

ZTE COMMUNICATIONS

September 2013, Vol.11 No.3

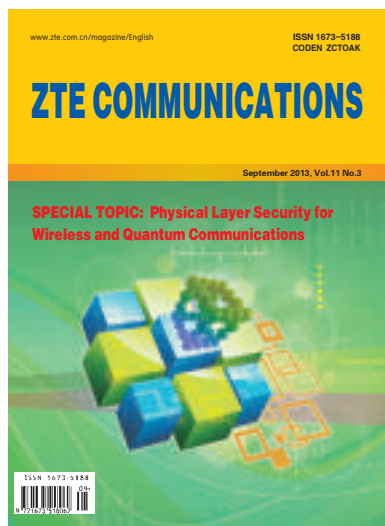
**SPECIAL TOPIC: Physical Layer Security for
Wireless and Quantum Communications**



ISSN 1673-5188



► 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copyrights of the accepted manuscript to *ZTE Communications*; and that the manuscript or parts thereof will thus not be published elsewhere in any language without the consent of the copyright holder.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

Physical Layer Security for Wireless and Quantum Communications

- | | |
|----|--|
| 01 | Guest Editorial
Jinhong Yuan, Yixian Yang, and Nanrun Zhou |
| 03 | Location Verification Systems in Emerging Wireless Networks
Shihao Yan and Robert Malaney |
| 11 | Wireless Physical Layer Security with Imperfect Channel State Information: A Survey
Biao He, Xiangyun Zhou, and Thushara D. Abhayapala |
| 20 | Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics
Syed Taha Ali and Vijay Sivaraman |
| 26 | An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels
Nan Yang, Maged El Kashlan, Phee Lep Yeoh, and Jinhong Yuan |
| 33 | Reducible Discord in Generic Three-Qubit Pure W States
Zhengjun Xi, Zhihui Li and Yongming Li |
| 36 | Two-Way Cooperative Quantum Communication with Partial Entanglement Analysis
Yunkai Deng, Zhujun Gao, and Ying Guo |
| 41 | A Coding and Automatic Error-Correction Circuit Based on the Five-Particle Entangled State
Xi Chen, Pei Zhang, and Xiaoqing Zhou |

► CONTENTS

ZTE COMMUNICATIONS

Vol. 11 No.3 (Issue 39)

Quarterly

First English Issue Published in 2003

Supervised by:

Anhui Science and Technology Department

Sponsored by:

ZTE Corporation and Anhui Science
and Technology Information
Research Institute

Staff Members:

Editor-in-Chief: Sun Zheng

Associate Editor-in-Chief: Zhao Jinming

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 Zhongjian Color Printing Company

Publication Date:

September 25, 2013

Publication Licenses:

ISSN 1673-5188

CN 34-1294/TN

Advertising License:

皖合工商广字0058号

Annual Subscription Rate:

RMB 80

46

Optimal Rate for Constant-Fidelity Entanglement in Quantum Communication Networks

Youxun Cai, Xutao Yu, and Yang Cao

Research Papers

51

IVI/MAP-T/MAP-E: Unified IPv4/IPv6 Stateless Translation and Encapsulation Technologies

Congxiao Bao and Xing Li

56

A Parallel Platform for Web Text Mining

Ping Lu, Zhenjiang Dong, Shengmei Luo, Lixia Liu, Shanshan Guan,
Shengyu Liu, and Qingcai Chen

Roundup

32

ZTE to Provide Disaster Recovery Solution to U Mobile Malaysia

45

ZTE Launches the World's Largest Capacity Data Center Switches

50

Powering Next-Generation Broadband Networks: ZTE's World-First Flexible, Configurable Router

61

ZTE USA Announces Its First Corporate Partnership and Consumer Marketing Push in Conjunction with the Houston Rockets

► Jinhong Yuan



Jinhong Yuan received his BE and PhD degrees in electronics engineering from Beijing Institute of Technology in 1991 and 1997. From 1997 to 1999, he was a research fellow at the School of Electrical Engineering, University of Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New

South Wales, Australia, and is currently a professor of telecommunications at that school. Dr. Yuan has authored two books, two book chapters, and more than 200 papers for telecommunications journals and conferences. He has also authored 40 industry reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density parity-check (LDPC) codes. He has co-authored three papers that have won Best Paper Awards or Best Poster Awards. His published work list is available at <http://www2.ee.unsw.edu.au/wel/JYuan.html>. Dr. Yuan is currently the NSW Chair of the joint Communications/Signal Processing/Ocean Engineering Chapter of IEEE. He is also an associate editor for IEEE Transactions on Communications. His research interests include error-control coding and information theory, communication theory, and wireless communications.

