$\overline{P_f(relay)}(\times 10^{-6})$	2.8	2.2	1.2	0.6
$\frac{Normalized}{P_f(realy)}$	4.67	3.67	2	1

cascading failure starts at a single line, which leads to the sequential trips of neighbor lines. However, recent research [27] demonstrated that this sequence is not easily characterized and may be geographically separated, i.e., the cascading does not necessarily develop in a contiguous manner. Our future investigation will focus on this new direction. Although the agent-based scheme is helpful in preventing the cascading failure, we notice that it also has the potential to mitigate the damage of already on-going cascading, e.g., by tripping certain lines in advance. The foundation of such schemes is reliable real-time network communications, from collecting system states to accurate transmission of decisions to each critical location.

References

[1] S. H. Horowitz and A. G. Phadke, "Third zone revisited," *IEEE Transactions on Power Delivery*, vol. 21, no. 1, Jan. 2006, pp. 23- 29. doi: 10.1109/TPWRD.2005.860244.
[2] NERC. *Rationale for the use of local and remote (zone 3) protective relaying back-up systems* [Online]. Available: http://www.nerc.com/docs/pc/spctf/Zone3Final.pdf, 2005.
[3] D. Novosel, M. Begovic, and V. Madan, "Shedding light on blackouts," *IEEE Power and Energy Magazine*, vol. 2, no. 1, Jan. 2004, pp. 32-43. doi:10.1109/MPAE.2004.1263414.
[4] D. C. E. de la Garza, "Hidden failures in protection systems and its impact on power system wide-area disturbances," M. S thesis, Virginia Polytechnic Institute and State University, 2000.
[5] J. S. Thorp, A. G. Phadke, S. H. Horowitz, and S. Tamronglak, "Anatomy of power system disturbances: Importance sampling," *International Journal of Electrical Power and Energy Systems*, vol. 20, no. 2, pp. 147-152, Feb. 1998.
[6] J. S. Thorp and A. G. Phadke, "Protecting power systems in the post restructuring era," *Computer Applications in Power, IEEE*, vol. 12, no. 1, pp. 33-37, 1999.
[7] H. Wang and J. S. Thorp, "Optimal locations for protection system enhancement: A simulation of cascading outages," *IEEE Transactions on Power Delivery*, vol. 16, no. 4, Oct. 2001, pp. 67. doi: 10.1109/MPER.2001.4311473.
[8] S. Garlapati, H. Lin, S. Sambamoorthy, S. K. Shukla, and J. S. Thorp, "Agent based supervision of zone 3 relays to prevent hidden failure based Tripping," In *2010 First IEEE International Conference on Smart Grid Communications*, Miami, USA, 2010, pp. 256-261.
[9] H. Lin, "Communication Infrastructure for the Smart Grid: Co-Simulation Based Study on Techniques to Improve the Power Transmission System Functions with Efficient Data Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2012.
[10] X. Fang, S. Misra, G. Xue, and D. Yang. *Smart grid - the new and improved power grid: A survey* [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.387.3141
[11] W. Wang, Y. Xu, and M. Khanna, "Survey paper: A survey on the communication architectures in smart grid," *Computer Network*, vol. 55, no. 15, October 2011, pp. 3604-3629. doi: 10.1016/j.comnet.2011.07.010.
[12] D. E. Bakken, B. Anjan, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, "Smart generation and transmission with coherent, real-time Data," *Proceedings of IEEE*, vol. 99, no. 6, pp. 928- 951, 2011. doi: 10.1109/JPROC.2011.2116110.
[13] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391-404, 2012.
[14] J. Zhang and Y. Dong, "Preventing false trips of zone 3 protection relays in smart grid," *TSINGHUA Science and Technology*, vol. 20, no. 2, pp. 142-154, 2015.
[15] J. Chen, J. S. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power & Energy Systems*, vol. 27, no. 4, pp. 318-326, 2005.
[16] U. S. -Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," 2004.
[17] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, 2010. doi: 10.1109/MPE.2009.934876.
[18] D. E. Bakken, C. H. Hauser, H. Gjermundrød, and A. Bose. *Towardsmore flexible and robust data delivery for monitoring and control of the electric power grid* [Online]. Available: http://www.gridstat.net/TR-GS-009.pdf
[19] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Chen, "cyber security and privacy issues in smart grids," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 981-997, 2012.
[20] V. Centeno, J. Thorp, and A. Phadke. *Advanced protection system using wide area measurements* [Online]. Available : http://www.uc-ciee.org/_ucciee68/images/downloadable content/electric grid/APWA Final Report.pdf, 2010
[21] PowerWorld Corporation. *Powerworld homepage* [Online]. Available: http://www. powerworld.com/
[22] A. Agatep, "Voltage stability analysis using simulated synchrophasor Measurements," M. S thesis, California Polytechnic State University, 2013.
[23] I. Musirin and T. A. Rahman, "On-line voltage stability based contingency ranking using fast voltage stability index (FVSI)," *IEEE/PES Transmission and Distribution Conference and Exhibition 2002: Asia Pacifi.*, Yokohama, Japan, 2002, pp. 1118-1123, 2002. doi: 10.1109/TDC.2002.1177551.
[24] C. Hertzog. *Reliability and the smart grid* [Online]. Available: http://www.smartgridlibrary. com/2010/08/02/reliability-and-the-smart-grid/
[25] R. Hasan, R. Bobba, and H. Khurana, "Analyzing naspinet data flows," In *Power Systems Conference and Exposition (PSCE'09), IEEE/PES*, pp. 1-6, 2009.
[26] S&C Electric Company. *Designing a smart grid communication system to achieve 99.999% link availability* [Online]. Available: http://www.sandc.com/edocs pdfs/edoc 075041.pdf
[27] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failuresanalysis and control implications," In *INFOCOM, 2014 Proceedings IEEE*, Toronto, Ontario, Canada, 2014, pp. 2634-2642.

Manuscript received: 2015-04-29

Biographies

Jiapeng Zhang (jiapengz@hawaii.edu) received his BS degree in Electronic Information Technology from the Macau University of Science and Technology in 2010 and MS degree in Telecommunication from the Hong Kong University of Science and Technology in 2011. He is currently pursuing his PhD degree in University of Hawaii at Manoa. His research interests are network scheduling, planning, simulation, and smart grid communication.

Yingfei Dong (yingfei@hawaii.edu) received his BS degree and MS degree in computer science at Harbin Institute of Technology, China, in 1989 and 1992, his Doctor degree in engineering at Tsinghua University in 1996, and his PhD degree in computer and information science at the University of Minnesota in 2003. He is currently an associated professor at the Department of Electrical Engineering at the University of Hawaii at Manoa. His current research mostly focuses on computer networks, especially in network security, smart grid communication security, cloud security, real-time networks reliable communications, Internet services, and distributed systems. His work has been published in many referred journals and conferences. He has served as both organizer and program committee member for many IEEE/ACM/IFIP conferences. He is also serving on several editorial boards for journals on security and networking. His current research is supported by National Science Foundation.

DOI: 10.3969/j.issn.1673-5188.2015.03.005
http://www.cnki.net/kcms/detail/34.1294.TN.20150902.1610.002.html, published online September 2, 2015

Experimental Study on Cloud-Computing-Based Electric Power SCADA System

Yongbo Chen[1], Jijun Chen[1], and Jiafeng Gan[2]
(1. ZTE Corporation, Nanjing 210012, China;
2. Dongfang Electronics Co., Ltd., Yantai 264000, China)

Abstract

With the development of smart grid, the electric power supervisory control and data acquisition (SCADA) system is limited by the traditional IT infrastructure, leading to low resource utilization and poor scalability. Information islands are formed due to poor system interoperability. The development of innovative applications is limited, and the launching period of new businesses is long. Management costs and risks increase, and equipment utilization declines. To address these issues, a professional private cloud solution is introduced to integrate the electric power SCADA system, and conduct experimental study of its applicability, reliability, security, and real time. The experimental results show that the professional private cloud solution is technical and commercial feasible, meeting the requirements of the electric power SCADA system.

Keywords

smart grid; cloud computing; electric power SCADA; professional private cloud; virtualization; cloud storage; real-time industrial control

1 Introduction

An electric power system typically involves generation, transmission, transformation, distribution, consumption, and dispatching processes. Electric power is generated and consumed simultaneously, and is not available for mass storage or transportation. Thus, as the key to the electric power system, monitoring and dispatching guarantee the reliability and security of electric power generation, transmission, distribution, and consumption, and play a key role in providing high-quality and economic electric power. An electric power dispatching and monitoring system is often called a supervisory control and data acquisition (SCADA) system, energy management system (EMS), or distribution management system (DMS) globally. In this article, we call it the electric power SCADA system.

Monitoring and dispatching of the electric power system relied on simple automatic devices, phones, and operation personnel from the very beginning, then on computers in the 1960s. With the popularity of high-performance micro-computers in the 1970s, more power monitoring and dispatching functions became available, and gradually developed into the electric power SCADA system. In the early stage, the electric power SCADA system mainly used a multi-computer architecture, consisting of single-server and two-server cluster systems. Currently, the system uses computer systems with a distributed open architecture [1]–[3]. The electric power SCADA system provides SCADA, automatic generation control (AGC), automatic voltage control (AVC), EMS, DMS, dispatcher training system (DTS), geographic information system (GIS), and other useful functions [3]. The software application system is constructed and developed by using the standard CIM model, and software architecture has evolved from the Client/Server architecture to the current Browser/Server architecture. The new-generation Smart Grid dispatching and control system uses multi-core computer cluster technology to improve system reliability and processing capacity, and uses a service-oriented architecture (SOA) to enhance system interoperability and achieve "horizontal integration and vertical interconnection" [4] of power grid dispatching services.

Hardware infrastructure of these application systems involves high-performance servers, complex high-speed computer networks, high-performance and highly reliable data storage systems, and workstations. The SCADA software is developed based on the platform which consists of Windows, UNIX, and Linux operating systems, and is based on relational databases. The whole system is connected through computer networks for data exchange and sharing, and application programs share information through an enterprise service bus (ESB). With the development of the traditional IT application systems, IT-based applications have been expanding deeply to another industry field, and encountered various problems and bottlenecks. The

same is true for the electric power SCADA system, which is a professional IT application system. Especially with the advancement of Smart Grid, the future electric power dispatching center should have high computing capacity, and powerful information acquisition, integration, and analysis functions. Existing centralized computing platforms of electric power systems can hardly meet the above requirements, which has become one of the major bottlenecks in the Smart Grid [5].

The major disadvantages are as follows:

1) Low basic resource utilization and poor scalability. A large amount of basic computing resources to meet the demands in peak hours are idle during off-peak hours. To ensure reliability, lots of resources are redundant, and cannot be fully utilized. Contradictions are growing between energy demands and conservation policies. Due to the upgrade of business, the existing IT infrastructure cannot be reused. Currently, analysis and computing in the electric power system rely on the centralized computing platform in the dispatching center. Due to limited computing capacity, poor scalability, and high upgrade costs, large-scale power systems suffer from insufficient data storage and analysis capabilities [5].
2) Poor system interoperability leading to information islands. Parallel application systems have their own architectural features, and therefore resources cannot be exchanged or reused, further hampering in-depth information and business integration. Due to parallel information island applications, computing resources cannot be shared, limiting the application of distributed computing, cloud storage, and big data.
3) Limited development of innovative applications, and long launch period of new business. Traditional business applications should go through a long period of design, project initiation, bidding, and procurement before they are launched, failing to meet the requirements of rapid business expansion. Compatibility with existing systems is achieved at the expense of functions, quality, and time. With the emergence of Smart Grid, Internet of Things (IoT), mobile Internet, and big data technologies, the existing architecture and technology can hardly meet the demands for new business development and application. With the development of Smart Grid construction, big data has been regarded as an important support for Smart Grid. Most of the current power data analysis systems are based on relational databases, with low analysis speed and poor scalability. Therefore, they can hardly meet the demands for big data storage and analysis in the era of Smart Grid, which has become a bottleneck for Smart Grid construction [6].
4) Increasing management costs and risks, and decreasing equipment utilization. For example, the installed capacity of data centers grows, rapidly increasing management and maintenance complexity. Management costs and energy consumption are increased. System reliability is lowered, while operational risks are increased. Upgrade costs are also increased.

Fig. 1 shows the relations between IT resources based on the statistical data of the Dongfang Electronics DF8000 dispatching master system in projects at different scales. Fig. 1 involves the number of services, storage space, energy consumption, availability, and operational costs.

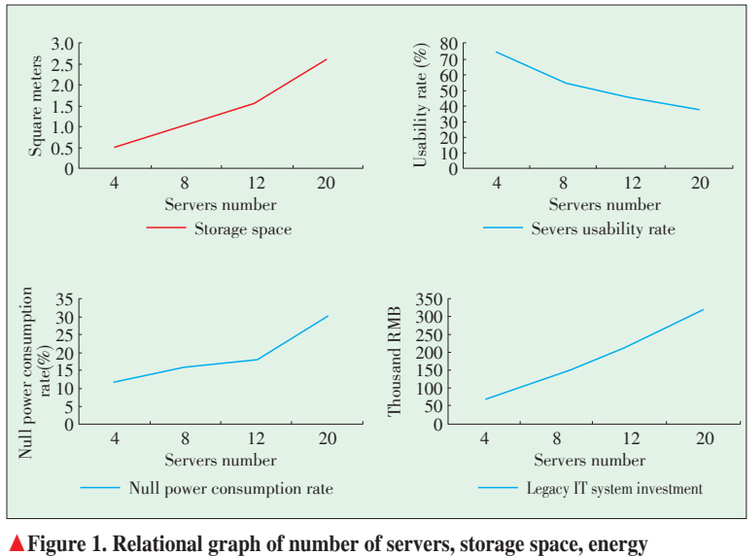
2 Cloud Computing Technology and Its Application in Electric Power Industry

2.1 Overview of Cloud Computing Technology

Since people proposed the Cloud Computing concept, cloud computing has been fully discussed and studied, and applied and developed in various scenarios in the past ten years. The major features of cloud computing are described in [7], including: 1) Use on demand; 2) Ubiquitous access; 3) Multiple users and resource pools; 4) Flexibility; 5) Measurement; 6) Redundancy.

Thanks to these features, cloud computing can be used to solve various problems occurred during application deployment, use, and innovation process of the electric power SCADA system.

The current cloud computing applications include public cloud, private cloud, and hybrid cloud, which are suitable for different application scenarios. A private cloud has advantages in application autonomy and security. However, the electric power SCADA system and other real-time industrial control systems have strong requirements for adaptability, reliability, security, and real time. A private cloud is applicable to common business scenarios, including office automation, enterprise resource planning (ERP), finance, and HR management,



▲**Figure 1. Relational graph of number of servers, storage space, energy consumption, availability, and operational costs.**

but is not suitable for specialized applications of industrial production. Therefore, a private cloud needs to be further improved. In this paper, we propose to use the professional private cloud solution to solve these problems. Professional private clouds are deployed in professional production control areas, which are logically or even physically isolated from non-control areas, to meet the strong requirements for adaptability, reliability, security, and real time.

2.2 Application of Cloud Computing in Electric Power Industry

In accordance with the *Power Monitoring System Security Regulations* (National Development and Reform Commission of the People's Republic of China <No. 14>), the field of electric power production and operations management is divided into production control areas and management information areas; and production control areas are further divided into control zones (Safety Zone I) and non-control zones (Safety Zone Ⅱ). The cloud computing technology has numerous practical applications in management information areas. The application scenarios include customer service, electric power marketing, video surveillance, collaborative office, and ERP; and the application areas include offices, maintenance companies, power plants, training schools, and business offices. The research of Zhejiang Provincial Electric Power Company (ZPEPC) on the application of enterprise management IT infrastructure in resource pool virtualization as well as related application results are described in [8]. The author describes the research and experimentation of Henan Electric Power Company on cloud computing–based data center platforms of power grid enterprises in [9]. The pilot construction and application results of cloud desktop technologies in State Grid Corporation of China are described in [10]. These applications of cloud computing technology in management information areas have greatly enhanced IT resource utilization and operation and maintenance efficiency of electric power enterprises, and achieved good economic and social benefits through exploration and practice of cloud computing application in the electric power industry.

Discussion and research of cloud computing technology are also conducted in production control areas. Because of the extreme importance of the electric power system to social and economic production and life, research and practice of cloud computing carried out in production control areas of the power system are conservative, with few research results and application cases.

The bottlenecks and limitations of traditional electric power dispatching systems are discussed in [5]. The author also describes the major features of cloud computing, and elaborates on the implementation of cloud computing platforms in electric power systems by focusing on physical components, system architecture, and software technology.

The advantages of cloud computing models, assesses potential risks are discussed in [11], the availability of popular cloud computing technologies in the electric power SCADA system are analyzed, and whether cloud computing models can be used in the electric power SCADA system are thoroughly explored. This article finally outlines an application architecture of cloud computing models in the electric power SCADA system based on four layers (including the infrastructure layer, resource management layer, cloud service layer, and application layer) and six applications (including models, data, searching, planning, calculation, and mutual backup).

The application of cloud computing in the Smart Grid dispatching system is studied in [12], and a task scheduling algorithm based on improved genetic algorithms are proposed in [12], aiming to improve distributed data processing capabilities and resource optimization capabilities of the Smart Grid dispatching system. Article [13] provides the cloud platform logic components and programming models of the Smart Grid operation and dispatching system.The Distributed Fusion Genetic Algorithm (DFGA) to cloud computing is also introduced in [13].

In [14], the author elaborates on innovative research and development and practical application of cloud computing in the electric power SCADA system, and describes the deployment solutions, function implementation, key technologies, innovations, applications, and economic and social effects of cloud computing–based electric power dispatching and online analysis systems. Pioneering research and development and practical application of cloud computing in the electric power SCADA system are described.

In accordance with the research results of these articles, common private cloud computing platforms cannot meet the requirements for security, reliability, real time, and adaptability of control areas (Safety Zone I). As of now, traditional electric power SCADA application systems are seldom deployed on cloud computing platforms, and production control SCADA systems are seldom used in the entire real-time industrial production field. Therefore, we use private cloud solutions in this experimental study to verify the technical and commercial feasibility of cloud computing platforms in the electric power SCADA system.

3 Goals and Solutions of Experimental Study on Cloud Computing–Based Electric Power SCADA System

3.1 General Idea and Goals of the Experimental Study

Based on the above analysis, the use of cloud computing technologies for new-generation electric power SCADA application systems will be a new development direction for Smart Grid. However, existing traditional electric power SCADA systems still have a large market share in the electric power dispatching market. The aforementioned problems will persist, and the new-generation Smart Grid dispatching application sys-

tem based on cloud computing is still at an early stage of exploration, research, and development, with a large room for large-scale commercial deployment. It is very meaningful and valuable to use cloud computing technologies to solve the existing problems in the electric power SCADA system, and facilitate smooth transition and evolution of the existing electric power SCADA system before sophisticated application of the cloud computing dispatching and monitoring system. Therefore, ZTE together with Dongfang Electronics made attempts in this regard, built a research platform in the laboratory environment for experimental verification, and achieved the expected results.

The general idea of the experimental study is to complete operation tests of traditional electric power SCADA systems on cloud computing platforms, and integrate the main application modules of the electric power SCADA systems on the cloud computing platforms to verify their adaptability, reliability, security, and real time.

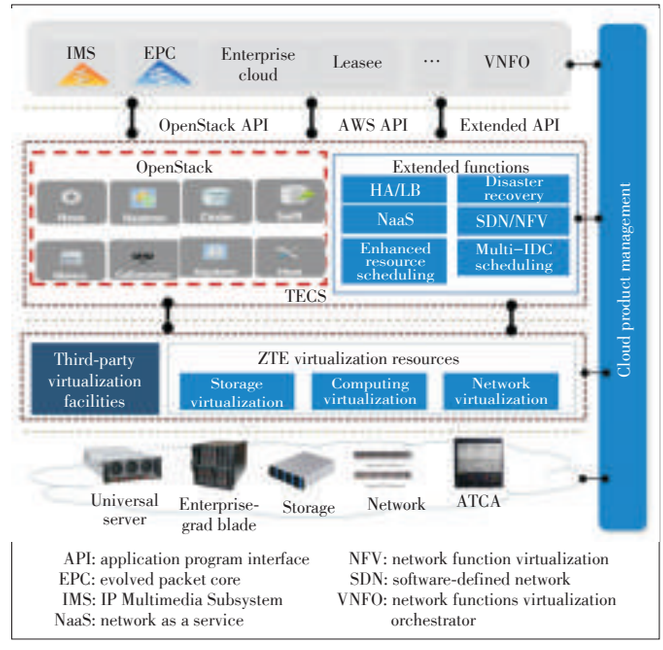
Major goals of this study include design and development of the solutions to integrating traditional electric power SCADA systems and cloud computing platforms, and test and validation of traditional electric power SCADA services on cloud computing platforms. This study assesses the adaptability, reliability, security, and real time of integrating cloud computing platforms and traditional electric power SCADA systems, thoroughly understands the differentiated requirements of electric power SCADA systems for cloud computing platforms, and proposes the development direction for electric power SCADA systems based on the cloud computing architecture.

3.2 Overall Solution to the Experimental Study

This experimental study uses the ZXTECS cloud computing platform developed by ZTE. The ZXTECS cloud computing platform based on computing, storage, and network virtualization provides resource management and scheduling functions. The ZXTECS platform based on the OpenStack cloud management platform integrates the network function virtualization (NFV) architecture, enhances the support for performance and high availability, and is an integrated ICT cloud management platform meeting both IT and CT cloud computing requirements.

Fig. 2 shows the system architecture of the ZXTECS platform. Major features of this platform include 1) Openness: open and unified resource pool management; 2) High performance: performance optimization of virtual computing to meet the requirements of NFV for high-performance virtualization; 3) High reliability: live migration of virtual machines, watchdog, exception recovery, remote resetting, and control node cluster functions; 4) High usability: automatic upgrade deployment, real-time alarms, and performance statistics.

The electric power SCADA system uses the DF8000 series integrated software of Dongfang Electronics for power dispatching. This is a new-generation power SCADA system developed



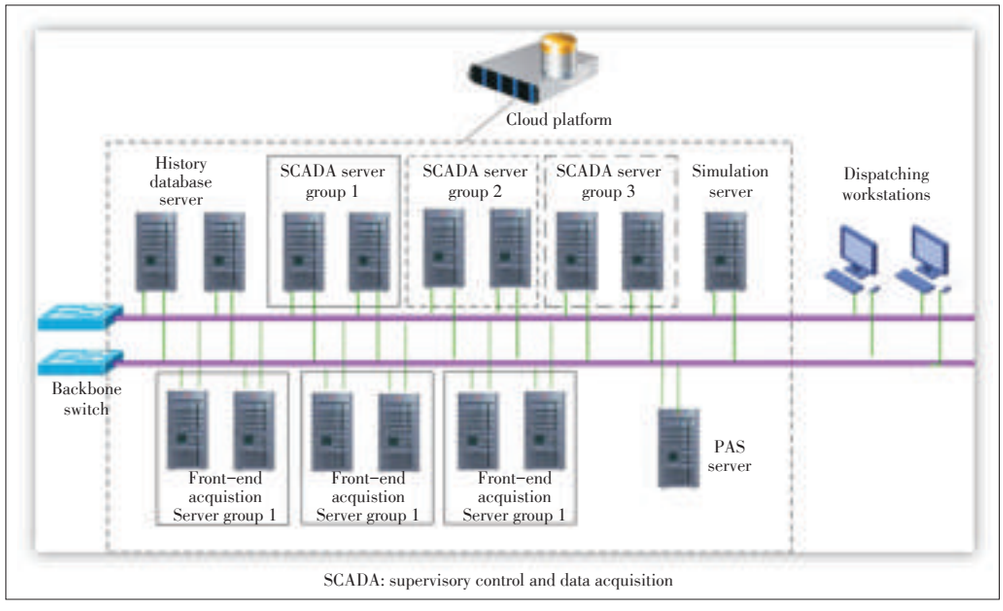
▲**Figure 2. System architecture of the ZXTECS cloud computing platform.**

by using the latest computer communications technology, database technology, object-oriented technology, component technology, Internet technology, and dynamic server technology, and following the CORBA middleware specifications, IEC61970 CIM/CIS, IEC61968, IEC61850, and international SOA standards. By using the SOA and loosely-coupled UI design, the DF8000 system achieves unified operations, monitoring, management, and maintenance of the entire system, following the trend for growing integration of dispatching information in the electric power system. The DF8000 system has been highly recognized in the international and domestic markets, and achieved an influential position in the industry.

The computing, storage, and network resources required for system tests are provided by the resource pools on the cloud computing platform, based on which the DF8000 system is integrated.

Fig. 3 shows the logical networking structure of the DF8000 system. Virtualization deployment of the history server, SCADA servers (multiple sets can be deployed as required, and one set is deployed in this experiment), front-end acquisition servers, and PAS server is implemented on the cloud computing platform. The system uses a dual-Ethernet architecture. To meet the reliability requirements of the system, two servers should be deployed for each of the aforementioned server type except the PAS server and simulation server. Two virtual servers are deployed on different physical machines, implementing the reliability function of traditional hot-standby clusters.

A simulation server is deployed in the system as the simulation data generation server for the experimental test. According to the dispatching master system of a provincial capital (in



▲Figure 3. Logical networking solution of the DF8000 SCADA application system.

which capacity of the power grid is more than 15 GW for 4.3 million users until 2015), the data size is 500,000 points. The simulation data generation server is connected to the front-end data acquisition server through the network provided by the cloud computing platform.

Restricted by the experimental resources, in order to ensure resource allocation to the servers, workstation scheduling resources are not provided on the cloud computing platform, and workstations are scheduled through ordinary PCs.

3.2.1 Physical Networking Solution

Fig. 4 shows that the system is divided into the computing plane and control plane. Two mutual-backup management servers are deployed on the control plane, and manage computing nodes through dual high-speed Ethernets. The control plane and computing plane (or the business plane) are isolated to ensure security. The control plane implements management and monitoring functions of the cloud computing platform. The computing plane consists of the computing server, storage server, high-speed Ethernet, and dispatching workstations, which are the basic physical resources of the cloud computing platform. This solution involves three computing servers, dual-plane high-speed Ethernet, a set of high-performance storage devices, and two dispatching workstations.

3.2.2 Integrated Logic Structure

Fig. 5 shows the logical integration architecture of the cloud computing platform and SCADA system. The cloud computing platform provides basic IaaS services, including cloud security, resource pool, operations management, and virtual machine scheduling management functions. The functions in the dotted red box are not involved in this experiment. In accordance with the logical networking structure shown in Fig. 3, the cloud computing platform provides the SCADA system with computing, storage, and network resources, as well as operating systems, databases, and other platform software through virtual machine scheduling management, and finally implements basic IaaS services of the cloud computing platform. The electric power SCADA software system deploys related application systems on the virtual machine in a conventional manner to achieve various functions of the electric power SCADA system.

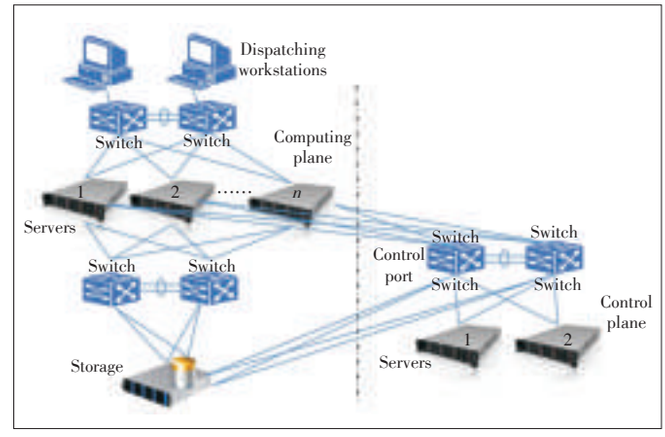
Tables 1 and **2** show the test platform environment and configurations.

This experimental test platform is built and deployed in a test lab of the Central R&D Institute in the ZTE Nanjing R&D Center. The professional electric power SCADA testers of Dongfang Electronics log in to the Dispatcher's Workstation through Remote Desktop, and perform tests in accordance with the test outline.

4 Content and Conclusion of the Experimental Test

4.1 Content and Analysis of the Experimental Test

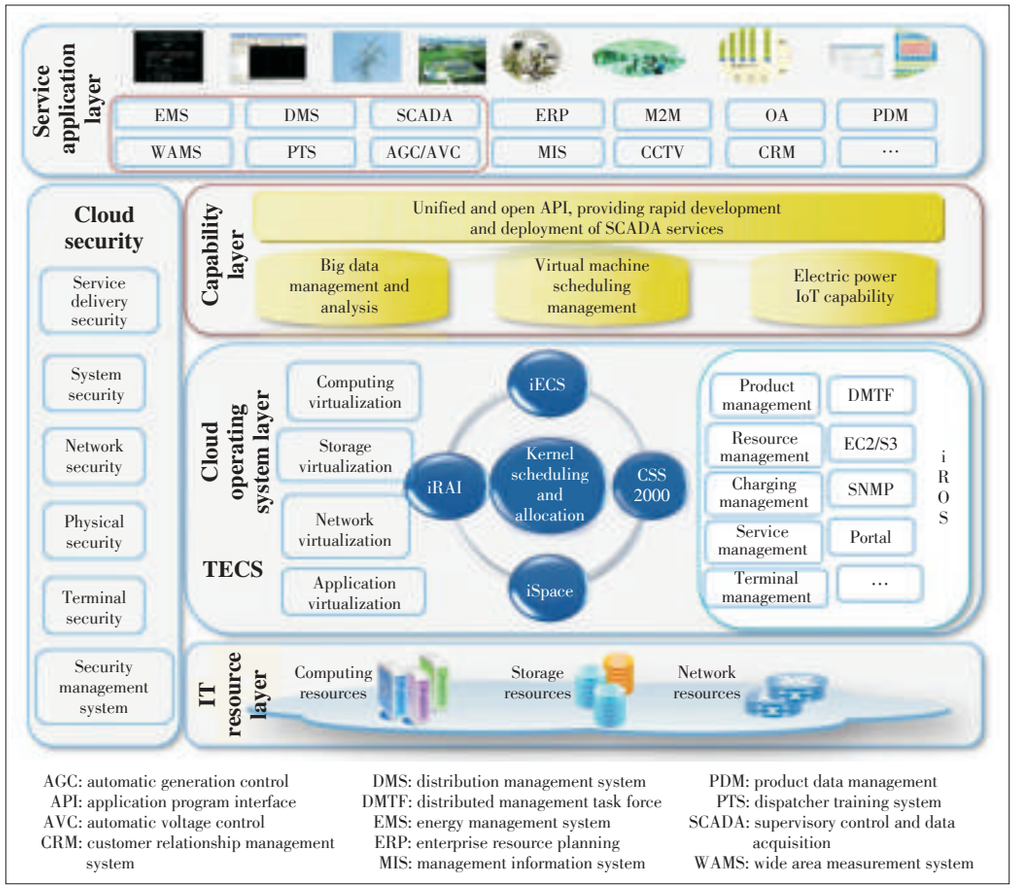
The experimental test involves function, performance, and saturation tests, which are performed in accordance with the standard test outline of the DF8000 application software.



▲Figure 4. Physical networking solution of the cloud computing platform in the experimental environment.

Experimental Study on Cloud-Computing-Based Electric Power SCADA System

Yongbo Chen, Jijun Chen, and Jiafeng Gan



▲**Figure 5. Integrated software architecture of the cloud computing platform and electric power SCADA system in the experimental environment.**

The function tests mainly verify the design functions to be implemented by the DF8000 on the cloud computing platform, and the integrity of its functions. As required by the test outline, the function tests involve four electric power dispatching functions (including SCADA, EMS, AVC, and AGC), with a total of 1343 function points and 59,389 I/O test points.

The performance tests are divided into two levels, with 66 level-1 test items and 206,104 I/O points, and 64 level-2 test items and 501,251 I/O points. The saturation tests are also divided into two levels, with 40 level-1 test items and 206,103 I/O points, and 64 level-2 test items and 501,251 I/O points.

Function tests of the above 1330 items in the 1343 function items were conducted, with a pass rate of 100%. The other 13 function items related to printing, GPS time calibration, and pulse meters were not tested because related devices were not deployed on the experimental test platform. These items are not directly related to the computing platform, and do not affect the test goals.

▼**Table 1. Software platform configurations of the experimental test platform**

	Category	Version
Server OS	Red Hat Linux (64-bit)	6.2
Client OS	Windows 7	Flagship Edition
Database	Oracle	11g (11.2.0.1.0)
Network	1000 Mbps	

The performance and saturation tests were conducted at two different load levels: level-1 system load with 206,103 I/O points, and level-2 system load with 501,251 I/O points. One item failed in the level-1 load performance tests, with a pass rate of 98.5%. Two items failed in the level-2 load performance test, with a pass rate of 96.9%. These items failed because the simulation PC memory load on the dispatcher node exceeded 30%.

The saturation tests were also conducted at two I/O load levels, with full-load operations for 72 hours. A total of 40 level-1 items and 64 level-2 items are involved, with the pass rates of

▼**Table 2. Logical server configurations and performance parameters of the experimental test platform**

Server name	Function	Number of virtual machines	Major performance indicator
History server	Saves historical data and electric power model data	2 × 1	CPU: 2.80 GHz, quad-core, Memory: 32 GB, Disk: 375 GB
SCADA server	Processes data and gives alarms in real time	2 × 1	CPU: 2.8 GHz, dual-core, Memory: 8 GB, Disk: 75 GB
Front-end acquisition server	Collects data and manages RTU communications	2 × 3	CPU: 2.80 GHz, dual-core, Memory: 8 GB, Disk: 75 GB
PAS server	Performs application computing and provides application services	1	CPU: 2.80 GHz, dual-core, Memory: 8 GB, Disk: 300 GB
Simulation server	RTU simulation	1	CPU: 2.70 GHz, dual-core, Memory: 8 GB, Disk: 75 GB

CPU: central processing unit RTU: remote terminal unit SCADA: supervisory control and data acquisition

97.5% and 96.9%, respectively. For the failed items, the memory usage on the dispatcher node exceeded 30%, and memory and CPU usage on the simulation server is high. Similar to performance tests, the dispatcher node is restricted by the experimental test platform. The simulation server is deployed only for the test, and is not needed in actual application deployment. Due to the limitations of test resources, the performance of the simulation server cannot be improved.

Table 3 is the detailed statistical results of experimental tests. **Table 4** is an analysis of the results of the experiment.

▼Table 3. Experimental test results

Test category	Number of test I/O points	Total number of test items	Number of tested items	Number of untested items	Number of failed items	Pass rate
Function test	59,389	1343	1330	13	0	100%
Performance test	206,103	66	66	0	1	98.5%
	501,251	64	64	0	2	96.9%
Pressure test	206,103	40	40	0	1	97.5%
	501,251	64	64	0	2	96.9%

▼Table 4. Test result analysis

Test category	Number of I/O points	Number of untested items	Number of failed items	Reason	Impact analysis
Function Test	59,389	13	0	Untested functions related to printing, GPS time calibration, pulse meters, and reports have nothing to do with the cloud computing platform.	Does not affect test goals
Performance Test	206,103	0	1 (Memory usage on the dispatcher node exceeds 30%)	The test item is the physical client, which is not related to the cloud computing platform.	Does not affect test goals
	501,251	0	2 (Memory usage on the dispatcher node exceeds 30%)	The dispatcher node test item is the physical client, which is not related to the cloud computing platform.	Does not affect test goals
Pressure Test	206,103	0	1 (Memory usage on the dispatcher node exceeds 30%)	The test item is the physical client, which is not related to the cloud computing platform.	Does not affect test goals
	501,251	0	3 (Memory and CPU usage on the RTU server is high)	RTU server test items are tested through distributed solutions.	Does not affect test goals

CPU: central processing unit RTU: remote terminal unit

- Suitability Evaluation

Through the whole tests, the SCADA system based on the ZXTECS Cloud computing platform are running very well, the test results have proved the professional private cloud platform are suitable to the power SCADA system deployment.

- Reliablity Evaluation

The reliablity test items such as Live Migration, Save/Restore, Fault Recover, Watch Dog, Fault Reset etc. are all passed successfully. All these tests are used to evalute the SCADA system reliable operation status, recover capabilties under the fault situations. The results have proved the SCADA system based on ZXTECS platform meet the power SCADA system reliability requirements.

- Security Evaluation

The cloud computing platform deployed for the electric power SCADA system is a professional private cloud platform, with the overall architecture deployed in the control zone (Safety Zone I), in line with the requirements of the Power Monitoring System Security Regulations. The system logic structure and security features of tested SCADA system are not changed. It provides the basic security. The professional private cloud provides comprehensive cloud securityprotection stucture.

- Real-time Evaluation

There are 12 items are related with the system real-time capabilities shown is **Table 5**. The test results indicate that realt-time performance is meet the requirement of the SCADA system. The CPU load rate, memory storage rate tests result indicate the cloud computing platform has eough computing perfor-

▼Table 5. The real-time performance test results

No.	Test items	Evaluation standard	Test 1st	Test 2nd	Test 3rd	Average	Pass/ Not pass
1	RTU host and backup channel switch automatically	≤ 30 s	25.15	27.19	23.52	25.29	Pass
2	RTU host and backup channel switch manually	≤ 4 s	2.71	2.45	3.11	2.76	Pass
3	Digital value change transmission	≤ 3 s	1.66	1.89	1.79	1.78	Pass
4	Operator interface telemetry update time	≤ 10 s	3.06	2.76	3.45	3.09	Pass
5	Remote command execution time	≤ 2 s	1.92	1.79	1.98	1.90	Pass
6	SOE alarm transmission time	≤ 6 s	2.62	2.14	2.01	2.26	Pass
7	Push Switch shift alarm frame to the Screen time	≤ 4 s	3.1	3.42	3.63	3.38	Pass
8	Remote control command processing time (with preset time)	≤ 3 s	2.22	2.31	2.35	2.29	Pass
9	Remote control command processing time (without preset time)	≤ 3 s	1.74	1.79	1.88	1.80	Pass
10	Historical data query time-data view query a remote measurement data of a day	≤ 5 s	1.71	1.49	1.8	1.67	Pass
11	MMI curves of the query time	≤ 5 s	1.52	1.12	1.14	1.26	Pass
12	The picture call response time (from the button to display the whole picture time)	85% picture call response time ≤ 3 s,the rest 15% response time≤4 s	2.97	2.93	2.58	2.83	Pass

mance margin. Professional private platform provide elastic computing resources allocation in time for the power SCADA system to gurantee the real-time performance adequately.

4.2 Results

Compared with the test results of the traditional IT architecture, the function, performance, and Saturation test results indicate that the indicators of the SCADA/EMS system based on the cloud computing platform meet the actual needs of power grid operations, and some indicators, such as the network load rate, are better than those of the traditional IT architecture. It can be seen from the function, performance, and pressure test results that the deployment of electric power SCADA system software on the cloud computing platform is feasible, with the applicability and real time of the system meeting commercial requirements. In addition, reliability function tests such as live migration of virtual machines, fault recovery, watchdog, and fault resetting were also conducted successfully, with the system reliability meeting the requirements of the electric power SCADA system. According to this experiment, the electric power SCADA system based on the cloud computing platform has the following advantages:

- Through the cloud computing virtualization technology, system platform resources can be flexibly allocated according to the data traffic of the power grid.
- Parallel data acquisition systems are used to significantly reduce hardware thresholds, improve data acquisition capacity, simplify future system expansion, and effectively improve system resource utilization.
- Parallel real-time data processing systems and distributed data storage are used to greatly improve data processing capabilities.
- Application software, storage, and data resources are provided as services, and resource utilization costs are decreased substantially by taking full advantage of cloud computing.
- The cloud computing virtualization technology reduces the coupling between resource users and resource implementation, so that users are no longer dependent on specific resource implementation, and the system administrator can reduce the impact of IT resource maintenance and upgrade on users.
- Throughout the experimental test, only a system administrator is needed for maintenance, significantly reducing the time required for maintenance.

5 Prospects of Cloud Computing Technology Application in the Electric Power SCADA System

5.1 Benefits Brought by the Cloud Computing Platform Deployed in the Electric Power SCADA System

The overall performance of the electric power SCADA system based on the cloud computing platform is much higher than that of the traditional IT platform. It can be seen from application analysis calculation of telecom operators that the average resource utilization of IT systems on traditional platforms is lower than 30%, and that on cloud computing platforms exceeds 60%. It takes 2–4 hours for terminal operation and maintenance through traditional PCs, and only a few minutes for VM maintenance based on cloud computing platforms. The average service launch period has also been shortened from 1–3 months on traditional platforms to 1–3 weeks on cloud computing platforms. The energy consumption of VM private cloud terminals is reduced by over 70% than traditional PCs. The cloud computing platform has higher data security than traditional IT platforms because of centralized data management and control. The customer experience on cloud computing platforms has been optimized significantly. Users only need to focus on business implementation, and corresponding hardware, software installation, operation and maintenance, and operating systems are maintained on the platform in a unified way, avoiding repeated work of professional users. In a word, the electric power SCADA system based on the cloud computing platform will help electric power industry customers reduce overall costs and improve efficiency.

5.2 Feasibility of Cloud Computing Platform Deployment in the Electric Power SCADA System

Technical feasibility: This experiment shows that the cloud computing platform meets the adaptability, real time, and reliability requirements of the electric power SCADA system, is in line with technological development trends and market demands, and therefore is technically feasible.

Economic feasibility: The features of the cloud computing platform, such as efficient resource usage, reduced energy consumption, and efficient maintenance, are in line with the requirements of power grids for upgrade, business continuity, rapid deployment of new services, and overall cost reduction.

Security feasibility: The security of electric power SCADA system based on professional private cloud platform is guaranteed and has been strengthened with cloud security functions.

6 Conclusion

In this paper, we describe the goals, contents, and results of the experimental study on the cloud computing–based electric power SCADA systems, and indicates that the professional private cloud computing platform meets the technical, economic, and security requirements of the electric power SCADA system, and has commercial feasibility. The electric power SCADA system is a typical application in the real-time industrial production control field. The results of this experimental study shows that industrial SCADA software systems can be deployed on similar professional private cloud platforms. The professional private cloud solution facilitates the application of

cloud computing technologies in the professional real-time production control field, and brings economic and social benefits for industrial production.