► Yixian Yang



Professor Yixian Yang is the Director of Information Security Center, Beijing University of Posts and Telecommunications. He is also chief of the National Engineering Laboratory for Disaster Backup and Recovery, National Key Laboratory for Network and Information Defense. He received his PhD degree in electrical engineering and communication systems from BUPT in 1988. His research interests include network coding, coding theory, cryptography, information security, internet/intranet security, communication theory, graph theory, neural networks, signal processing, software radio, wavelet theory, discrete mathematics, and e-commerce. Dr. Yang has authored more than 500 research papers in academic journals such as IEEE Transactions on Communications, and has also authored textbooks and monographs.

► Nanrun Zhou



Nanrun Zhou received his BSc degree in Physics Education and his MSc degree in Theoretical Physics from Jiangxi Normal University in 2000 and 2003. He received his PhD degree in Communications and Information Systems from Shanghai Jiaotong University in 2005. In 2006, he joined the School of Information Engineering, Nanchang Uni-

versity, and is currently a professor and PhD supervisor at that school. From September 2011 to July 2012, he was a visiting scholar in the School of Computer Science, Beijing University of Posts and Telecommunications. Previously, he has been selected to the first and second ranks of the Jiangxi Province Baiqianwan Talents for the New Century Programme, the Young Scientists of Jiangxi Province (Jinggang Star), and the Ganpo Programme 555 for Outstanding Talent. His research interests include quantum communication, quantum cryptography, optical image encryption, and wireless communication security. He has published more than 110 papers in refereed international journals and conference proceedings.

Physical Layer Security for Wireless and Quantum Communications

This special issue is dedicated to security problems in wireless and quantum communications. Papers for this issue were invited, and after peer review, eight were selected for publication. The first part of this issue comprises four papers on recent advances in physical layer security for wireless networks. The second part comprises another four papers on quantum communications.

Wireless networks have become pervasive in order to guarantee global digital connectivity, and wireless devices have quickly evolved into multimedia smartphones running applications that demand high-speed data connections. Multiuser multiple-input multiple-output (MIMO) wireless techniques meet this demand by achieving high spectral efficiency. Security is also regarded as critical in wireless multiuser networks because users rely on these networks to transmit sensitive data. Because of the broadcast nature of the physical medium, wireless multiuser communication is very susceptible to eavesdropping, and it is essential to protect transmitted information. Wireless communications have traditionally been secured by network layer key-based cryptography. However, in large, dynamic wireless networks, classical cryptography might not be suitable. Classical cryptography tends to cause problems in terms of key distribution and management (for symmetric cryptosystems) and computational complexity (for asymmetric cryptosystems). Moreover, classical cryptography is potentially vulnerable because it relies on the unproven assumption that certain mathematical functions are difficult to invert. Recently, methods have been proposed to provide an additional level of protection and to achieve perfect secrecy without encryption keys. These methods, collectively referred to as physical layer security, exploit the randomness inherent in noisy channels. Physical layer security has been identified as the highest form of security and will be a critical part of future communication networks. The core principle of physical layer security is to restrict the amount of useful information that can be extracted at the symbol/signal level by an unauthorized receiver. This is achieved by carefully designing intelligent and appropriate coding and precoding techniques that exploit the wireless medium's channel state information. As opposed to classic cryptography, physical layer security is based on information-theoretic principles and does not rely on secret keys or the limited computational capacity of the eavesdropper. Over the past few years, the information-theoretic aspect of secrecy at the physical layer has attracted significant interest and promises to significantly affect both the theory and practical design of future wireless networks.