References

[1] T. Fusheng, *Power System Dispatching Automation and Energy Management System*. Chengdu, China: Sichuan University Press, 2004.
[2] Z. Mingguang, *Electric Power System Telecontrol and Dispatching Automation*. Beijing, China: China Electric Power Press, 2010.
[3] Z. Yongjian, *Electric Power System Monitoring and Dispatching Automation*. Beijing, China: Electric Power Press, 2004.
[4] X. Yaozhong, S. Junjie, and Z. Jingyang, "Technology development trends of Smart Grid dispatching and control systems," *Automation of Electric Power Systems*, vol. 39, no. 1, pp. 3–6, 2015, doi: 10.7500/AEPS20141008024.
[5] Z. Junhua, W. Fushuan, X. Yusheng, and L. Zhenzhi, "Cloud computing: Implementing an essential computing platform for future power systems," *Automation of Electric Power Systems*, vol. 34, no. 15, pp. 1–7, 2010.
[6] W. Kaifeng, L. Wantao, and L. Yanhu, "Cloud computing-based power big data analysis technology and its application," *China Power*, vol. 48, no. 2, 111–113.
[7] E. Thomas, M. Zaigham, and P. Ricardo, *Cloud Computing Concepts, Technology and Architecture*. Beijing: China Machine Press.
[8] S. Zhihao, M. Feng, and J. Hongcheng, "Research on application of resource pool virtualization technology," *Electric Power Information and Communication Technology*, vol. 13, no. 3, pp. 39–43, 2015.
[9] W. Zhimin and X. Bo, "Study on provincial power grid enterprise data center platform based on cloud computing," *Electric Power Information and Communication Technology*, vol. 13, no. 3, pp.14–18, 2015.
[10] C. Y. Yuesong, Z. Jia, and D. Haiting, "Information data center management supported by cloud platform," *Electric Power Information and Communication Technology*, vol. 12, no. 7, pp. 79–82, 2014.
[11] C. Yang, G. Zhiyuan, and Y. Shengchun, "Application of cloud computing in power dispatching systems," *China Power*, vol. 45, no. 6, pp.15–16, 2012.
[12] H. Zhixin and L. Lian, *Research on Smart Grid dispatching system based on cloud computing*. Tianjin: Tianjin University of Technology, 2014.
[13] Z. Yihui. "*Research on the operation dispatching technology system of Smart Grid based on cloud computing*," *China Electric Power Education*, no. 15, pp. 151–152, 2011.
[14] L. Lixin, D. Fangchun, L. Qiang, and H. Jing, *Retrieved from Outstanding IT-Based Achievements of the Electric Power Industry*. Beijing: China Electricity Council.

Manuscript received: 2015-07-01

Biographies

Yongbo Chen (chen.yongbo212@zte.com.cn) received the bachelor degree in water conservancy and hydroelectric engineering from North China University of Water Resources and Electric Power. He is now the senior engineer of ZTE Smart Grid Industry Planning. His research interests include the integration of smart grid and M-ICT technology integration innovation R&D.

Jijun Chen (chen.jijun@zte.com.cn) received his master's degree in electrical engineering in control Theory and Application Department from Automatic Control, Northwestern Polytechnic University in 2002. He is now the chief engineer of ZTE Government & Enterprise business department. His research engaged in advanced information and communication technologies in the field of smart grid application research and planning.

Jiafeng Gan (ganjiafeng@dongfang-china.com) graduated from Hefei University of Technology in 1998, and received his master's degree from Tianjin University Computer Science in 2007. He is the senior engineer of Yantai Dongfang Electronics Co., Ltd.. His research mainly engaged in the research and development of electric power SCADA system.

Call for Papers

ZTE Communications Special Issue on
Security and Privacy in Communications

Modern communication allows billions of objects in the physical world as well as virtual environments to exchange data with each other in an autonomous way so as to create smart environments. However, modern communication also introduces new challenges for the security of systems and processes and the privacy of individuals. There is an increasing demand for development of new security and privacy approaches to guarantee the security, privacy, integrity, and availability of resources in modern communication.

This feature topic will benefit the research and development community towards identifying challenges and disseminating the latest methodologies and solutions to security and privacy issues in modern communication technologies. Its objective is to publish high-quality and practical articles presenting open issues, algorithms, protocols, policies, frameworks, standards, systems, and solutions for communication related to security and privacy. All received submissions will be sent out for peer review by at least two experts in the field and evaluated with respect to relevance to the special issue, level of innovation, depth of contributions, and quality of presentation. Reviews and case studies, which address state-of-art research and state-of-practice industry experiences, are also welcome. Guest editors will make an initial determination of the suitability and scope of all submissions.

Paper Submission

Please send your manuscripts in pdf format to the Guest Editors (wanlei.zhou@deakin.edu.au and CC to g.min@exeter.ac.uk). Your papers should be no more than 25 pages double-spaced or 10 pages single-spaced and double columns.

Timetable

Paper Submission Due: December 1, 2015.
Confirmation of acceptance: February 1, 2016
Final Manuscript Due: March 1, 2016
The publication is scheduled on June 2016.

Guest Editors

Professor Wanlei Zhou, School of Information Technology, Deakin University, Australia (wanlei.zhou@deakin.edu.au)

Professor Geyong Min, Department of Mathematics and Computer Science, University of Exeter, UK (g.min@exeter.ac.uk)

DOI: 10.3969/j. issn. 1673-5188. 2015. 03. 006
http://www.cnki.net/kcms/detail/34.1294.TN.20150917.1628.002.html, published online September 17, 2015

A General SDN-Based IoT Framework with NVF Implementation

Jie Li[1], Eitan Altman[2], and Corinne Touati[2]
(1. Faculty of Engineering, Information and Systems, University of Tsukuba, Ibaraki 305-8577, Japan;
2. National Research Institute in Computer Science and Control (INRIA), Le Chesnay 78153, France)

Abstract

The emerging technologies of Internet of Things (IoT), software defined networking (SDN), and network function virtualization (NFV) have great potential for the information service innovation in the cloud and big data era. The architecture models of IoT, SDN with NFV implementation are studied in this paper. A general SDN-based IoT framework with NFV implantation is presented. This framework takes advantages of SDN and NFV and improves IoT architecture.

Keywords

Internet of Things; saftware defined networking; network function virtualization

1 Introduction

The Internet of Things (IoT) is a paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of smart things or devices such as radio-frequency identification (RFID) tags, sensors, actuators and smart mobile phones through unique addressing schemes for interacting with each other and cooperating with their neighbors to reach common goals in an intelligent way [1]. Advancement in wireless networking has let these thousands of smart devices connect to the internet anywhere and anytime. With the development of IoT, the amount of data produced per day increases exponentially [1], [2].

In today's cloud computing and big data era, most of computing and communication resources are shared and provided to users. This era has the characteristics of diversity, dynamics, and big data explosion, and brings a big challenge for the design of IoT architecture.

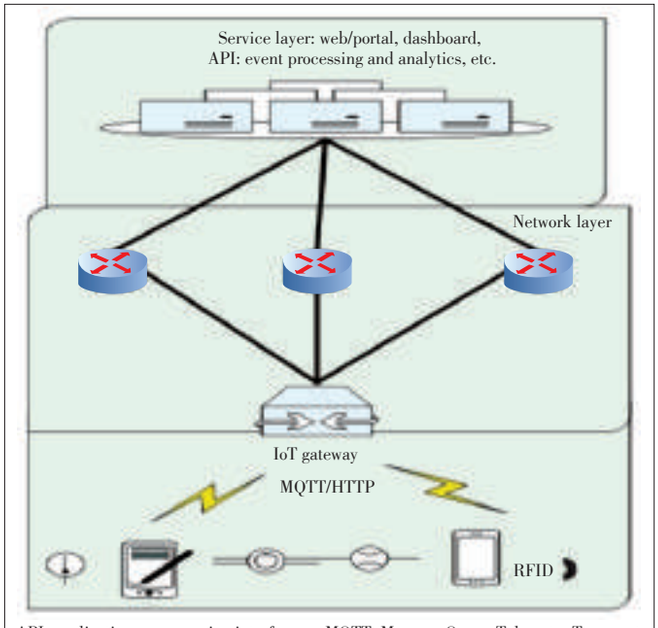
Current networks should be more intelligent, more powerful, more efficient, more secure, more reliable, and more scalable to meet the requirements of diversity and dynamics. The software defined networking (SDN) [3] and network functions virtualization (NFV) [4], [5] are two promising technologies for addressing the challenges and leveraging IoT architecture in the cloud era.

In this paper, we present a general SDN-based IoT framework with NFV implementation.

The rest of paper is organized as follows. Section 2 describes the conventional IoT architecture. Section 3 introduces the concepts of SDN and NFV and the design problems. Section 4 presents a general SDN-based IoT framework with NFV implementation. Section 5 concludes the paper.

2 IoT Architecture Models

Several IoT architecture models have been proposed [1], [6], [7]. These exiting IoT architecture models focus on different application aspects related to IoT. In this paper, we want to study the impacts of SDN and NFV on the IoT architecture. We divide the IoT architecture into the sensing layer, network layer, and service layer based on [6], [7] (**Fig. 1**).



▲**Figure 1. IoT architecture.**

The sensing layer includes sensing devices such as sensors, actuators, and RFID. These devices are usually not expensive but smart enough for sensing. They sense and collect data from different physical, human, and natural worlds in an intelligent and collaborative way, and store the collected data in the devices with small amount of memory.

The collected data are then transmitted to the gateways for wireless transmission. The gateways usually use Message Queue Telemetry Transport (MQTT) protocol or Hypertext Transfer protocol (HTTP). Since the amount of sensed and collected data may be large, the data compression and aggregation methods are necessary for efficient data transmission. The network layer includes the gateways and the routes for data transmission from gateways to different application users.

The service layer provides information services according to requirements. This layer includes powerful data centers and different data servers for data mining, analysis, processing, storage, and applications.

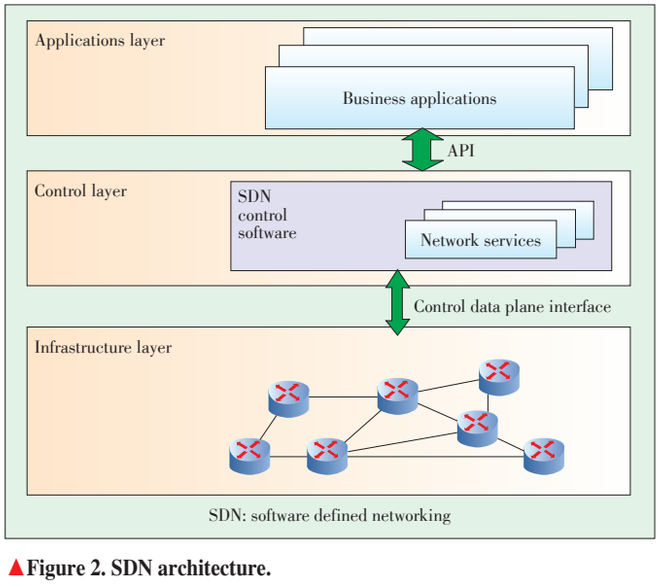
3 SDN and NVF Overview

SDN [8]–[10] is a novel networking paradigm. It separates the system and makes decisions where traffic is sent (the control plane) from the underlying system that forwards traffic to the selected destination (the data plane). In traditional routers and switches, the control and data planes are in one device. However, the separation of the control and data planes enables network more flexible, manageable, and adaptable, which meets the requirements of current applications for high-bandwidth, dynamic performance [3]. The Open Networking Foundation (ONF) [3] takes the leading role in SDN standardization, and has defined an SDN architecture model as depicted in **Fig. 2**. This model consists of the application layer, control layer, and infrastructure layer. End-user business applications are on the application layer and use SDN communications services. The control layer uses SDN controllers to provide the logically centralized control functionality that supervises the network forwarding behavior through an open interface. The infrastructure layer consists of the network elements (NE) and devices such as switches and routers which belong to the data plane. Packet switching and forwarding are implemented at this layer.

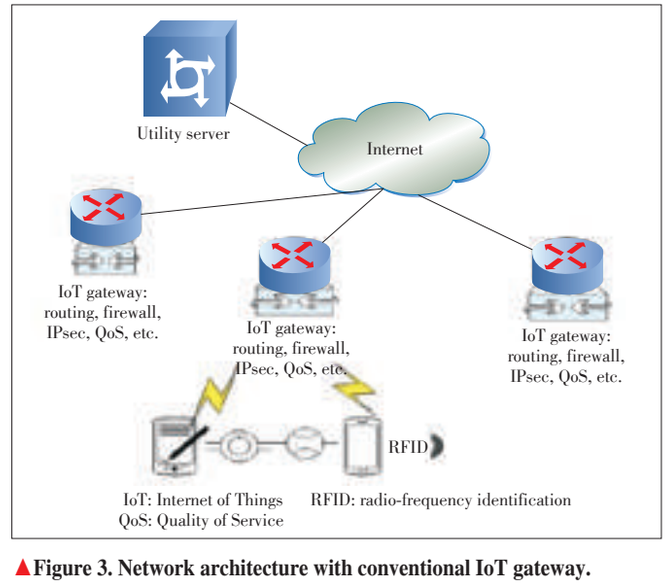
NFV [4], [5] is a network architecture concept that uses IT virtualization related technologies to virtualize entire network functions into building blocks. These blocks may be connected, or chained, to create communication services. An NFV system uses one or more virtual machines to run different software and processes on network servers, switches, storage, and even cloud computing infrastructure. In this way, the hardware does not need to be customized for each network function. Introduction of NFV and SDN to the IoT framework can leverage the network efficiency and implement the programmability and flexibility of networks [5], [11], [12]. For example, the OpenFlow-based SDN (SDN-OF) technologies, with NFV implementation, can achieve the IoT networking functions such as routing, access control in firewalls, secure tunneling between IoT gateway and utility server in IPSec protocol, and prioritizing critical and control traffic for QoS in a centralized programmable controller [12]. **Fig. 3** shows the network architecture with conventional IoT gateways. **Fig. 4** shows network architecture using SDN-OF and NFV technologies. The efficiency and network agility of IoT can be leveraged significantly by the network function virtualization of an SDN-based IoT framework.

4 A General SDN-Based IoT Framework with NFV Implementation

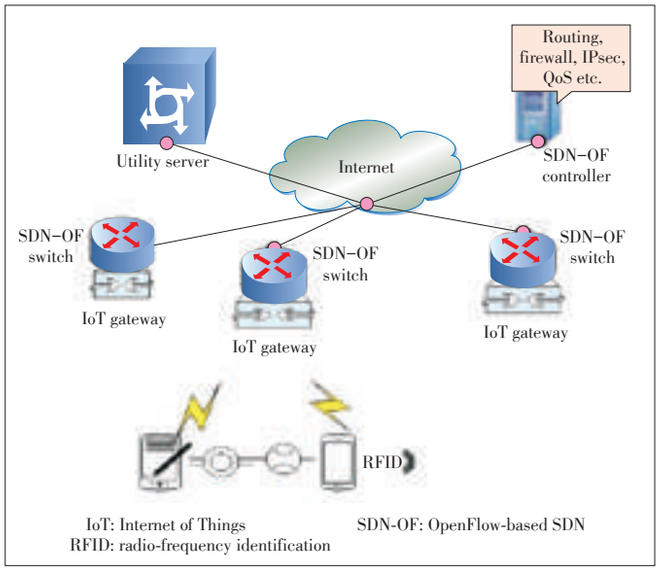
In SDN architecture, the controller is very important. It



▲Figure 2. SDN architecture.



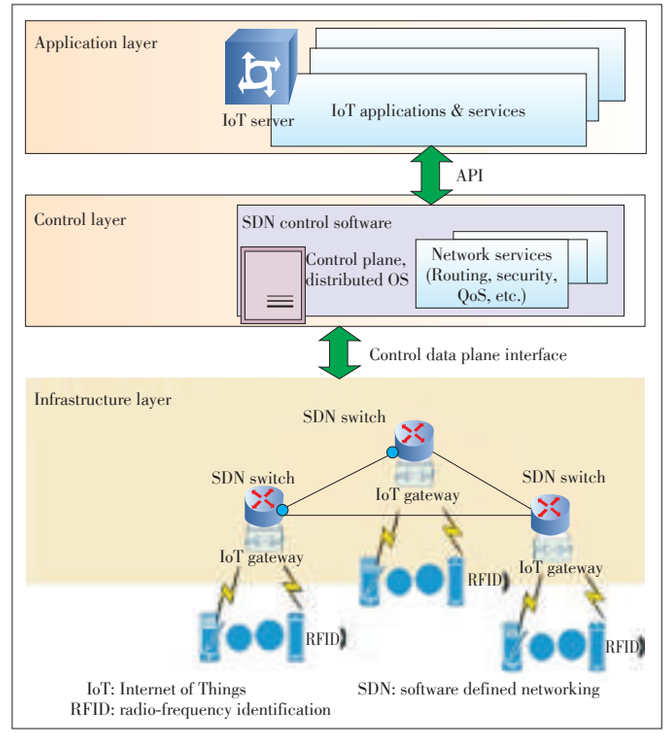
▲Figure 3. Network architecture with conventional IoT gateway.



▲Figure 4. Network architecture using SDN-OF and NFV technologies.

deals with networking services such as routing, firewall, load balancing, QoS, and charging for the whole network. A centralized controller for a network overall controls the whole network. This is a desirable characteristic for system implementation and development. It is clear that a centralized controller cannot provide all the networking services when the size of a network becomes large [13], [14]. Hu *et al.* [13] provides a survey of controllers and proposed methods for enhancing controllers' performance. Xavier and Seol [14] mention that placement of controllers in a SDN network can be centralized, physically distributed, hierarchically distributed, and logically distributed briefly. Kang *et al.* [9] presents a rule-placement algorithm that distribute data forwarding policies while managing rule-space constraints across general SDN networks in a logically centralized way. Voellmy *et al.* [15] presents an efficient programming model to design algorithms for SDN control. An interesting idea about the SDN-based framework combing 4G cellular networks for machine-to-machine communications is presented in [8]. The proposed framework depends on a specific 4G cellular network architecture. An extended Multinetwork Information Architecture (MINA) with layered SDN controller is proposed for IoT [16]. However, the research works has not studied the general IoT architecture using SDN and NFV.

Based on the study of IoT architecture, SDN architecture, NFV technologies, we propose a general SDN-based IoT framework with NFV implementation (**Fig. 5**). In the framework, the application layer consists of IoT servers for different applications and services through APIs. The control layer consists of SDN controllers run by distributed operating system (OS). The distributed OS provides a logically centralized control and view of IoT in a physically distributed network environment for network data forwarding. The infrastructure layer consists of IoT gateways combined with SDN switches for access to different IoT devices such as RFIDs and sensors through the control data plane interface. It can be treated as an extension of the SDN architecture for IoT.



▲Figure 5. A general SDN-based IoT framework with NFV implementation.

An efficient distributed OS for the SDN-based IoT plays an important role in the proposed general SDN-based IoT framework. The distributed OS in the control plane is the brain of SDN-based IoT with NFV implementation and provides a centralized control and visibility of different IoT services. Because of the diversity and dynamics of different users and infrastructures in IoT, designing and implementing an efficient distributed OS for this framework is a big challenge. Recently, many SDN associations such as OpenFlow and ONF are trying to make the standardization of the APIs in order to address the issue. NOSIX [17] has been proposed to achieve the portability and performance across different SDN switches. It provides a lightweight portability layer for the SDN OS. The Open Network Operating System (ONOS) project [18] aims at releasing a basic SDN-based distributed OS. The important issues of performance, scalability, and availability of the SDN control plane have been addressed in [19] and [20]. The design and implementation of an efficient distributed OS for the SDN-based IoT are ongoing.

5 Conclusion

The emerging technologies of IoT, SDN, and NFV have great potential for the information service innovation in the cloud

and big data era. Decoupling the control plane from the data plane in SDN architecture achieves centralized system and control of IoT. However, the design of an efficient SDN-based IoT architecture with NFV is a big technical challenge. In this paper, we provide a brief up-to-date overview of IoT architecture model, SDN, and NFV. We study the characteristics of these emerging technologies. A general SDN-based IoT framework with NFV implantation is presented. As a future work, we will study the organization and components of each part in the SDN-based IoT framework.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. doi: 10.1016/j.comnet.2010.05.010.
[2] D. Giusto, A. Iera, G. Morabito, and L. Atzori, *The Internet of Things*, Berlin, Germany: Springer, 2010.
[3] *SDN Architecture*, *Issue 1*, ONF TR-502, Jun. 2014.
[4] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: a survey," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 24–31, Nov. 2013. doi: 10.1109/MCOM.2013.6658648.
[5] Open Networking Foundation. (2014, Feb. 17). *OpenFlow-Enabled SDN and Network Functions Virtualization* [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf
[6] P. Fremantle. (2014, May25). *A Reference Architecture for the Internet of Things* [Online]. Available: http://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things/
[7] IoT-A. (2015). *Internet of Things-Architecture* [Online]. Available: http://www.iot-a.eu/public
[8] G. Savarese, M. Vaser, and M. Ruggieri, "A software defined networking-based context-aware framework combining 4G cellular networks with M2M," in *Proc. 16th International Symposium on Wireless Personal Multimedia Communications*, Atlantic, USA, pp. 1–6, June, 2013.
[9] N. Kang, Z. Liu, J. Rexford, and D. Walker, "Optimizing the 'one big switch' abstraction in software-defined networks," in *Proc. 9th International Conference on Emerging Networking Experiments and Technologies*, Santa Barbara, California, USA, 2013, pp. 13–24. doi: 10.1145/2535372.2535373.
[10] D. Kreutz, F. M. V. Ramos, P. Verissimo, *et al.* (2015). *Software-Defined Networking: A Comprehensive Survey* [Online]. Available: http://arxiv.org/abs/1406.0440
[11] Open Networking Foundation. (2013, Sept. 30). *SDN in the Campus Environment* [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-enterprise-campus.pdf
[12] V. R. Tadinada, "Software defined newtorks: redefining the future of internet in IoT and cloud era," in *Proc. International Conference on Future Internet of Things and Cloud*, Barcelona, Spain, 2014, pp. 296–301. doi: 10.1109/FiCloud.2014.53.
[13] F. Hu, Q. Hao, and K. Bao, "Survey on software-defined network and OpenFlow: from concept to implementation," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, May 2014. doi: 10.1109/COMST.2014.2326417.
[14] H. F. Xavier and S. Seol, "A comparative study on control models of software-defined networking (SDN)," *Contemporary Engineering Sciences*, vol. 7, no. 32, pp. 1747–1753, 2014. doi: 10.12988/ces.2014.411234.
[15] A. Voellmy, J. Wang, Y. R. Yang, *et al.*, "Maple: simplifying SDN programming using algorithmic policies," in *Proc. ACM SIGCOMM 2013*, Hong Kong, China, pp. 87–98.
[16] Z. Qin, G. Denker, C. Giannelli, *et al.*, "A software defined networking architecture for the internet-of-things," in *Proc. IEEE Network Operations and Management Symposium*, Krakow, Poland, pp. 1–9, May, 2014. doi: 10.1145/2535372.2535373.
[17] M. Raju, A. Wundsam, and M. Yu, "NOSIX: a lightweight portability layer for the SDN OS," *ACM SIGCOMM Computer Communication Review*, vol. 44, no.2, pp. 29–35, April 2014. doi: 10.1145/2602204.2602209.
[18] ONOS. (2015). *Open Network Operating System Project* [Online]. Available: http://onosproject.org
[19] ONOS. (2015, Apr. 6). *Raising the Bar on SDN Control Plane Performance and Scalability* [Online]. Available: http://onosproject.org/wp-content/uploads/2014/11/Whitepaper-ONOSBlackbirdperformance-generalaudience-Apr-7.pdf
[14] ONOS. (2015, Apr. 6). *Raising the Bar on SDN Control Plane Performance, Scalability, and High Availability* [Online]. Available: http://onosproject.org/wp-content/uploads/2014/11/PerformanceWhitepaperBlackbirdrelease - technical.pdf

Manuscript received: 2015-03-19

Biographies

Jie Li (lijie@cs.tsukuba.ac.jp) received his ME degree in electronic engineering and communication systems from China Academy of Posts and Telecommunications and Dr. Eng. degree from the University of Electro-Communications, Japan. He is a full professor with Faculty of Engineering, Information and Systems, University of Tsukuba, Japan. His current research interests include mobile distributed computing and networking, big data and cloud computing, OS, and modeling and performance evaluation of information systems. He is a senior member of IEEE and ACM, and a member of Information Processing Society of Japan (IPSJ). He is the Chair of Technical Sub-Committee on Big Data (TSCBD), IEEE Communications Society. He has served as a secretary for Study Group on System Evaluation of IPSJ and on several editorial boards for the international Journals, and on Steering Committees of the SIG of System EVAluation (EVA) of IPSJ, the SIG of DataBase System (DBS) of IPSJ, and the SIG of MoBiLe computing and ubiquitous communications of IPSJ. He has also served on the program committees for several international conferences such as IEEE INFOCOM, IEEE GLOBECOM, and IEEE MASS.

Eitan Altman (Eitan.Altman@inria.fr) received his BA degree in physics (1984) and the PhD degree in electrical engineering (1990), from the Technion-Israel Institute, Israel. He has been a researcher at National Research Institute in Computer Science and Control (INRIA) in Sophia-Antipolis, France since 1990. His research interests include network engineering games and social networks and their control. He is the editorial board member of several scientific journals including *Wireless Networks*, *Computer Networks*, *Computer Communications*, *J. Discrete Event Dynamic Systems*, *SIAM J. of Control and Optimisation*, *Stochastic Models*, and *Journal of Economy Dynamic and Control*. He received the best paper awards at the conferences of Networking 2006, Globecom 2007, IFIP Wireless Days 2009 and CNSM 2011 (Paris). He received the Grand Prix de France Telecom from the French Academy of Sciences in 2012.

Corinne Touati (Corinne.Touati@inria.fr) obtained her MS from Telecom INT, France in 2000, and PhD from University of Nice Sophia-Antipolis, France in 2003. She is a tenured INRIA researcher at Grenoble, France since 2006. Her research interests include performance evaluation, continuous and stochastic optimization, game theory and learning theory in communication networks and distributed systems. She has published over 40 research articles in peer-reviewed journals and conferences. She also worked at University of Tsukuba, Japan for three years.

DOI: 10.3969/j.issn.1673-5188.2015.03.009
http://www.cnki.net/kcms/detail/34.1294.TN.20150522.0920.001.html, Published online May 22, 2015

Crawler for Nodes in the Internet of Things

Xuemeng Li, Yongyi Wang, Fan Shi, and Wenchao Jia
(Department of Computer Science, Electronic Engineering Institute, Hefei 230037, China)

Abstract

Determining the application and version of nodes in the Internet of Things (IoT) is very important for warning about and managing vulnerabilities in the IoT. This article defines the attributes for determining the application and version of nodes in the IoT. By improving the structure of the Internet web crawler, which obtains raw data from nodes, we can obtain data from nodes in the IoT. We improve on the existing strategy, in which only determinations are stored, by also storing downloaded raw data locally in MongoDB. This stored raw data can be conveniently used to determine application type and node version when a new determination method emerges or when there is a new application type or node version. In such instances, the crawler does not have to scan the Internet again. We show through experimentation that our crawler can crawl the IoT and obtain data necessary for determining the application type and node version.

Keywords

crawler; local storage; nodes; Internet of Things

1 Introduction

With the fast development and increasing popularity of the Internet of Things (IoT), more and more devices are being used in everyday life and are being incorporated into the Internet. Such devices are also called nodes. Because these nodes are exposed to the Internet, they are not as safe many of the owners and users of these nodes think. The ability to connect to, communicate with, and remotely manage an incalculable number of networked, automated devices via the Internet has become pervasive. As we become increasingly reliant on intelligent, interconnected devices in everyday life, protecting billions of these devices from intrusion and interference has become a serious issue. Unauthorized intrusions can compromise personal privacy or even public safety [1]. Vulnerability is related to the application and many of the affected devices as possible in order to give warnings and manage the problem. In this paper, we describe a crawler for nodes in the IoT. This crawler is based on local storage. By collecting and storing information about the nodes' features, we can determine the application and version of individual nodes locally and conveniently.

ZoomEye [2] and Shandon [3] are two mature search engines that enable web users to search for application type and version. Using a distributed web crawler, ZoomEye collects information from Internet nodes all over the world. The ZoomEye interface enables the user to search for application, version, location, open port, and so on. The nodes from which this information is collected include websites and devices. Shodan, by contrast, is only focused on IoT device. It is used to expose vulnerabilities in routers, switches, and industrial control systems [2] and is often seen as a valuable tool for hackers. Shodan can be used to detect just about anything on the Internet, such as printers that can be controlled remotely; open, accessible web cameras; and other unsecured devices.

A popular strategy for determining the node application and version is first to crawl the Internet and then directly use the downloaded information. Then, the determinations are stored, and the raw information is abandoned. If there is a new strategy for determining the application and node version or if there is a new node application or version, the only thing that can be done it to scan the Internet a second time in order to retrieve the raw information again. This significantly increases scanning costs. We improved the existing web crawler by putting the NoSQL database to use. Our proposed distributed web crawler can retrieve fingerprint information in the IoT. The raw information returned by crawler is stored in the NoSQL database and used to determine the node application and version. The NoSQL database has high storage capacity, which the crawler demands, but does not occupy much of the system. Because it can search big data efficiently, the NoSQL database might be helpful for searching through the innumerable results returned by the web crawler [3], [4].

In section 2, we introduce MongoDB and traditional web crawler. In section 3, we describe the overall system structure, crawler design, data structure, local storage, and design of the database. In section 4, we experiment on our proposed crawler and show that it is efficient enough to satisfy the system requirements.

2 Related Works

2.1 MongoDB

The company 10gen develops the MongoDB, which is a doc-

This research work is supported by the ZTE Corporation and University Joint Research Project under Grant No. CON1307100001, and the National High Technology Research and Development Program of China under Grant No. 2013AA013602.

ument-oriented NoSQL database, not a traditional relational database. Although it is non-relational, MongoDB is faster, more expansible, and has more useful than a relational database [5]. MongoDB has many more functions than a relational database, including sorting, secondary indexing, and range searching [6]. Mongo DB has the following features:

- binary JavaScript object notation (BSON) for data storage. This increases the speed of index page traversal.
- non-relational storage and support for sharding. With sharding, big data is automatically divided into small data blocks that are then stored in an appropriate server. Although separate, user searching and combining of results can be done in a highly efficient way, and servers can linearly increase expandability and performance.
- flag_id as the only flag of the document. The value of this flag can be automatically assigned by the database or assigned by users themselves.
- a combination of key and value as the means of storing data. This is a loose-storage solution that makes inserting data into MongoDB easier than inserting data into a relational database. In this way, a user does not need to define the detailed table structure in advance, which is necessary in a relational database.
- no support for transactions. MongoDB sacrifices transactional support for easy use, high speed, and expandability.

2.2 Principle of the Traditional Web Crawler

A web crawler is a computer program used to downloading the source page of a website. Web crawlers are widely used in Internet search engines or for managing web page caches [7]. Crawling usually starts from one URL or a collection of URLs. Crawlers store these URLs permanently in a queue. Guided by a priority principle, a web crawler selects one URL from the URL queue and downloads the corresponding web page. If there are any other URLs in the web page, crawler extracts these URLs from the page after it has been downloaded. These extracted URLs are also stored in the queue. The downloading and extracting process loops until the web crawler is turned off, and downloaded pages are stored in the server database.

3 System Design

3.1 Background Requirements

The system must have a web crawler and database storage. As much as possible, the web crawler must crawl nodes on the IoT and grab information that is as complete as possible. Information stored locally in the database must be easy to understand, convenient to search, and useful for determining the application type and node version. At the same time, the crawling depth and width of the web crawler must be guaranteed.

A distributed web crawler is necessary to ensure high crawling speed and in-depth crawling. Web crawlers are now very cooperative with each other, and a scheduling relationship can be established between multiple web crawlers.

Traditional web crawling technology must also be improved so that traditional web crawlers can be used to grab specific information from nodes in the IoT. The information from these nodes can be used to determine the application type and node version in the future work.

MongoDB is necessary to store the collected information locally. Because the web crawler is distributed and MongoDB does not support transactions, independent MongoDB interfaces must to be designed for database reading and writing. In this way, MongoDB remains consistent.

Local storage is necessary for storing the information downloaded by the web crawler. Local storage enables the application type and node version to be determined locally, and scan time can be saved.

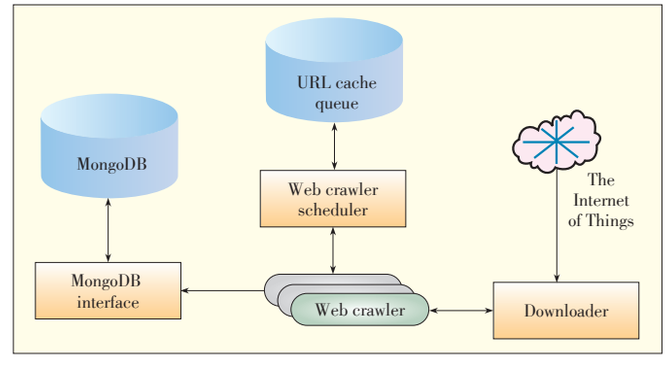
3.2 Overall Design

The system structure that best satisfies the previously mentioned requirements is shown in **Fig. 1**.

Within this system, the web crawler scheduler selects a URL from the URL cache queue, which has been sorted, and assigns the URL to a free web crawler. The web crawler crawls the web and downloads information from web pages or pages returned by devices. At the same time, the downloader also deletes duplicate useless webpages. Finally, the web crawler delivers the downloaded information to the MongoDB interface, which converts the information to BSON format and stores it. The web crawler scheduler, URL cache queue, and the web crawler can inherit the ones in mature crawler, so they are not covered in this paper.

3.3 Downloader Design

The IoT can be divided into public IoT and special IoT. In the former, all devices are connected. Public IoT covers one whole area of administration and connects to the public Internet. Public IoT is regarded as a true social information infrastructure [8]. Each sensor and entity connected to the IoT corresponds to one web source defined by a web page URL and can be accessed by HTTP protocol. All these web sources can



▲Figure 1. Overall system structure.

be expressed as HTML pages and are usually regarded as sensor pages or entity pages. These pages contains the type of the nodes, reading of the nodes, and some unstructured information [9]. Devices that can only be accessed with administrator privileges will return the administration web pages or error pages. These pages can also be used as the fingerprint of the device. By downloading the information included in these web pages, we can determine the application type and node version.

Our proposed downloader is different from a traditional downloader in three ways:

- Our proposed downloader scans more ports. The downloader of the traditional web crawler mainly scans ports 80 and 8080 whereas the downloader of our web crawler aimed at the IoT also scans ports such as 21, 22, and 23.
- The content downloaded by our proposed downloader is different. The downloader of a traditional web crawler downloads texts, pictures, files, and so on whereas the content downloaded by the web crawler of our proposed system only includes information useful for determining the application type and node version.
- Before our downloader downloads information, it has to determine whether the node belongs to the IoT or not.

The content downloaded by our web crawler aimed at the IoT must be useful for determining the application type and node version. After analyzing existing fingerprint-judging software, we realized that there was much more information that could be used to determine the application type and node version than we initially thought. We need to find out as much as possible about the node's fingerprint as accurately as we can and consider the load of the web crawler and capacity of MongoDB. We also need to download the URL address, header of the HTML page, body of the HTML page, banner information, and the geographic location. The downloader should also remove duplicates of the pages and complete cleaning of the content. The system needs to be capable of incremental crawling from time to time to obtain complete and accurate node data.

3.4 Local Storage of Node Data

Raw data from nodes is commonly used to determine the application type and node version but is not stored. The downloaded data is used as soon as it is downloaded, and after a determination has been made, only the application type and node version are stored in the database. However, a problem emerges when a new method is introduced for determining application type and node version or if there is a new application type or node version. To maintain the integrity of the database, devices should be scanned a second or even third time to obtain data, then the new approach is used to judge these devices. This "directly using without storing" method wastes scanned data and creates more scanning workload.

In terms of storing data, the system must avoid repetitive work. Our system stores the raw information downloaded by the downloader but stores it separately from the determinations. While the crawler is crawling devices, the data returned is directly passed to MongoDB and stored locally. The application type and node version are determined locally and independently. In the future, when derminations are being made about devices, regardless of whether or not the determination is made successfully, the raw information will be kept in MongoDB. If a new method for determining application type or node version emerges or if there is a new application type or node version, the only solution is to iterate through the database and obtain the fingerprint data of scanned devices.

3.5 Data Structure and Design of MongoDB

3.5.1 Data Structure

The data downloaded by the downloader must be stored in MongoDB in a certain format. After removing duplicates, the data is converted into BSON format by MongoDB interface and then stored in the database. The data to be downloaded includes URL address, header of the HTML page and so on.

3.5.2 Design of MongoDB

The collection obtained by MongoDB is similar to the table of a relational database. However, the definition of the collection is not as strict as that of a table. The MongoDB collection only comprises similar elements. Each data item in the collection is called a document. In our system, we create one document for every IP address. The fixed data structure of every document is shown in **Table 1**. Because MongoDB does not strictly define the collection, we can improve the downloader according to the background requirements. The structure of MongoDB does not need to change obviously. The design of MongoDB is shown in **Fig. 2**.

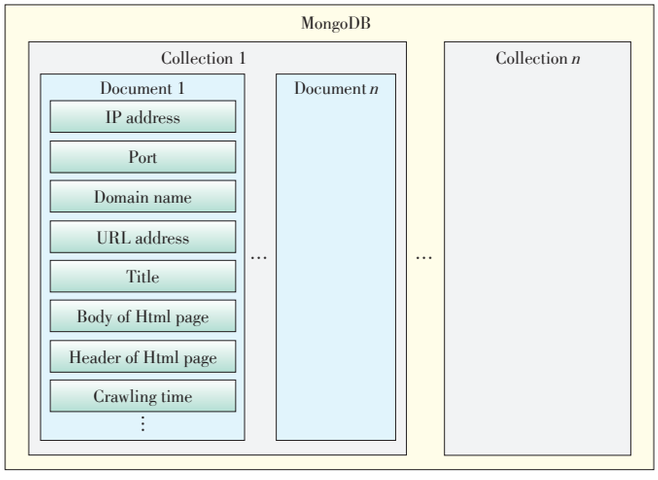
4 Realization of the Key Technology

4.1 Dividing Web

For N web pages, by using some certain dividing rule, the

▼Table 1. Data structure

Field	Data type	Description
ipAddr	string	IP address
Port	string	Port
Domain	string	Domain name
UrlAddr	string	URL address
Title	string	Title
htmlBody	string	Body of HTML page
htmlHead	string	Header of HTML page
HTTPheader	string	HTTP header
UpdateTime	datetime.utc	Time of crawling converted into utc timestamp
Location	string	Geographic location of nodes



▲Figure 2. Design of MongoDB.

collection G of web pages to be downloaded is divided into M (where $M > N$) subsets: $\{G_1, G_2, \ldots, G_M\}$. If $G_1 \cup G_2 \cup \ldots \cup G_M = G$, $G_1 \cap G_2 \cap \ldots G_M = \varphi$, and $|G_i| \approx |G_j|$, then G is called a division of N. Reasonable division of web pages prevents agents belonging to the system from crawling the same pages and increases the overall efficiency of web page crawling. The system uses dynamic distribution. At the start of a crawling job, the system distributes 1 to N subsets of web pages to N agents for crawling. Once an agent has finished crawling, the system distributes the next subset of web pages to the crawler. This distribution lasts until the end of the crawling job. To increase the efficiency of web crawling, the crawler should crawl web pages as close to it in network as possible. Therefore, a threshold timeout value is set for every agent. During crawling, if the time to connect to the web server exceeds the timeout threshold, the crawler will give up trying to connect. The agent will keep these URL addresses in its own list, and after a specified period, will pass the list to the system scheduler. This scheduler will re-schedule the nodes that the crawler could not connect to.

The advantage of dynamic distribution is that the load can be dynamically balanced and the agent is not turned down mistakenly [10].

4.2 Agent Synergy

Division of web pages requires the synergy of every agent in the system. To adapt to the strategy of web page division, our system synergizes with a scheduler. Each agent passes URL addresses that have been newly crawled to the scheduler, which distributes them in a uniform way. At the same time, the scheduler re-schedules nodes that the crawler could not connect to. Agent synergy is useful for controlling the division of web pages but overloads individual nodes and causes single-node failure [10].

An exchange approach is used to deal with links that cross the subset of the division. If an agent finds a URL that does not belong to its division subset, it passes the URL address to the crawler responsible for it.

4.3 Incremental Crawling

To ensure the integrity of the fingerprint database, incremental crawling is required. The easiest method of incremental crawling is to crawl pages again every specified period. However, doing this requires huge effort. Web pages are updated at different times, and some pages may not be updated for a long time. Therefore, the update period for web pages must be considered in the incremental crawling strategy. Among nodes in the IoT, there are important nodes whose accuracy must be guaranteed. As in [11], we categorize the nodes in the IoT as very important, important, general, or not important. The attribute of incremental crawling is the weighted average of the quantized importance and the update frequency. The incremental crawling attribute of all the nodes in the IoT is calculated to obtain the average. If a node has a higher-than-average incremental crawling attribute, the system crawls that node three times faster than average. If a node has a lower-than-average incremental crawling attribute, the system crawls that node at a speed 0.8 times the average.

5 Experiments and Conclusion

The performance of our web crawler under experimentation was affected to an extent by network bandwidth and hardware. We used Windows 7; internal storage was 2 GB; hard drive capacity was 250 GB; and network bandwidth was 100 Mbps. If the thread count of the distributed web crawler for the IoT is set to 10, 1085 URL address can be accessed in ten minutes. The downloaded information from 114 of these URL addresses belonged to nodes in the IoT. We used mature software to determine the application type and node version from this downloaded information. Fifty-six nodes were determined correctly, 49 of which included the application type.

After the web crawler had crawled the Internet and downloaded information from nodes over a period of time, we tested the local storage. MongoDB containing the raw crawling data was put into use in this experiment. We selected vulnerability CVE-2015-2049 published on 2 March 2015 in the China National Vulnerability Database [12]. This vulnerability in a D-Link DCS-931L remote wireless cloud camera with firmware 1.04 or earlier is an intermediate risk. Unrestricted file upload vulnerability in the camera allows a remote unauthenticated user to execute an arbitrary code by uploading a file with an executable extension [13]. In the previous identification for fingerprint, the application type and node version related to this vulnerability were not determined. To monitor the posture of the vulnerability, the application type and version need to be determined. First, we need to find fingerprint used for the determination. After information has been collected from the Internet,

the fingerprint is defined by the keyword SCS-931L in the WWW-Authenticate field of the HTTP header. After constructing a query statement for MongoDB and searching for the results in the raw information database, several results were returned (**Fig. 3**). The time cost for this search was less than 2 s,

▲**Figure 3. The search result of D-Link DCS-931L.**

which is much faster than crawling the Internet and collecting information a second time.

References

[1] *Security in the Internet of Things* [online]. Available: http://www.Windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
[2] *The instruction to Shodan* [online]. Available: http//: drops.Wooyun.org/1tips/2469
[3] Y. Gu, S. Shen, and G. Zheng, "Application of NoSQL database in web crawling," *International Journal of Digital Content Technology and its Applications*, vol. 5, no. 6, pp. 261—266. 2011.
[4] H. Dong, A. Wu, Q. Wu, and X. Zhu, "A novel distributed web crawling approach based on Mongodb," *International Journal of Advancements in Computing Technology (IJACT)*, vol. 5, no. 6, pp. 794—801. 2013.
[5] H. David, P. Eelco, M. Peter, and H. Tim, *The Definitive Guide to MongoDB, Second Edition*. Beijing, China: tsinghua university press, 2015, pp. 4—8.
[6] H. Li, *Design and Implementation of Crawler System for Public Feelings on Internet*. Xia Men, China: Xia Men University, 2014.
[7] P. Zhao, *Design and Implementation of Distributed Books Web Crawler System*. Cheng Du, China: Southwest Jiaotong University, 2014.
[8] S. Shen, Y. Mao, Q. Fan, P. Zong, and W. Huang, "The concept model and architecture of the internet of things," *Journal of Nanjing University of Post and Telecommunication (Nature Science)*, vol. 30, no. 4, pp. 3—8, 2010.
[9] Z. Wang, Q. Pan, and T. Xing, "Survey on real-time search engine for entities of internet of things," *Application Research of Computers*, vol. 28, no. 6, pp. 2001—2010, 2011.
[10] X. Xu, W. Zhang, H. Zhang, and B. Fang, "WAN-based distributed web crawling," *Journal of Software*, vol. 21, no. 5, pp. 1067—1082, 2010. doi: 10.3724/SP.J.1001.2010.03725.
[11] X. Su, *The Research, Implement on Technology of Distributed Web Crawler*. Harbin, China: Harbin Institute of Technology, 2006.
[12] *Vulnerability summary for CVE-2015-2049* [online]. Available: https//:web.Nvd. Nist. gov/view/vuln/detail? vulnId=CVE-2015—2049
[13] *Cross-site request forging loophole of D-Link-DCS-931L* [online]. Available: http//:www.cnvd.org.cn/flaw/show/CNVD-2015-01375

Manuscript received: 2015-04-22

Biographies

Xuemeng Li (benqer@126.com) received her BS degree in computer science from Electronic Engineering Institute. She is currently a graduate student at the Electronic Engineering Institute, Hefei. Her research interest is computer security.

Yongyi Wang (rose_1203@yeah.net) is a professor of computer science at the Electronic Engineering Institute. He receives his graduate degree at the Electronic Engineering Institute. His research interest is computer security.

Fan Shi (shif00@gmail.com) received his master's degree in computer science from Electronic Engineering Institute. He now works in Electronic Engineering Institute. His research interests include networks and search engine.

Wenchao Jia (jiatoday2013@163.com) received his master's degree at the Electronic Engineering Institute. He is currently a PhD candidate there. His research interests include networks and big data.

Call for Papers

ZTE Communications Special Issue on

Vehicular Communications, Networks, and Applications

Vehicular communications and networking can improve road safety, facilitate intelligent transportation, support infotainment, data sharing, and location based services, and will be a critical component in the Internet of Things. This special issue aims to present the state of the art in research and development of vehicular communication technology and its potential applications. We are soliciting original contributions. The topics of interest include, but are not limited to:

- Vehicle-to-vehicle and vehicle-to-infrastructure transmissions, DSRC, channel models, and mobility models;
- Vehicular networking protocols, vehicular/cellular interworking, user privacy protection, and network information security;
- Road safety, data offloading, data sharing, remote diagnosis, platooning, cooperative driving, driving assistance, vehicle traffic monitoring and management;
- Standardization, regulations, testbed, prototyping, human machine interfaces, and pilot systems.

Paper Submission

Please directly send to Li Zhu (zhu.li1@zte.com.cn) and copy to both guest editors, with subject title "ZTE-VCN-Paper-Submission".

Tentative Schedule

Paper submission deadline: January 1, 2016
Editorial decision: April 1, 2016
Final manuscript: May 1, 2016

Guest Editors

Prof. Weihua Zhuang, University of Waterloo, Canada (wzhuang@uwaterloo.ca)

Prof. Hongzi Zhu, Shanghai Jiaotong University, China (hongzi@cs.sjtu.edu.cn)

DOI: 10.3969/j. issn. 1673-5188. 2015. 03. 008
http://www.cnki.net/kcms/detail/34.1294.tn.20150918.1645.002.html, published online September 18, 2015

An Improved Wireless Sensor Network Routing Algorithm

Shengmei Luo[1], Xue Li[2], Yiai Jin[1], and Zhixin Sun[2]
(1. ZTE Corporation, Shenzhen 518057, China;
2. School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract

High performance with low power consumption is an essential factor in wireless sensor networks (WSN). In order to address the issue on the lifetime and the consumption of nodes in WSNs, an improved ad hoc on-demand distance vector routing (IAODV) algorithm is proposed based on AODV and LAR protocols. This algorithm is a modified on-demand routing algorithm that limits data forwarding in the searching domain, and then chooses the route on basis of hop count and power consumption. The simulation results show that the algorithm can effectively reduce power consumption as well as prolong the network lifetime.

Keywords

wireless sensor network; low power consumption; lifetime; AODV; LAR

1 Introduction

Wireless sensor networks (WSN) consist of a large number of cheap micro sensor nodes that are deployed in the examination area, aiming at forming a multi-hop self-organization network system by wireless communication [1]. Applied to WSN, the ad hoc on-demand distance vector routing (AODV) [2] protocol is a typical on-demand routing protocol. It is a combination of dynamic source routing (DSR) [3] and destination sequenced distance vector (DSDV) [4]. AODV borrows the basic programs of route discovery and route maintenance from DSR, and Hop-by-Hop route, destination node serial number and periodic update mechanism in routing maintenance phases from DSDV.

One major disadvantage of WSN is the energy limitation of its nodes. However, AODV does not consider a node's current residual energy when it establishes routing. Much research has been done to improve the AODV protocol by solving the problem of energy consumption in WSN. The existing research work has just paid attention to controlling the number of packets in the process of establishing routing, or focused on the energy consumption of nodes and the path load. In fact, the improvement is not ideal. In this paper, we propose an improved ad hoc on-demand distance vector routing (IAODV) algorithm based on the existing location-aided routing (LAR) routing protocol to reduce the number of route request (RREQ) packets. The IAODV algorithm uses the improved routing control packets and streamlined routing tables and route request tables. It simplifies the route discovery process and reduces the number of routing control packets and the power consumption of the network. This algorithm also uses the path selection function that takes the hop and energy consumption into account. This function helps optimize the power consumption of sensor network nodes and prolong the lifetime of the network.

2 Related Work

Location-based routing protocols, such as geographical adaptive fidelity (GAF) and geographical and energy aware routing (GEAR) [5], [6], need to wake up the sensor nodes nearest to the tracking target in an application that wants to obtain information related to the target position. The Greedy Perimeter Stateless Routing (GPSR) [7] protocol is a typical location-based routing protocol. Its main strategy is to choose the node that is closest to the sink nodes as the next hop in every jump. Network nodes then use the classical flooding routing protocol [8] to forward packets in the form of broadcast. This protocol is based on flooding, so the signaling overhead is huge.

Combining the location-based routing protocol and flooding routing protocol, the LAR routing protocol is proposed in [9]. LAR uses the location information to restrict the flooding range of query packets. Based on the concept of expectation domain, location information is used to restrict the flooding range of RREQ, reduce the number of broadcast packets, reduce the power consumption of the network, and improve the network performance [9], [10]. These proposed routing protocols use a series of mechanism to reduce the number of packets transferring in the network in order to make routing overhead relatively small. However, they do not take the network nodes' limited energy into account, so network nodes cannot efficiently send packets in the limited lifetime of the network.

An enhancement to the AODV routing protocol is proposed

This work is supported by the National Natural Science Foundation of China under Grant Nos. 61373135, 60973140, and 61170276, Key University Science Research Project of Jiangsu Province under Grant No. 12KJA520003, Project for Production Study & Research of Jiangsu Province under Grant No. BY2013011, and The Science and Technology Enterprises Innovation Fund Project of Jiangsu Province under Grant No. BC2013027.

in [11]. It uses cluster-based mechanism to support congestion control in a mobile ad hoc network (MANET). The main feature of this approach is clustering and the selection of the cluster head is on the basis of the congestion status of the nodes. This protocol is highly efficient in dealing congestion by achieving QoS constraints (good packet delivery ratio, low delay and reduction of packet drops), as well as energy efficient. However, it reselects the cluster head frequently due to the rapid energy consumption of the cluster head.

Energy values of the nodes and forwarding packets along the path of least energy consumption are evaluated in [12], making the network adaptive in nature. However, the influence of the hop count on energy consumption of the whole network is not fully considered in [12]. The distributed Dynamic Route Change Algorithm (DRCA) [13] dynamically finds a shorter route to the destination by using the hello message of neighbor in the AODV routing protocol. DRCA first changes the hello message format of AODV to make it contain the list of recently forwarded destination, hop count and sequence number. The nodes that receive this hello message decide whether they change the next hop to the destination or not by comparing the hop count and sequence number in their routing table to those in the received hello message. However, the impacts of power consumption of broadcast packets are ignored in [13]. A new maximum - energy Local Route Repair (LRR) approach with multicast AODV routing protocol is proposed in [14]. This repair mechanism provides each node in the network with route establishment capability. However, the impacts of power consumption of broadcast packets and transmission hops are also ignored in [14].

Based on the AODV protocol's routing selection criteria, the load path and the quality of the link are considered in [15] in order to save energy and prolong the network lifetime. Three factors of noise ratio, the number of active neighbor nodes and each node's queue state of filling are considered to improve the AODV protocol, and improve the performance of the network [15]. However, this method [15] may waste sources if it uses certain a path frequently and makes energy consume quickly while there is much left energy in other routes of the network. Piggyback and Weighted neighbor stability Ad hoc On-demand Distance Vector routing (PWAODV) [16] reduces the route cost and network delay effectively by using piggyback mechanism and weighted neighbor stability algorithm, However, the count of packets does not get good control in this method, which makes power consumption unsatisfactory. AODV++ protocol [17] establishes routes from the source node to the destination node according to the node's residual energy and traffic load, but it does not fully consider the influence of the hop count on the whole network's energy consumption.

In order to solving the problems of AODV and improved AODV protocols, we propose an improved routing algorithm—IAODV in this paper. The algorithm limits forwarding packets in a certain area, and uses the path selection function that considers the hop and energy consumption. It realizes the decrease of the packets number while reducing power consumption and prolonging the lifetime of wireless sensor network.

3 IAODV Algorithm

3.1 Format of Packets

3.1.1 Route Request (RREQ) Packets

On the basis of the original format of RREQ packets, the proposed RREQ packets (**Fig. 1**) remove five flags, transform the original reserved field to the distance field to record the distance from the current node to the destination node, and set up the energy field to record total nodes' residual energy in each routing path. At the same time, RREQ takes out the destination sequence number and originator sequence number field.

3.1.2 Route Reply (RREP) Packets

The format of RREP packets (**Fig. 2**) is basically consistent with RREQ packets. In RREP packets, the type field is set to 10, and RREP packets change the distance field of RREQ to

type	D	O	Distance	Hop count	Energy	RREQ ID	D address	O address

type (2 bit):01----route request (RREQ).
D (1 bit):0------D Address is a EUI-64 bit address.
1------D Address is a 16 bit short address.
O (1 bit):0------O Address is a EUI-64 bit address.
1------O Address is a 16 bit short address.
Distance (11 bit): the distance from the current node to destination node.
Hop Count (4 bit): hop count from the originating node to destination node.
Energy (5 bit): the sum of the total surplus energy from the originating node to destination node.
RREQ ID (8 bit): When the originating node creates a RREQ, RREQ ID plus 1; after destination node receives the RREQ, the route reply (RREP) takes corresponding RREQ ID.
D Address: the address of destination node.
O Address: the address of originating node.

▲**Figure 1. Route request packet format of IAODV.**

type	D	O	Reserved	Hop count	Energy	RREQ ID	D address	O address

type (2 bit):01----route request (RREQ).
D (1 bit):0------D Address is a EUI-64 bit address.
1------D Address is a 16 bit short address.
O (1 bit):0------O Address is a EUI-64 bit address.
1------O Address is a 16 bit short address.
Reserved (11 bit): It is set to zero and ignored when the node accepts.
Hop Count (4 bit): hop count from the originating node to destination node.
Energy (5 bit): the sum of the total surplus energy from the originating node to destination node.
RREQ ID (8 bit): When the originating node creates a RREQ, RREQ ID plus 1; after destination node receives the RREQ, the rout reply (RREP) takes corresponding RREQ ID.
D Address: the address of destination node.
O Address: the address of originating node.

▲**Figure 2. Route reply format of IAODV.**

the reserved field and set it to 0. The RREP ignores the reserved field when the node accepts RREP packets.

3.1.3 Route Error (RERR) Packets

RREQ removes the destination sequence number and originator sequence number field and switches to the path selection function for path selection. Therefore, as shown in **Fig. 3**, the proposed RERR packets, based on the original RERR packet format, take out the destination count and unreachable destination sequence number field. At the same time, RERR sets up the failing packet ID field to record the first packet sequence number that fails to send messages.

3.1.4 Routing Table and Routing Request Table

The IAODV routing table (**Fig. 4**) removes the source node serial number field, destination node serial number mark field, another state or routing marks field, the hop count from the source node to destination node field, and the forward pointer table field from AODV routing table. The IAODV algorithm uses the streamlined routing table and route request table, and simplifies the route discovery process.

Each node that receives RREQ puts the source node address and RREQ ID information into the routing request table (Fig. 4). The node automatically deletes entries in the routing request table if going beyond the time limit.

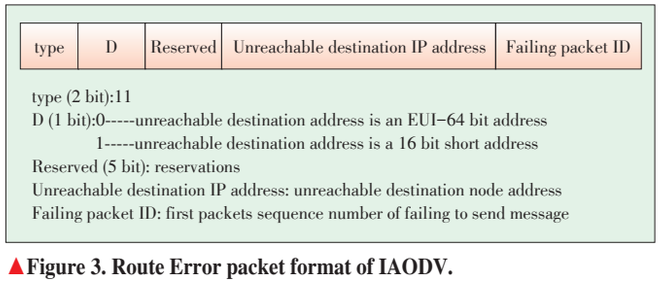
3.2 Routing Algorithm

The algorithm uses the distance strategy of the LAR control routing lookup strategy to determine the size of the search area. Looking for routing area is then limited to a small search domain, which reduces routing requests. The routing algorithm assumes that each node knows its own energy consumption in the network and that each node is fixed. In the initialization phase of the network, nodes in the network use GPS to determine their locations, and then send their own coordinates to the nodes within the scope of one hop. The form of flooding is kept until each node owns the entire topological graph of network.

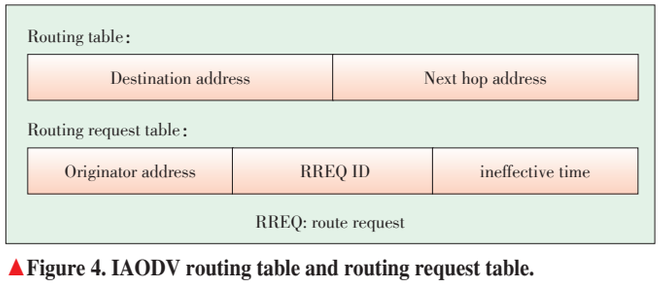
If the source node wants to send data to the destination node when there are no necessary items in the routing table, it needs to broadcast the RREQ packets to find the destination node. For each node that receives the RREQ, it first judges whether the RREQ is repetitive. Next decision is made only when the RREQ is not repetitive. If the node is in the request zone, it will forward the RREQ. If not, it does not do that. The number of RREQ packets sent by the node is reduced by this way. After the destination node receives the RREQ from the originating node, it sends a RREP packet to the source node conversely. Only the destination node can build the RREP. The intermediate node only broadcasts the RREQ, even though it knows the rout of the destination node. Therefore, the sent RREP packets are effectively reduced, and the problem of invalid RREP packets is avoided. A routing to the destination is built for the RREP packets that the destination node sends. These packets go through every intermediate node, and finally reach the source node. The RREP packets are then inspected if they match the RREQ. If not, the RREP is discarded. Conversely, the path selection function is used for sending data. If there is no appropriate routing within the fixed time, the originating node will expand the search range and broadcast the RREQ again. **Figs. 5 and 6** show the flow charts of RREQ and RREP routing.

When a link is disconnected, the node uses unicast to the source node for noticing the link failure. The RERR packets point out the unreachable destination nodes.

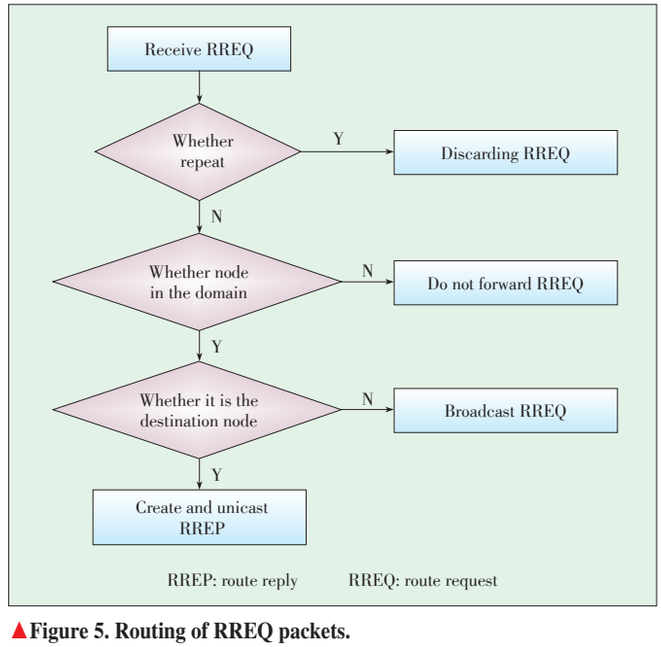
In **Figs. 7 and 8**, A is the source node and D is the destina-



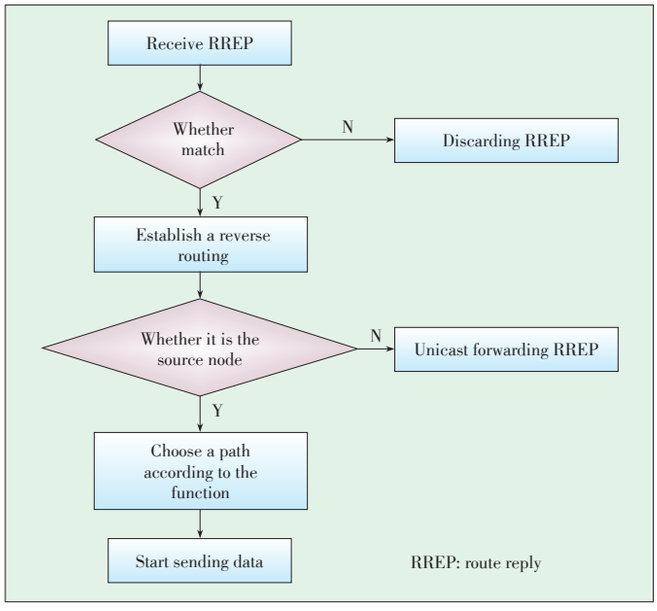
▲**Figure 3. Route Error packet format of IAODV.**



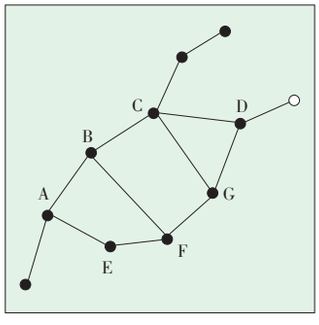
▲**Figure 4. IAODV routing table and routing request table.**



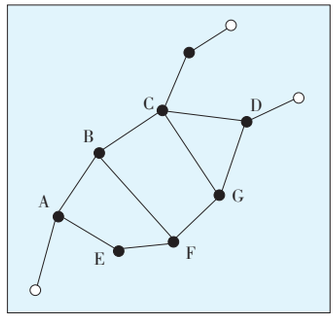
▲**Figure 5. Routing of RREQ packets.**



▲Figure 6. Routing of RREP packets.



▲Figure 7. Flooding.



▲Figure 8. Inhibition flooding.

tion node. Only the black nodes forward RREQ during the routing process. When Fig. 7 is compared with Fig. 8, it is seen that the inhibition flooding method can effectively reduce the number of RREQ packets. This is duo to in the process of inhibition flooding, routing area is limited to a small search domain, which reduces routing requests.

3.2.1 Path Selection

The power consumption of wireless sensors mainly includes consumption in perception, processing, communication, and positioning. Among them, the consumption of communication is the biggest of all. Each source node sends data to destination node consuming energy that is connected with the hop count. A path selection function is defined by the node's residual energy and hop count in the process of routing selection. A routing in which the nodes' average residual energy is biggest is selected as the best routing. In this way, the node's energy consumption is optimized and the network's lifetime is prolonged.

The IAODV related definitions are as follows.

Definition 1: a route is expressed as $r_i = a_1, a_2, ..., a_j$, where a_1 is the source node, a_j is the destination node, and N is the number of hops from the source node to destination node.

Definition 2: E_i is the residual energy of a_i, the average residual energy of each node on the route r_i:

$$f(r_i) = \frac{\sum_{i=1}^{j} E_i}{N+1} \quad (1)$$

Definition 3 (path selection function):

$$f(r_{\max}) = MAX\{f(r_i) | r_i \in R\} \quad (2)$$

where R is the set of all paths from the source node to the destination node.

Equations (1) and (2) show that the path that has more residual energy and less hops is more likely to be selected. When paths have the same residual energy, the path with the least hops is selected. When paths have the same hop count, the path with the most residual energy is selected.

4 Simulation Experiment

4.1 Simulation Environment

In order to verify the IAODV algorithm performance, we implemented a simulation experiment on the NS-2.35 simulation platform. The simulation parameters were set as shown in **Table 1**.

The simulation experiment evaluates the following indicators:

(1) The number of survival nodes, which reflects the lifetime of the network in different periods

(2) The rate of residual network energy, which is the proportion of the sum of all nodes' residual energy and the initial total energy and reflects the power consumption of the routing algorithm

4.2 Simulation Results and Analysis

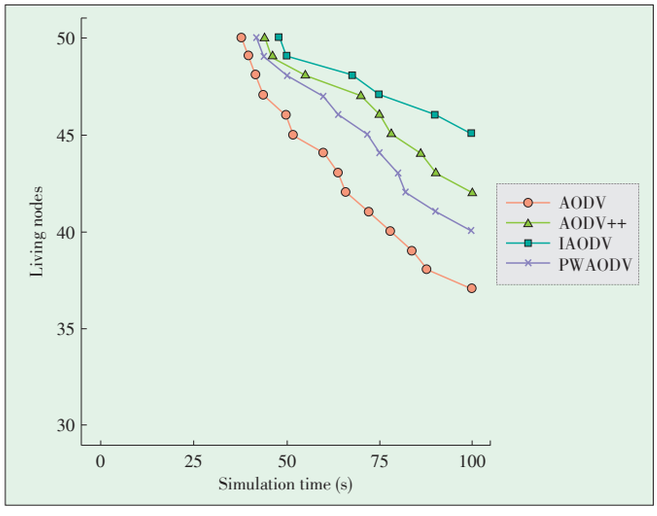
In the experiment, IAODV is compared with AODV, PWAODV [16] and AODV++ [17] in the same simulation environment.

According to the simulation results shown in **Fig. 9**, the polylines of the four algorithms coincide at 0–30 s. As the simulation time goes on, the number of survival nodes in the net-

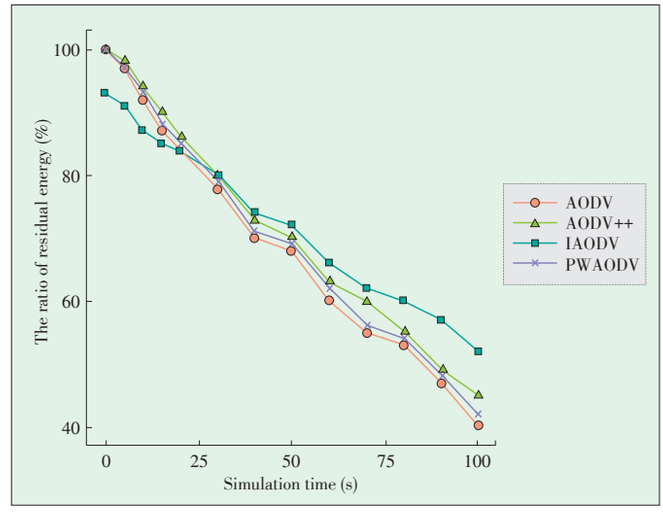
▼Table 1. IAODV simulation parameter values

Parameters	Values
MAC layer	IEEE802.15.4
The number of nodes	50
The size of the simulation platform (m×m)	50×50
Simulation time (s)	100
Transmission rate (k/bs)	250
Initial energy of nodes (J)	30
Transmission distance (m)	10

MAC: media access control



▲Figure 9. Living nodes.



▲Figure 10. The ratio of residual energy.

work tends to reduce no matter which protocol is adopted. With IAODV, the first node death time is at 50 s and there are five dead nodes at the end of the simulation. With AODV++, the first node death time is at 46 s and there are eight dead nodes at the end of the simulation. With PWAODV, the first node death time is at 44 s and there are 10 dead nodes at the end of the simulation. With AODV, the first node death time is at 40 s and there are 13 dead nodes at the end of the simulation.

The death time of nodes in the AODV-based network is the earliest and the number of dead nodes at the end of the simulation is also the most in this network, because the AODV protocol does not consider the energy consumption of nodes in the process of routing discovery. PWAODV uses piggyback mechanism and weighted neighbor stability algorithm to reduce the route cost and network delay effectively. The AODV++ protocol establishes routes from the source node to destination node according to the residual energy and traffic load of nodes. Compared with AODV, PWAODV and AODV++ have certain improvement in the energy consumption of the network. However, they fail to consider the influence of the hop count to the energy consumption of the whole network.

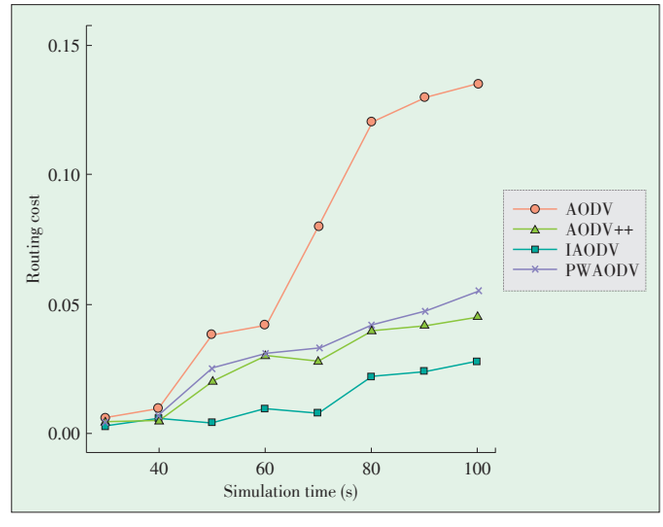
IAODV considers the hop count and energy consumption by using the path selection function. Compared to the other three protocols, it achieves the latest death time of nodes and the fewest dead nodes. In this way, the IAODV algorithm reduces the number of dead nodes in limited time and prolongs the lifetime of the network.

Fig. 10 shows that the ratio of residual network energy tends to reduce no matter which protocol is adopted. In an IAODV based network, the nodes first confirm their own locations by GPS and send the coordinate to all the nodes in one hop. Therefore, the ratio of residual energy is low at the initial stage of the simulation. According to Fig. 10, the residual energy ratio of the IAODV based network is higher than those of the networking using the other three protocols, and the gap becomes bigger as the simulation time goes on.

According to **Fig. 11**, the routing costs of the four protocols are small, when the number of nodes is small. However, with the increase of nodes, the routing cost of AODV dramatically increases. The increase of the routing costs of AODV++ and PWAODV is smaller than AODV. IAODV has the least increase of the routing cost because it optimizes the network routing process.

5 Conclusions

We propose IAODV, an improved routing algorithm, for realizing low power consumption and longer lifetime of WSN. The proposed algorithm combines the AODV and LAR routing protocols and gives full consideration to the network's energy consumption problem. According to the simulation results, this al-



▲Figure 11. Routing cost.

gorithm achieves the goal of improving the performance of the network and prolonging the lifetime of network.

References

[1] L. Sun, J. Li, and Y. Cheng, *Wireless Sensor Networks*, Beijing, China: Tsinghua University Press, 2005.
[2] *Ad Hoc On-Demand Distance Vector (AODV) Routing*, IETF RFC3561, Jul. 2003.
[3] *The Dynamic Source Routing Protocol (DSR) For Mobile Ad Hoc Networks For IPv4*, IETF RFC 4728, Feb. 2007.
[4] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *Computer Communication Review*, vol. 24, no 4, pp. 234–244, 1994. doi: 10.1145/190314.190336.
[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, Oct. 2002. doi: 10.1109/TWC.2002.804190.
[6] K. Akkaya, F. Senel, and B. McLaughlan, "Clustering of wireless sensor and actor networks based on sensor distribution and connectivity," *Journal of Parallel and Distributed Computing*, vol. 69, no. 6, pp.573–587, Jun. 2009. doi: 10.1016/j.jpdc.2009.02.004.
[7] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *6th Annual International Conference on Mobile Computing and Networking*, Boston, USA, 2000, pp. 243–254.
[8] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003. doi: 10.1109/JPROC.2003.814918.
[9] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," *Wireless Networks*, vol. 6, no. 4, pp. 307–321, Jul. 2000. doi: 10.1023/A:1019106118419.
[10] H. Asenov and V. Hnatyshin, "GPS-enhanced AODV routing," in *International Conference on Wireless Networks*, Las Vegas, USA, Jul. 2009, pp.1–7.
[11] N. Phate, M. Saxena, and M. A. Rizvi, "Minimizing congestion and improved QoS of AODV using clustering in mobile ad hoc network," in *Recent Advances and Innovations in Engineering*, Jaipur, India, May 2014, pp.1–5. doi: 10.1109/ICRAIE.2014.6909217.
[12] A. P. Patil, B. Varsha Chandan, S. Aparna, *et al.*, "An improved energy efficient AODV routing protocol for MANETs," in *Eleventh International Conference on Wireless and Optical Communications Networks*, Vijayawada, India, Sept. 2014, pp. 1–5. doi: 10.1109/WOCN.2014.6923063.
[13] Y. Choi, D. Kang, and S. Bahk, "Improvement of AODV routing protocol through dynamic route change using hello message," in *International Conference on Information and Communication Technology Convergence*, Busan, South Korea, Oct. 2014, pp. 117–121. doi: 10.1109/ICTC.2014.6983096.
[14] P. Jain and A. Suryavanshi, "Energy efficient local route repair multicast AODV routing schemes in wireless ad hoc network," in *International Conference on Advanced Communication Control and Computing Technologies*, Ramanathapuram, India, May 2014, pp. 1168–1173. doi: 10.1109/ICACCCT.2014.7019282.
[15] A. Singh, A. Konsgen, and C. Goerg, "Enhancing AODV performance by improved link metrics," in *5th International Conference on Information and Automation for Sustainability*, Dec. 2010, pp. 183–188. doi: 10.1109/ICIAFS.2010.5705657.
[16] N. Wang and Y. Cao, "An improved AODV protocol with lower router cost and smaller delay - PWAODV," in *Fourth International Conference on Intelligent Computation Technology and Automation*, Shenzhen, China, Mar. 2011, pp. 435–438. doi: 10.1109/ICICTA.2011.393.
[17] S. Ren, H. Han, B. Li, *et al.*, "An improved wireless sensor networks routing protocol based on AODV," in *12th IEEE International Conference on Computer and Information Technology*, Chengdu, China, Oct. 2012, pp. 742–746. doi: 10.1109/CIT.2012.153.

Manuscript received: 2015-04-02

Biographies

Shengmei Luo (luo.shengmei@zte.com.cn) received his master degree in communication and electronics from Harbin Instituted of Technology in 1996. He is the chief architect of the Cloud Computing and IT Institute of ZTE Corporation. His research interests include cloud computing, network storage, and big data.

Xue Li (lixue7168@163.com) is a graduate student in computer software and theory at Nanjing University of Posts and Telecommunications. Her research direction is software application technology based on computer networks.

Yiai Jin (jin.yiai@zte.com.cn) received his master degree in computer science from Jilin University in 2005. He is a senior engineer of ZTE Corporation. His research interests include cloud computing and security.

Zhixin Sun (sunzx@njupt.edu.cn) received his PhD degree in aeronautics and astronautics manufacturing engineering from the Nanjing University of Aeronautics and Astronautics in 1998. He is a doctoral supervisor at Nanjing University of Posts and Telecommunications. His research interests include computer application and network safety, multimedia communications, and Internet of Things.

DOI: 10.3969/j. issn. 1673-5188. 2015. 03. 007
http://www.cnki.net/kcms/detail/34.1294.TN.20150909.1509.006.html, published online September 9, 2015

Fast, Exact and Robust Set Operations on Polyhedrons Using Localized Constructive Solid Geometry Trees

Ping Lu[1], Xudong Jiang[2], Wei Lu[2], Ran Wei[1], and Bin Sheng[3]

(1. ZTE Corporation, Nanjing 210012, China;
2. Autodesk China Research & Development Center, Shanghai 200061, China;
3. Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract

Regularized Boolean operations have been widely used in 3D modeling systems. However, evaluating Boolean operations may be quite numerically unstable and time consuming, especially for iterated set operations. A novel and unified technique is proposed in this paper for computing single and iterated set operations efficiently, robustly and exactly. An adaptive octree is combined with a nested constructive solid geometry (CSG) tree by this technique. The intersection handling is restricted to the cells in the octree where intersection actually occurs. Within those cells, a CSG tree template is instanced by the surfaces and the tree is converted to plane-based binary space partitioning (BSP) for set evaluation; Moreover, the surface classification is restricted to the cells in the octree where the surfaces only come from a model and are within the bounding-boxes of other polyhedrons. These two ways bring about the efficiency and scalability of the operations, in terms of runtime and memory. As all surfaces in such a cell have the same classification relation, they are classified as a whole. Robustness and exactness are achieved by integrating plane-based geometry representation with adaptive geometry predicate technique in intersection handling, and by applying divide-and-conquer arithmetic on surface classification. Experimental results demonstrate that the proposed approach can guarantee the robustness of Boolean computations and runs faster than other existing approaches.

Keywords

Boolean operations; polyhedrons; constructive solid geometry; binary space partitioning tree

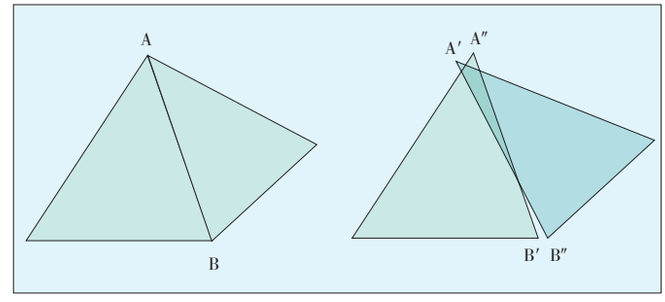
The work is supported by the Natural Science Foundation of China under Grant No. 61202154 and No. 61133009, the National Basic Research Project of China under Grant No. 2011CB302203, Shanghai Pujiang Program under Grant No.13PJ1404500, the Science and Technology Commission of Shanghai Municipality Program under Grant No. 13511505000, and the Open Project Program of the State Key Lab of CAD&CG of Zhejiang University under Grant No. A1401.

1 Introduction

Regularized Boolean operations [1] are defined as a closure of corresponding set-theoretic operations on the interior of two solids. The combination of set operations on polyhedrons, such as regularized union (U*), regularized intersection (∩*) and regularized difference (-*) can construct an arbitrary complex 3D model from simpler inputs. Thus, these operations have been widely used in interactive modeling systems, CAD/CAM applications, simulation systems and many other areas of computer graphics.

In order to evaluate the iterated set operations, an arbitrary set of polyhedrons is often organized into a constructive solid geometry (CSG) tree in which the leaf nodes are polyhedrons and the internal nodes are specific set operators. Then the evaluation of the CSG tree is generated by decomposing it into a combination of serial binary set operations with conventional methods.

The accumulation of numerical errors is introduced in the evaluation procedure of set operations. It often leads to system crashes or failure to generate correct result, such as holes and surface overlap (**Fig. 1**) when evaluating very complex models or when iterative set operations are required. Achieving geometric robustness by overcoming the problem is easy in the absence of efficiency. Thus, the major challenge of implementing such set operations is to take into account both robustness and efficiency for interactive applications. By carefully handling degeneracies and implementing set operations with arbitrary precision arithmetic, the algorithms [2]–[5] that can realize both goals have been proposed. However, they are too costly to be practical. In order to avoid these drawbacks, some methods [6]–[11] tried to implement set operations with voxels based on volumetric representations. However, all of these have to perform conversion between boundary representation (B-rep) and volumetric representation. Therefore, it is inevitable to lose geometric details and precision for input models in the conversion procedure. Another research stream for solving the robustness and exactness problem in set operations is to marry plane-based geometry representation and binary space partition (BSP) structure together with the adaptive geometry predicates technique [12], [13]. Nevertheless, the state-of-art BSP-based



▲**Figure 1. Topology inconsistency arising from accumulation of numerical error in Boolean operations.**

method [13] still suffers from robustness issues in some special cases because the method needs to split surfaces along with the boundary of critical cells, although the efficiency was improved by localized intersection handling. Moreover, in these methods, repetitive conversion between different representations and BSP merge operations may lead to robustness issues and poor performance when evaluating iterated set operations.

In contrast to B-rep-based methods [2], [3], [14], BSP-based methods have unique abilities for handling non-manifold surfaces and simplifying the procedure of processing all possible intersections and degeneracies among polyhedrons. Thus, the motivation of our study is to develop a fast and unified method for single and iterated set operations. This method can inherits the robustness and exactness of BSP-based approaches, and limits the cost of conversion between different representations.

In this paper, we exploit a new approach that uses localized CSG trees to efficiently compute Boolean operations on polyhedrons. Similar to the previous BSP-based work, our method implements robustness and exactness by integrating a plane-based geometry representation with adaptive geometry predicates technique. In order to significantly improve performance, we also apply an operation localization scheme to change the surface topology only at an intersection region. The surfaces at non-intersection region remain unchanged by employing a new adaptive octree construction algorithm which will be detailed discussed later. Unlike the method in [13], numeric errors are not introduced in the procedure of octree construction by avoiding split surfaces in ours. The main ingredient, which is the key to implementing the unified method for single or iterated set operations, is embedding a CSG tree into each octree cell where polyhedrons intersect with the help of an adaptive octree. Regularized set operations are evaluated on each CSG tree by converting it into a BSP tree and then extracting the boundary from the BSP tree.

A side effect caused by the operation localization scheme is that surface classification has to be performed for the polygon surface at non-intersecting regions. However, the procedure is quite time consuming when the number of those surfaces is very big. In order to improve classification efficiency, a partial surface classification scheme is employed based on the fact that classification of actual surfaces can be made only at the regions that are completely inside the bounding box of other polyhedrons, and the regions are covered by a set of octree cells. By classifying each cell as a whole, surface classification is further accelerated with the help of the octree. Through this divide-and-conquer strategy, the accuracy and robustness of classification is guaranteed because classification always performs between surfaces with original polyhedrons.

2 Related Work

Regularized Boolean operations have been investigated for many years. Corresponding methods can be classified into three categories: volumetric methods, approximate methods, and exact methods.

By converting B-rep into a volumetric representation, regularized set operations can be easily and robustly evaluated with voxels [6], [7]. However, the precision for models is inversely proportional to the size of voxel. Small voxels are quite expensive in terms of sampling time and memory consumption. Moreover, the sharp edges and corners of input models are lost in the converting process. In order to alleviate the problems, the methods in [8], [15] reconstruct the geometric details on surfaces of the resultant model by encoding the normal information of surfaces into the sampling process. Some [9]–[11], [16] also made efforts to preserve topology or manifold information in the results by applying dual-contour algorithms. Nevertheless, it is unavoidable for those methods to damage the geometric details and precision of the resulting models due to the conversion between different representations.

The performance penalty of exact Boolean operation is inevitable, so some researchers try to compute approximate Boolean operations instead. Biermann *et al*. [17] implemented approximated set operations on two free-form solids bounded by parametric surfaces based on a multi-resolution subdivision representation [18]. Robustness is achieved by applying the numeric perturbation [19] in intersection computation between the coarse meshes in the method. However, in the case when an intersection result is uncertain, the technology has to use new perturbation to compute the intersection again. Thus, the method is time-consuming for complex models. Smith and Dodgson [20] presented a topologically robust method for set operations on B-rep models. By carefully defining a series of interdependent operations, this approach can always guarantee the result with correct connectivity if the input models have valid connectivity. However, due to interdependent operations, this method cannot benefit from the power of parallel computation, which is common for modern processors,. Until recently, Wang [21] has proposed an approach to efficiently evaluate approximated set operations on two polygon meshes with the help of Layered Depth Images (LDI) [22]. A trimmed adaptive contouring algorithm is used to reconstruct the surfaces in the intersected region from the LDI/mesh hybrid, and then the surfaces are stitched together with the surfaces in non-intersected regions. In this way, the same robustness with that in the methods based on volumetric representation is obtained and geometric details are preserved at meaning time. Nevertheless, the trimmed adaptive contouring algorithm may damage the topological consistency of the resultant model.

The algorithms for exact Boolean operations have been accompanied with notorious robustness issues since they were introduced in 1980s [2]–[5]. Even though the arbitrary precision arithmetic and careful handling of degeneracies can be used in these algorithms to implement robustness, such implementations are too costly to be practical.

Naylor and Thibaut [23]–[25] have found that a BSP tree

can facilitate Boolean operations of manifold or non-manifold solids. They proposed a much simpler alternative algorithm for B-rep ones by converting Boolean operation into BSP structure merging. BSP-based methods avoid handling all possible intersections and degeneracies. However, this approach is fragile due to error accumulation in the merging stage. Sugihara and Iri [26] introduced plane representation for polyhedrons for solving the robustness issue with geometry computation. By representing polygons with a supporting plane and a set of bounding planes, the rudimentary modeling operation can robustly performs. In 2009, Bernstein and Fusel [12] combined these two methods—plane based geometry representation and BSP structure—together with the adaptive geometry predicates technique [27], and proposed a robust BSP-based Boolean operation method in the true sense. However, this approach spends too much time on pre-computation. Both the time and space complexity of the merging algorithm is almost $O(n^2)$, making it impractical for large scale meshes. A year later, Camped and Kobbelt [13] improved this approach by introducing operations localization scheme. The improved algorithm subdivides input polyhedrons by an adaptive tree and marks the cells in which operant polyhedrons intersect as critical cells. BSP merge is then performed only in those critical cells. This optimization dramatically saves time and memory space for plane-based BSP Boolean operation while keeping robustness. However, the approach still suffers from the robustness issue in some special cases because it needs to split surfaces along with the boundary of critical cells. Moreover, in these methods, repetitive conversion between different representations and BSP merge operations may lead to robustness issues and poor performance when evaluating iterated set operations.

3 Overview

Given any two polyhedrons P_i and P_j, the evaluation of regularized Boolean operations between them implies the selection of boundary surfaces according to following equations [28].

$$P_i \cup^* P_j = \{F_i\ Out\ P_j\} \cup \{F_j\ Out\ P_i\} \cup \{F_i\ With\ P_j\} \quad (1)$$

$$P_i \cap^* P_j = \{F_i\ In\ P_j\} \cup \{F_j\ In\ P_i\} \cup \{F_i\ With\ P_j\} \quad (2)$$

$$P_i -^* P_j = \{F_i\ Out\ P_j\} \cup \{F_j\ In\ P_i\} \cup \{F_i\ Anti\ P_j\} \quad (3)$$

The surfaces set F_x is the boundary surfaces of P_x. The classification sets $F_x OutP_y$, $F_x InP_y$, $F_x\ With\ P_y$, and $F_x AntiP_y$ correspond to the subsets of boundary surfaces F_x that are respectively outside, inside, on the boundary with same orientation, and on the boundary with an orientation opposite to the polyhedron P_y. Moreover, the boundary surfaces of P_x can be classified into the union of three kinds of disjoint sets, i.e. $Px = \{S_{in}, S_{out}, S_{intersected}\}$, $S_{in} \cap S_{out} = S_{in} \cap S_{intersected} = S_{out} \cap S_{intersected} = \varnothing$, where S_{in}, S_{out}, and $S_{intersected}$ correspond to the set of surfaces that are completely inside, outside, and intersect with the minimum Axis-Aligned Bounding Box (AABB) of other models respectively. Then through the use of the classification, F_x can be generated from the classification set S_{in}, S_{out}, $S_{intersected}$ respectively.

$$F_x = F_{x1} \cup F_{x2} \cup F_{x3},\ F_{x1} \subset S_{in},\ F_{x2} \subset S_{out},\ F_{x3} \subset S_{intersected} \quad (4)$$

Thus, the evaluation of regularized Boolean operations between P_i and P_j can be discomposed to three procedures:

- to get F_{x2} from S_{out} of each polyhedron through expression simplification rules given in **Table 1** since all surfaces in S_{out} are outside the others.
- to collect F_{x1} from S_{in} of each polyhedron by classifying surfaces in the set since they are either completely outside or inside the other polyhedrons.
- to obtain F_{x3} form $S_{intersected}$ of each polyhedron by intersection handling.

The same strategies can be adopted to the evaluation of regularized set operations based on a CSG tree. Given a CSG tree T and a set of polyhedrons $P_{i=(1..n)}$ in its leaf nodes, T can also be decomposed into the union of three disjoint sub-trees, i.e. $T = T_{in} \cup T_{out} \cup T_{intersected}$, where T_{in}, T_{out}, $T_{intersected}$ are CSG trees composed of S_{in}, S_{out}, $S_{intersected}$ from all polyhedrons respectively. A leaf node of any sub-tree can contain an empty surface set in case of the corresponding S is $\varnothing$. The evaluation of T can be simplified to the results collection of all sub-tree's evaluation. **Fig. 2** shows an example of CSG decomposition.

By using an octree, T can efficiently be decomposed into a series of sub-trees. Thus, our algorithm can compute set operations on a set of polyhedrons in four steps.

1) CSG tree construction

The first step of our algorithm is to convert input Boolean expression into a CSG tree in which the leaf nodes are polyhedrons and the internal nodes are specific Boolean operators. For single set operations, the CSG tree is trivial, which only has two leaf nodes and one non-leaf node.

2) Localized intersection handling

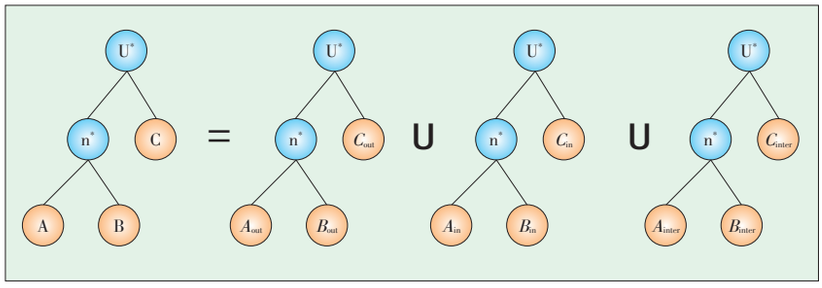
The purpose of this step is to decompose the CSG tree into disjoint sub-trees, and restrict intersection handling in the trees which contain the surfaces in an intersection region with

▼Table 1. Boolean operation simplification rules for the polygons outside other polyhedrons

Operation	Left operand	Right operand	Result
∪*	a	b	a ∪ b
∩*	a	b	∅
−*	a	b	a

* a and b mean the polygon from left polyhedrons and that from right polyhedrons respectively.

Fast, Exact and Robust Set Operations on Polyhedrons Using Localized Constructive Solid Geometry Trees
Ping Lu, Xudong Jiang, Wei Lu, Ran Wei, and Bin Sheng



▲Figure 2. An example of CSG tree decomposition.

the help of an adaptive octree. We first construct an octree to classify input polyhedrons into three kinds of nodes: internal nodes, external nodes, and intersected nodes (Section 4.1). Intersection computation is restricted to those intersected nodes where surfaces belong to at least two models. Before processing each intersected node, a CSG template is created based on the CSG tree constructed in the first step in order to improve performance (Section 4.2). Within each intersected node, all surfaces are converted to plane-based representation, then grouped according to the polyhedrons they belong to. If a surface spans at least two intersected nodes, the surface will be clipped along with six bounding planes of current node, and the remaining parts will associate to original surface. The CSG template is instanced with the grouped surfaces, then converted to BSP. The result of Boolean operations on the instanced CSG tree is obtained by extracting the boundary from the BSP.

3) Partial surfaces classification

In order to evaluate the CSG sub-tree where all surfaces are either entirely inside other models, or entirely outside other models, or on other models, we need to determine every surface relation with respect to other polyhedrons by a point-in-polyhedron test. Several strategies are employed in surface classification either to speed up the classification or to make the procedure robust. First, the classification is restricted to the internal nodes where surfaces only come from a model and are within the AABBs of other polyhedrons. All surfaces in each internal node are clustered as a whole for classification. The point-in-polyhedron test arithmetic based on spatial structure is then employed to further improve efficiency.

Distinct from conventional classification based on CSG, The divide-and-conquer method is used to achieve the robust and exact classification (Section 4.3).

4) Boolean operation result generation

The result of a Boolean operation is obtained by collecting the evaluation results from different CSG sub-trees. In this step, all surfaces in the intersected nodes and internal nodes are evaluated. Therefore, we only need to evaluate the set operations on the surfaces within external nodes where all surface only come from a model and are outside the AABBs of other polyhedrons. Knowing the relations of surfaces in each external node with respect to other polyhedrons, we can quickly evaluate those surfaces according to the simplification rules in

Table 1.

4 Localized Evaluation and Classification

4.1 Adaptive Octree Construction

In recent years, an adaptive octree has been employed to find intersected areas of input polyhedrons by several Boolean algorithms [13], [20], [27]. Different from those methods, the adaptive octree constructed in this paper allows a single surface to add into multiple nodes, which avoids the numerical error caused by clipping the surface during the tree construction. Meanwhile, the nodes of the octree are classified into three categories: external nodes, internal nodes, and intersected nodes, and different schemes for different nodes can be applied to accelerate the algorithm execution.

The adaptive octree algorithm takes all the surfaces of all polyhedrons as input, recursively subdivides the minimum AABB encompassing whole input polyhedrons along X axis, Y axis and Z axis of its Cartesian coordinates, and then classifies the surfaces according to the sub-bounding-boxes to generate the tree. Different from the conventional construction strategy, the procedure subdivides the current node if and only if the node contains surfaces from different models and the surfaces in the nodes exceed an adjustable parameter m. In this way, the octree can automatically adapt to the complexity of the model. During the generation period of the octree, each node is classified to one type of the following three categories:

- Intersected node: surfaces in the node belong to at least two models;
- Internal node: surfaces in the node only come from a model and are within the AABBs of other polyhedrons;
- External node: surfaces in the node only come from a model and are outside the AABBs of other polyhedrons.

All surfaces of the octree spread over the leaf nodes classified by spatial relation, and the surfaces in each leaf node are either entirely within the cell or intersected with it. Therefore, a surface can span multiple leaf nodes. To manage this case, our algorithm defines the priorities of different node types: the priority of an intersected node is higher than that of an internal node, while internal node is higher than external node. It means when a surface is shared by several nodes with different types, the surface is considered to belong to the node with highest priority and will be handled in this node. For example, if a surface is shared by an internal node and an external node, it will be handled in the internal node. To determine the ownership of each shared surface, those surfaces are set one of the following flags:

- Multi-intersected: the surface spans at least two intersected nodes.
- Single-Intersected: the surface only spans a intersected node;

- Internal: the surface can at least be shared by an internal node while cannot be shared by intersected nodes;
- External: the surface can only be shared by external nodes.

The four flags correspond to the node categories respectively. These flags define how to traverse the surfaces of the octree. When visiting external nodes, all the surfaces with single-intersected or internal flags are skipped because they are traversed by the corresponding intersected or internal nodes; the surfaces with multi-intersected flag are checked if and only if there are the remaining sub-surfaces after clipping. When visiting internal nodes, all single-intersected surfaces are skipped because they are traversed by the corresponding intersected nodes, and the surfaces with multi-intersected flag are processed as before. **Fig. 3** illustrates spatial subdivision on two 2D polygons by using adaptive octree.

The octree generated by this algorithm has three properties:

1) The internal and external nodes can only be leaf nodes, and only the intersected nodes may have children.

During the octree construction, the node is not be recursively subdivided unless it is an intersected node with the surfaces that exceed the threshold. This explains why the parent of an internal or external node can only be an intersected node, and the node cannot be subdivided any more.

2) All the surfaces within an internal node have the same relationship. They are either totally outside other models, or totally inside other models, or totally on the same surface with other models.

According to the definition and property 1, an internal node is a leaf node with all surfaces belonging to a single model. Assuming there exists a surface outside other models while the remaining surfaces are inside the model, those surfaces will cross the boundary of model, which means the surfaces intersecting with them are also in this node. This assumption does not meet the definition of internal node, so this propositions is true.

3) Only the surfaces of intersected nodes have the probability to intersect with other models.

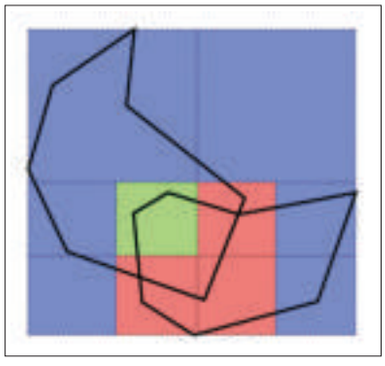
Assuming there is a surface in an internal or external node of the octree intersecting with models, the node contains surfaces from other models, or the surface is shared by a single/multi-intersected node. In the first situation, the node is an intersected node, unconformable to the assumption; in the second situation, the surface is handled by the intersected node, and this propositions is true.

The octree construction strategy implicitly divides the surfaces of each input model into three different regions: the intersected region, internal region, and external region. The regions consist of the surfaces from same model among all intersected nodes, all internal nodes and all external nodes respectively. **Fig. 4** shows an example of different regions on each polyhedron. Different strategies can be applied on the surfaces of different regions. In summation, the algorithm only needs to do the intersection handling on the surfaces of intersected regions, classifies the surfaces of internal regions, and directly evaluate the surfaces of external regions. The triangles from the exclusive group can be evaluated in early stage according to Table 1. Triangle-triangle intersection tests are limited to within each intersected group. A point-in-polyhedron test is performed for the triangulating results of every intersection test and performed only once for each inclusive group.

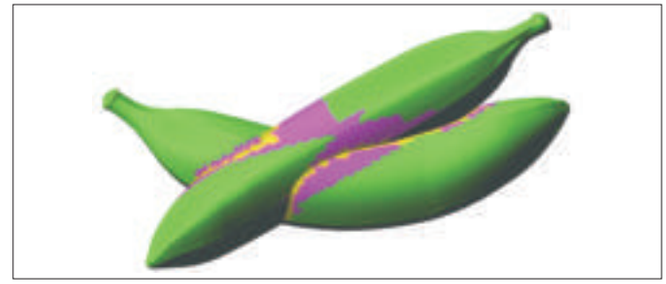
4.2 Localized Intersection Handling

In intersection handling, it is inevitable that operations change the topology of polyhedrons. By using predicates rather than constructions, it is easier to make the operations robust since no new geometric data are generated from existing geometric information [29]. Hence, vertex coordinates are not used in the operations such as intersection computation and clipping polygons, but the surfaces are converted to planed-based representation before further processing. The plane-based representation of a polyhedron consists of a support plane and a set of bounding planes. With the representation, a vertex of the polyhedron is defined implicitly by the intersections among the support plane and two bounding planes, while an edge is defined implicitly by the support plane and a bounding plane. Given a polygon $P=(V_1, V_2, \ldots V_n)$, where V_i is a vertex defined in counter clock wise order, we can get its plane-based representation $P=\{S, B_1, B_2, \ldots B_n\}$, where S is the support plane and B_i is a bounding plane by the plane equations in the forms:

$$f(S)=\left((V_3-V_2)\times(V_1-V_2)\right)\cdot(p-V_1)=0 \quad (5)$$



◀Figure 3. 2D illustration of subdividing two polygons by adaptive octree. Blue denotes exclusive cells; red denotes intersected cells; and green denotes inclusive cell.



▲Figure 4. An example of different regions on each polyhedron constructed by an adaptive octree. Green, pink and yellow denote the external, internal, intersected region respectively.

$$f(B_i)=\left((V_{i+1}-V_i)\times\left((V_3-V_2)\times(V_1-V_2)\right)\right)\cdot(p-V_i)=0 \quad (6)$$

where f is the implicit function of a plane and p is a point in the defined plane. Related geometric operations based on the representation were proposed in [12].

With the constructed octree, the intersection handling is restricted to the intersected nodes. Before processing intersected nodes, a CSG tree template is constructed in order to improve the efficiency in terms of runtime and memory. The CSG tree template is instanced by filling the polygons based on plane representation, and then converted to BSP for set operations evaluation in each intersected node. The evaluation results of are obtained by extracting the boundary from the BSP tree. The procedure is implemented in the three steps: constructing a CSG tree template, instancing the template in each intersected node, and converting CSG to BSP and extracting boundary.

4.2.1 Constructing CSG Tree Template

A general CSG template inherits the CSG tree constructed in the first step (Section 3). It is reused in the whole procedure of intersection handling, and instanced with the surfaces based on plane representation in each intersected node. In order to construct the template, we copy the original CSG tree, and replace the primitive in each leaf node with a pair of key-value, where the key is the identifier of the primitive while the value is a list of faces from each intersected node of the octree. **Fig. 5** shows a CSG tree template.

4.2.2 Instancing Template in Each Intersected Node

Within each intersected node, an empty group list is created corresponding to the set of input polyhedrons, and each group has a unique identifier for quickly finding the polyhedron where the surfaces in the group come from. A copy of each surface is converted into the plane-based representation, and then different processing strategies are taken according to surface flags. If a surface has a multi-intersected flag, the plane-based representation is clipped by six boundary planes of the cell by the clipping algorithm presented in [12], and the inner parts are added into the corresponding group by matching, while the outer parts are associated to the original surface, which will be clipped again when another relevant intersected cell is processed, otherwise, it is added into the corresponding group directly. After all surfaces are processed, the CSG template is instanced by filling the faces list in each leaf node with the surfaces from the group. The identifier of a group is used to quickly locate the leaf node by matching it. Many technologies can be used for this purpose such as a hash table.

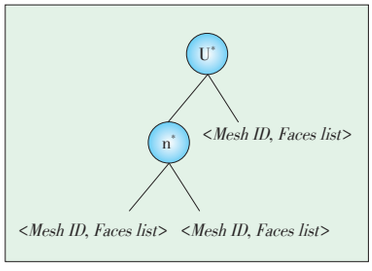


Figure 5.
In a CSG tree template, every primitive is replaced by a pair of key-value with mesh ID and face-list when instancing.

4.2.3 Converting CSG into BSP and Extract Boundary

There are two ways converting the instanced CSG into BSP. One is converting each primitive in leaf nodes into BSP, and then evaluating the tree down-to-up by performing BSP merging operation [24]. The other is converting the CSG tree into BSP tree directly [23]. In order to evaluate the CSG tree efficiently and avoid massive merging operations, we use the latter method. After the conversion, the results of set operations on the CSG tree are obtained by extracting the boundary from the BSP tree [23]. The results must be converted into B-rep and generate the final output by being combined with the evaluation results from other CSG sub-trees.

4.3 Partial Surfaces Classification

Such classification is used to determine the relationship of surfaces within an internal node of an octree with respect to other input models. This way helps determine whether the surfaces should be remained in the final results. The surfaces within an internal node are either entirely inside other models, or entirely outside other models, or on other models. Therefore, the relationship of a surface and a polygon is abstracted to specifying the relationship between the centroids of the polygon and the polyhedron. The classification based on CSG tree starts from bottom, and passes the classification results upwards to the parent node of the current node. The intermediate results are classified with respect to the models representing the brother nodes of the current node. This process ends at the root node and the final classification is achieved.

However, conventional approaches are confined to directly applying classification on the models that are represented by the two children of a CSG tree. When the two children are leaf nodes, the classification is executed between the models represented by them. If one of the two children is a non-leaf node, the intermediate result represented by the node always participates in the classification. This scheme makes the numerical errors propagated upwards, which may impair the topological consistency (such as holes or splits on the resultant polyhedron). In order to avoid such the issue, our algorithm uses a divide-and-conquer method to ensure the classification always happens between the surfaces and the original input model. We further optimize the performance of surface classification by using clustering strategy and octree.

Given a candidate surface p, ourmethod first decides whether the brother node n of the node containing p is a leaf node. If so, the algorithm of point-in-polyhedron is used to determine the relationship of the centroid of p with the input model corresponding to n . Otherwise, the relationship between t and the models represented by two children of n will be checked. The recursion is performed downwards to the leaf nodes to classify

t with respect to the models corresponding to the two leaf nodes. After the classification, the results are propagated upwards again to the father node, and then the classification results are obtained from the predefined rule tables (**Tables 2–4**) based on required Boolean operations. The clasification results keep on propagating to the brother node of n. The concrete process is described in **Algorithm 1**, in which the function Combine makes use of the Boolean operations defined on n and the classification results of left and right sub-trees to get the classification results of the surface p by querying Tables 2 to 4.

▼**Table 2. Classification relation between model C and A ∪* B**

	CinB	CoutB	CwithB	CantiB
CinA	In	In	In	In
CoutA	In	Out	With	Anti
CwithA	In	With	With	In
CantiA	In	Anti	In	Out

"In" denotes a face is inside the model while "Out" has opposite meaning, "With" denotes a face is on the model with same normal, and "Anti" means a face is on the model with opposite normal.

▼**Table 3. Classification relation between model C and A ∩* B**

	CinB	CoutB	CwithB	CantiB
CinA	In	Out	With	Anti
CoutA	Out	Out	Out	Out
CwithA	With	Out	With	Out
CantiA	Anti	Out	Out	Anti

"In" denotes a face is inside the model while "Out" has opposite meaning, "With" denotes a face is on the model with same normal, and "Anti" means a face is on the model with opposite normal.

▼**Table 4. Classification relation between model C and A −* B**

	CinB	CoutB	CwithB	CantiB
CinA	Out	In	Anti	With
CoutA	Out	Out	Out	Out
CwithA	Out	With	Out	With
CantiA	Out	Anti	Anti	Out

"In" denotes a face is inside the model while "Out" has opposite meaning, "With" denotes a face is on the model with same normal, and "Anti" means a face is on the model with opposite normal.

Algorithm 1 ClassifyFacet (Polygon p, CSG-tree-node n)

```
1: if n is a leaf node then
2:     return Point-in-polyhedron (p.barycenter, n.mesh);
3: else
4:     return Combine (ClassifyFacet (p, n.left), ClassifyFacet
           (p, n.right), n.operator);
5: end if
```

Our algorithm uses the octree to complete classification in linear time by combining clustering strategy with the optimized point-in-polyhedron test based on spatial structure. First, the surfaces within each external node of an octree are known to be outside the bounding boxes of other models while the surfaces of each intersected node have been estimated through embedded in the CSG tree. Therefore, we only need to decide the surfaces within internal node with respect to other models. Regarding Property 2, all surfaces within the internal nodes of an octree have the same relationship. Therefore, we can cluster all surfaces as a whole in an internal node and take only one randomly for testing to decide the relationships of all surfaces of an internal node, which dramatically optimizes the performance of classification.

The point-in-polyhedron test is a basic geometric issue, and many researchers have proposed different methods for it [30]–[33]. Those approaches are divided into non-spatial structure methods and spatial structure methods, according to whether spatial structure for acceleration is used. Non-spatial structure methods test all surfaces of the model, while spatial structure methods only need to test a part of the surfaces from the model. Common spatial structure methods include octree, k-d tree, and BSP tree. Since the point-in-polyhedron test based on spatial structure only needs partial geometric information of the polyhedron, its performance is much better than a non-spatial structure method. However, it usually requires pre-process time to construct the spatial structure. The time complexity of classification between two models based on non-spatial structure method is $O(n*k)$, where n is the surface number of tested models and k is the number of tested surfaces. By adapting the ray-casting algorithm based on octree, the time complexity of classifying two models can be decreased to $O(n*\log n)$ yet plus the time of octree traversal. However, octree traversal can be accelerated by parameterization methods [34].

Algorithm 2 shows the pseudo-code of the classification procedure. This algorithm begins with the root node of the CSG

Algorithm 2 Evaluate (CSG-tree-node n)

```
1: if n.left is a leaf node then
2:     Store all facet groups in n.left into G_l;
3: else
4:     G_l = Evaluate (n.left);
5: end if
6: if n.right is a leaf node then
7:     Store all facets groups in n.right into G_r;
8: else
9:     G_r = Evaluate (n.right);
10: end if
11: for each facet group g in G_l do
12:     store the first facet in g into f;
13:     if IsAcceptable(ClassifyFacet(f, n.right), n.operator)) then
14:         store g in node n;
```

```
    end if
end for
for each facet group g in G_r do
    store the first facet in g into f;
    if IsAcceptable(ClassifyFacet(f, n.left), n.operator)) then
        store g in node n;
    end if
end for
return all facet groups in node n;
```

tree in which each leaf node has a list of facet groups. The lists are formed by grouping all surfaces from each internal node of the octree as a whole and then by storing the surfaces into the corresponding list. The recursive process collects the facet groups from child nodes at every stage. Since the surfaces in a group have the same membership, only the first facet in each group involves in the membership test with respect to the polyhedron representing by the brother child node implicitly. The test results, along with the specific selection rules (Section 3), determine whether the group that contains the tested facet is retained in the current node. This process ends at the root node and the final results are achieved in the node.

5 Experiments

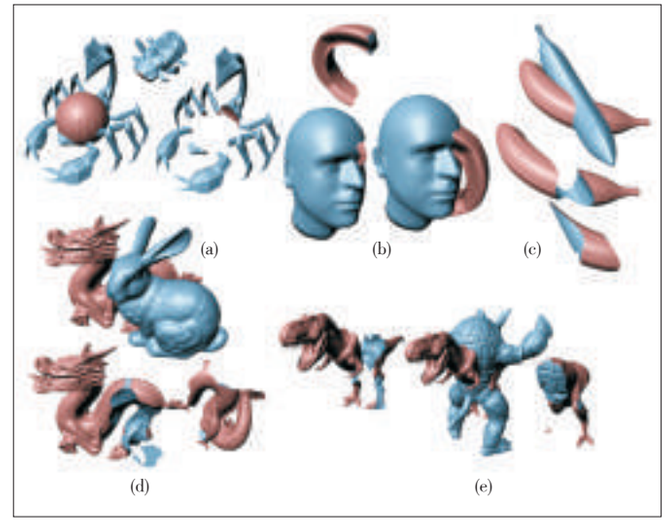
5.1 Setup

The implementation of our method is written in C++. Also, the Intel TBB multi-thread library is used to improve the performance. In order to reach a balance between the depth of octree and the number of polygon pairs for intersection test, the max polygon count in each octree leaf node is around 17.

We evaluated the performance of our method on a system with Intel i5-4200 1.53 GHz CPU and 16 GB RAM. In order to compare the quality of the results and the overall performance, we tested other systems including Maya Campen's method [13]. The input is closed triangle meshes with only vertices position and face indices information. The running time presented below includes pre-processing time.

5.2 Single Boolean Test

A single Boolean test is often used in interactive modeling systems which pursue robust and efficient solutions. We evaluate the robustness and speediness of our method from two aspects. First, we confirm the consistency of performance by performing regularized intersection, union and difference on a series of polyhedral pairs with increasing facet count (**Fig. 6**). The average execution time of the methods was then compared (**Table 5**). Second, we inspected the relationship between the execution time of our method and the number of the facets by constantly subdividing a polyhedron and by performing different set operations on it. The corresponding experimental results are shown in **Table 6**.



▲**Figure 6. Models and its Boolean results: (a) Scorpion; (b) Head; (c) Banana; (d) Bunny; and (e) Dino.**

▼**Table 5. Average time for Boolean operations (intersection, union, difference) of different polyhedrons in Fig. 6**

Models	Facet count	Maya2015 (ms)	Campen's (ms)	Our method (ms)
Scorpion	2400	62	113	31
	9600	219	272	79
	38,200	920	800	254
Head	10,000	281	349	97
	40,000	1217	1192	258
	160,000	5679	5481	934
Banana	48,000	983	1725	368
	192,000	4946	11,576	1303
	768,000	24,960	89,852	6757
Bunny	170,000	20,187	37,774	5370
	680,000	110,885	333,072	29,343
	4430,000	Fail	Out of memory	50,200
Dino	770,000	131,711	92,793	5,202

"Fail" means we get a wrong evaluation result from programs.
"Out of memory" means program crashed because system ran out of memory.

The results in Table 5 show that Maya2015 and Campen's approach went well for simple models. But their performance dropped significantly when models contain over about 200,000 facets. Moreover, the two methods also experienced robustness problems when models contain over 4000,000 facets.

On the contrary, our method can correctly evaluate all examples with high efficiency. Especially, our method is 5 times faster than Maya2015, and 10 times faster than Campen's approach for complex models (over 150,000 facets). This is due to the fact that our method only splits the facets that span over two intersected cells in intersection handling, and speeds up the classification by partial surface classification scheme.

▼Table 6. Average time for Boolean operations with increasing facet count

Facet count	Maya2015 (ms)	Campen's (ms)	Our method (ms)
8000	250	319	139
32,000	797	971	313
128,000	3406	4516	771
512,000	16,438	34,113	2554
2048,000	87,453	32,790	12,371

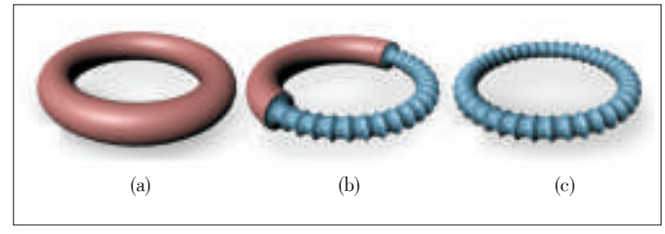
Moreover, our method spent much more processing time on Bunny - Dragon (680,000) than Dino - Monster (770,000) although they have similar facet count. The reason is that the computing time of our method is spent on both intersected handling and membership classification. Our method has to take more time to classify facets when there are a lot of internal cells in the constructed octree. Taking the model pair of Bunny -Dragon as an example, each model has many facets inside the other, which leads to many internal cells in the octree. In general, the system spends the least time on classification for two mutually orthogonal models.

To evaluate the complexity of the algorithm, we prepared a list of mesh pairs with increasing facet count by iteratively subdividing mesh pair Banana (Fig. 6c). Each subdivision increases the facet count by four times. Then we performed set operations on each mesh pair and recorded the average processing time. Table 6 shows that our algorithm is more efficient than the other two methods. This is because the octree constructed in our method only increases the number of intersected cells, while the number of internal and external cells stay fairly constant with the increase of facet count, when the position of two models remains unchanged. As a result, the efficiency of our method is determined by the processing time of intersection handling. Table 6 also shows that the complexity is approximately $O(n)$, where n is the polygon count of mesh, because our method can complete intersection handling in linear time.

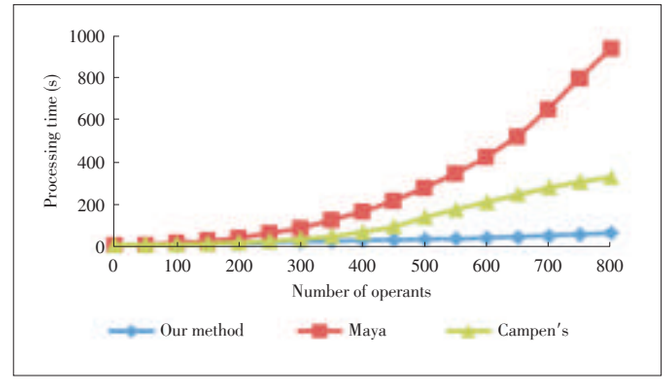
5.3 Iterative Boolean Test

In order to test the iterative Boolean operation performance and robustness of our method, we cut out a large polyhedral object, a ring, by performing iterative intersection operations among a series of small spheres and the ring. Meanwhile, we constantly increase the number of spheres so as to evaluate different methods. **Fig. 7** shows the ring and partial results of the intersection operation.

The experiment results (**Fig. 8**) show that Maya experiences an exponential growth in the process time with constantly increasing spheres, and performance of Campen's method falls dramatically after over 400 spheres. This is because the approaches decompose iterative set operations into a series of binary Boolean operation and then perform them one by one. However, each iteration needs to clip facets, and thereby generates new facets by intersection handling. The situation becomes worse for Campen's method because the method requires extra effort on splitting surfaces along with the boundary of critical cells and performing conversion between different representations. Consequently, the time spent on iterative Boolean operations for the method is greater than the sum of time for all single operations, and the performance and robustness of the method get more and more serious with the growth in iterations. On the contrary, our approach can parse and execute the whole Boolean operation once for all by two major steps: constructing an adaptive octree and embedding a CSG tree into each intersected cell to evaluate all facets in the intersected region, and then using divide-and-conquer method and cluster classification strategy to classify all surfaces in the internal region with the help of the constructed octree. Thus, our method greatly increases the processing speed, and also implements robustness and exactness by integrating plane-based geometry representation with adaptive geometry predicates technique.



▲Figure 7. Sculpting a ring: (a) original mesh (b) 400 spheres cut out (c) after 800 spheres cutting.



▲Figure 8. Iterative Boolean operation for different methods.

6 Conclusion

In this paper, we propose a unified method for efficiently computing single and iterated set operations on polyhedrons. By using localized CSG Trees evaluation strategy, the proposed method can evaluate very complex polyhedrons or massive iterated operations in a few seconds. This method uses the partial surface classification strategy to complete set membership classification in linear time with octree. Moreover, plane-based geometry computation is integrated in this method to make it robust. Experiments have verified that our system is very effi-

cient for CSG trees with different sizes while keeping good quality and stability.

References

[1] T. Ertl, *Computer Graphics—Principles and Practice*. Berlin, Germany: Springer, 1996.
[2] A. A. Requicha and H. B. Voelcker, "Boolean operations in solid modeling: boundary evaluation and merging algorithms," *Proceedings of the IEEE*, vol. 73, no. 1, pp. 30–44, 1985. doi: 10.1109/PROC.1985.13108.
[3] D. H. Laidlaw, W. B. Trumbore, and J. F. Hughes, "Constructive solid geometry for polyhedral objects," *ACM SIGGRAPH Computer Graphics*, vol. 20, no. 4, pp. 161–170, 1986.
[4] F. Yamaguchi and T. Tokieda, "A unified algorithm for Boolean shape operations," *IEEE Computer Graphics and Applications*, vol. 4, no. 6, pp. 24–37, 1987. doi: 10.1109/MCG.1984.275959.
[5] P. Hachenberger and L. Kettner, "Boolean operations on 3D selective Nef complexes: optimized implementation and experiments," in *Proc. ACM Symposium on Solid and Physical Modeling*, Cambridge, USA, 2005, pp. 163–174.
[6] S. F. Frisken, R. N. Perry, A. P. Rockwood and T. R. Jones, "Adaptively sampled distance fields: a general representation of shape for computer graphics," in *Proc. 27th Annual Conference on Computer Graphics and Interactive Techniques*, New Orleans, USA, 2000.
[7] K. Museth, D. E. Breen, R. T. Whitaker, and A. H. Barr, "Level set surface editing operators," *ACM Transactions on Graphics*, vol. 21, no. 3, pp. 330–338, Jul. 2002.
[8] T. Ju, F. Losasso, S. Schaefer, and J. Warren, "Dual contouring of hermite data," *ACM Transactions on Graphics*, vol. 21, no. 3, pp. 339–346, Jul. 2002.
[9] G. Varadhan, S. Krishnan, Y. J. Kim, and D. Manocha, "Feature-sensitive subdivision and isosurface reconstruction," in *IEEE Visualization*, Seattle, USA, 2003, pp. 99–106. doi: 10.1109/VISUAL.2003.1250360.
[10] G. Varadhan, S. Krishnan, T. V. N. Sriram, and D. Manocha, "Topology preserving surface extraction using adaptive subdivision," in *Proc. Second Eurographics Symposium on Geometry processing*, Nice, France, 2004, pp. 235–244.
[11] N. Zhang, W. Hong, and A. Kaufman, "Dual contouring with topology-preserving simplification using enhanced cell representation," *IEEE Visualization*, pp. 505–512, Oct. 2004. doi: 10.1109/VISUAL.2004.27.
[12] G. Bernstein and D. Fussell, "Fast, exact, linear Booleans," *Computer Graphics Forum*, vol. 28, no. 5, pp. 1269–1278, Jul. 2009. doi: 10.1111/j.1467–8659.2009.01504.
[13] M. Campen and L. Kobbelt, "Exact and robust (self-) intersections for polygonal meshes," *Computer Graphics Forum*, vol. 29, no. 2, pp. 397–406, Jun. 2010. doi: 10.1111/j.1467–8659.2009.01609.
[14] F. R. Feito, C. J. Ogáyar, R. J. Segura, and M. Rivero, "Fast and accurate evaluation of regularized Boolean operations on triangulated solids," *Computer-Aided Design*, vol. 45, no. 3, pp. 705–716, Mar. 2013. doi: 10.1016/j.cad.2012.11.004.
[15] L. P. Kobbelt, M. Botsch, U. Schwanecke, and H. P. Seidel, "Feature sensitive surface extraction from volume data," in *Proc. 28th Annual Conference on Computer Graphics and Interactive Techniques*, New York, USA, 2001. doi: 10.1145/383259.383265.
[16] S. Schaefer, T. Ju, and J. Warren, "Manifold dual contouring," *IEEE Transactions on Visualization and Computer Graphics*, vol. 13, no. 3, pp. 610–619, 2007. doi: 10.1109/TVCG.2007.1012.
[17] H. Biermann, D. Kristjansson, and D. Zorin, "Approximate boolean operations on free-form solid," in *28th Annual Conference on Computer Graphics and Interactive Techniques*, New York, USA, 2001, pp. 185–194. doi: 10.1145/383259.383280.
[18] M. Lounsbery, T. D. DeRose, and J. Warren, "Multiresolution analysis for surfaces of arbitrary topological type," *ACM Transactions on Graphics*, vol. 16, no. 1, pp. 34–73, 1997. doi: 10.1145/237748.237750.
[19] R. Seidel, "The nature and meaning of perturbations in geometric computing," *Discrete & Computational Geometry*, vol. 19, no. 1, pp. 1–17, Jan. 1998. doi: 10.1007/PL00009330.
[20] J. M. Smith and N. A. Dodgson, "A topologically robust algorithm for Boolean operations on polyhedral shapes using approximate arithmetic," *Computer-Aided Design*, vol. 39, no. 2, pp. 149–163, Feb. 2007. doi: 10.1016/j.cad.2006.11.003.
[21] C. C. Wang, "Approximate boolean operations on large polyhedral solids with partial mesh reconstruction," *IEEE Transactions on Visualization and Computer Graphics*, vol. 17, no. 6, pp. 836–849, Jun. 2011. doi: 10.1109/TVCG.2010.106.
[22] J. Shade, S. Gortler, L. W. He, and R. Szeliski, "Layered depth images," in *Proc. 25th Annual Conference on Computer Graphics and Interactive Techniques*, Orlando, USA, 1998, pp. 231–242. doi: 10.1145/280814.280882.
[23] W. C. Thibault and B. F. Naylor, "Set operations on polyhedra using binary space partitioning trees," *ACM SIGGRAPH computer graphics*, vol. 21, no. 4, pp. 153–162, 1987. doi: 10.1145/37402.37421.
[24] B. Naylor, J. Amanatides, and W. Thibault, "Merging BSP trees yields polyhedral set operations," *ACM SIGGRAPH Computer Graphics*, vol. 24, no. 4, pp. 115–124, Aug. 1990. doi: 10.1145/97880.97892.
[25] W. C. Thibault, "Application of binary space partitioning trees to geometric modeling and ray-tracing," Ph.D. dissertation, Georgia Institute of Technology, Atlanta, Georgia, USA, 1987.
[26] K. Sugihara and M. Iri, "A solid modelling system free from topological inconsistency," *Journal of Information Processing*, vol. 12, no. 4, pp. 380–393, 1990.
[27] J. R. Shewchuk, "Adaptive precision floating-point arithmetic and fast robust geometric predicates," *Discrete & Computational Geometry*, vol. 18, no. 3, pp. 305–363, Oct. 1997. doi: 10.1007/PL00009321.
[28] K. Kuratowski and A. Mostowski, *Set Theory*. Waltham, USA: Elsevier, Academic Press, 1968.
[29] J. R. Shewchuk, "Lecture notes on geometric robustness," in *Eleventh International Meshing Roundtable*, 1999, pp. 115–126.
[30] F. R. Feito and J. C. Torres, "Inclusion test for general polyhedra," *Computers & Graphics*, vol. 21, no. 1, pp. 23–30, 1997. doi: 10.1016/S0097–8493(96)00067–2.
[31] J. Liu, Y. Q. Chen, J. M. Maisog, and G. Luta, "A new point containment test algorithm based on preprocessing and determining triangles," *Computer-Aided Design*, vol. 42, no. 12, pp. 1143–1150, 2010. doi: 10.1016/j.cad.2010.08.002.
[32] C. J. Ogayar, R. J. Segura and F. R. Feito, "Point in solid strategies," *Computers & Graphics*, vol. 29, no. 4, pp. 616–624, Aug. 2005. doi: 10.1016/j.cag.2005.05.012.
[33] W. Wang, J. Li, H. Sun, and E. Wu, "Layer-based representation of polyhedrons for point containment tests," *IEEE Transactions on Visualization and Computer Graphics*, vol. 14, no. 1, pp. 73–83, 2008. doi: 10.1109/TVCG.2007.70407.
[34] J. Revelles, C. Urena, and M. Lastra, "An Efficient Parametric Algorithm for Octree Traversal," in *WSCG*, Plzen-Bory, Czech Republic, 2000, pp. 212–219.

Manuscript received: 2015-06-05

Biographies

Ping Lu (lu.ping@zte.com.cn) received his ME degree in automatic control theory and applications from South East University. He is the chief executive of the Cloud Computing and IT Institute of ZTE Corporation. His research interests include augmented reality and multimedia services technologies.

Xudong Jiang (denny.jiang@gmail.com) received his master's degree in computer science and technology from Shanghai Jiao Tong University. He is currently working at the Autodesk China Research & Development Center. His research interests include computer graphics and solid modeling.

Wei Lu (ddhansh@gmail.com) received her PhD degree in computer science and technology from Nanjing University. She is currently working at the Autodesk China Research & Development Center. Her research interests include computer graphics, mesh deformation, and virtual reality.

Ran Wei (wei.ran233@zte.com.cn) received his master's degree in communications and electronic information from Chongqing University of Posts and Telecommunications. He is currently a pre-research engineer of ZTE Corporation. His research interests include machine vision and graphics and image processing.

Bin Sheng (shengbin@cs.sjtu.edu.cn) received his MS degree in software engineering from University of Macau in 2007, and PhD degree in computer science from The Chinese University of Hong Kong in 2011. He is currently an associate professor at Department of Computer Science and Engineering, Shanghai Jiao Tong University. He also works with the Institute of Software, Chinese Academy of Sciences. His research interests include virtual reality, computer graphics, and image based techniques.

ZTE Communications Guidelines for Authors

• Remit of Journal

ZTE Communications publishes original theoretical papers, research findings, and surveys on a broad range of communications topics, including communications and information system design, optical fiber and electro-optical engineering, microwave technology, radio wave propagation, antenna engineering, electromagnetics, signal and image processing, and power engineering. The journal is designed to be an integrated forum for university academics and industry researchers from around the world.

• Manuscript Preparation

Manuscripts must be typed in English and submitted electronically in MS Word (or compatible) format. The word length is approximately 4000 to 7000, and no more than 6 figures or tables should be included. Authors are requested to submit mathematical material and graphics in an editable format.

• Abstract and Keywords

Each manuscript must include an abstract of approximately 150 words written as a single paragraph. The abstract should not include mathematics or references and should not be repeated verbatim in the introduction. The abstract should be a self-contained overview of the aims, methods, experimental results, and significance of research outlined in the paper. Five carefully chosen keywords must be provided with the abstract.

• References

Manuscripts must be referenced at a level that conforms to international academic standards. All references must be numbered sequentially in-text and listed in corresponding order at the end of the paper. References that are not cited in-text should not be included in the reference list. References must be complete and formatted according to ZTE Communications Editorial Style. A minimum of 10 references should be provided. Footnotes should be avoided or kept to a minimum.

• Copyright and Declaration

Authors are responsible for obtaining permission to reproduce any material for which they do not hold copyright. Permission to reproduce any part of this publication for commercial use must be obtained in advance from the editorial office of *ZTE Communications*. Authors agree that a) the manuscript is a product of research conducted by themselves and the stated co-authors, b) the manuscript has not been published elsewhere in its submitted form, c) the manuscript is not currently being considered for publication elsewhere. If the paper is an adaptation of a speech or presentation, acknowledgement of this is required within the paper. The number of co-authors should not exceed five.

• Content and Structure

ZTE Communications seeks to publish original content that may build on existing literature in any field of communications. Authors should not dedicate a disproportionate amount of a paper to fundamental background, historical overviews, or chronologies that may be sufficiently dealt with by references. Authors are also requested to avoid the overuse of bullet points when structuring papers. The conclusion should include a commentary on the significance/future implications of the research as well as an overview of the material presented.

• Peer Review and Editing

All manuscripts will be subject to a two-stage anonymous peer review as well as copyediting, and formatting. Authors may be asked to revise parts of a manuscript prior to publication.

• Biographical Information

All authors are requested to provide a brief biography (approx. 150 words) that includes email address, educational background, career experience, research interests, awards, and publications.

• Acknowledgements and Funding

A manuscript based on funded research must clearly state the program name, funding body, and grant number. Individuals who contributed to the manuscript should be acknowledged in a brief statement.

• Address for Submission

magazine@zte.com.cn
12F Kaixuan Building, 329 Jinzhai Rd, Hefei 230061, P. R. China

ZTE COMMUNICATIONS

ZTE Communications has been indexed in the following databases:

- Cambridge Scientific Abstracts (CSA)
- China Science and Technology Journal Database
- Chinese Journal Fulltext Databases
- Inspec
- Norwegian Social Science Data Services (NSD)
- Ulrich's Periodicals Directory
- Wanfang Data—Digital Periodicals