In "Location Verification Systems in Emerging Wireless Networks," Yan and Malaney discuss location-based techniques and applications. They show that in recent years, there has been an explosion of activity related to location-verification techniques in wireless networks. This work has focused on intelligent transport system (ITS) because of the mission-critical nature of vehicle location verification within ITS. The authors review recent research on wireless location verification related to the vehicular networks. In particular, they focus on location verification systems that rely on formal mathematical classification frameworks and show how many systems are either partly or fully encompassed by such frameworks.

Physical Layer Security for Wireless and Quantum Communications

Jinhong Yuan, Yixian Yang, and Nanrun Zhou

In “Wireless Physical Layer Security with Imperfect Channel State Information: A Survey,” Bao He et al. provide a comprehensive survey of physical layer security in wireless networks with imperfect channel state information (CSI) at communication nodes. The authors describe the main information-theoretic ways that secrecy is measured when CSI is imperfect. They also describe signal processing enhancements for secure transmission. These enhancements include secure on-off transmission, beamforming with artificial noise, and secure communication assisted by relay nodes or cognitive radio systems. The authors discuss the recent development of physical layer security in large, decentralized wireless networks as well as open problems and future research directions.

In “Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics,” Ali and Sivaraman give an overview of current research on shared secret-key agreement between two parties. This agreement is based on the wireless channel characteristics of the radio. The authors discuss the advantages of shared secret-key agreement over traditional cryptographic mechanisms and describe the theory behind this technique. They also describe the key agreement process, threat model, and typical performance metrics. A shared secret-key agreement comprises four processes: sampling, quantization, information reconciliation, and privacy application. The authors also discuss existing challenges and future research directions.

In “An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels,” Yang et al. propose transmit antenna selection as a low-complexity, energy-efficient way of improving physical layer security in multiple-input multiple-output wiretap channels. The authors describe a general framework for analyzing the exact and asymptotic secrecy of transmit antenna selection. This framework includes receive maximal ratio combining, selection combining, or generalized selection combining. The results show that secrecy is significantly increased when the number of transmit antennas is increased.

Significant progress has been made in quantum communications as a result of increased support from governments and enterprises. There is a practical need for quantum communication, and it will significantly alter future communications. Quantum cryptography can benefit from the properties of quantum systems, e.g. entangled systems. Quantum entanglement lies at the heart of quantum information processing and communication. For a long time, entanglement was seen merely as a fancy feature that makes quantum mechanics counterintuitive. Quantum information theory has recently shown how quantum correlations are tremendously important to the formulation of new methods of information transfer and for algorithms based on quantum computers. Quantum correlation makes quantum information processing powerful and interesting. In a quantum many-particle system, classifying and quantifying correlations in a multipartite quantum state and deter-

mining how much knowledge about the quantum system can be acquired from subsystems are fundamental problems. The main task of quantum information processing and communication is the delivery of quantum states. The main focus of quantum information processing and communication is the delivery of quantum states. A quantum carrier or quantum channel can perform miracles compared with conventional signal processing and communication. In practice, it is very difficult to deliver entangled photons over long distances because of channel loss and detector noise. Quantum error correction coding is necessary for practical, reliable quantum information processing and can be performed in a noisy or real channel or in an imperfect processor.

In “Reducible Discord in Generic Three-Qubit Pure W States,” Zhihui Li et al. show that quantum correlation in generic three-qubit pure W states can be given by the two-qubit discord of these states. The authors show that reducing discord in the generalized three-qubit pure W state is complicated.

In “Two-Way Cooperative Quantum Communication with Partial Entanglement Analysis,” Ying Guo et al. describe an improved cooperative two-way quantum communication scheme. This scheme works in a forward-and-backward manner and is based on the five-qubit entangled Brown state. It allows Alice and Bob to simultaneously exchange arbitrary unknown states with the help of trusted Charlie. The authors show how to transfer arbitrary unknown states in a secure cooperative manner using encryption performed by trusted Charlie.

In “A Coding and Automatic Error-Correction Circuit Based on the Five-Particle Entangled State,” Xiaoqing Zhou et al. propose a quantum-coding and error-correction circuit for the five particle entangled state. This circuit can correct the bit-reversed or phase-flip error of one and two quantum states. The authors also simplify the design of a multiple quantum error-correction circuit.

In “Optimal Rate for Constant-Fidelity Entanglement in Quantum Communication Networks,” Xutao Yu et al. describe how to achieve constant fidelity entanglement over long distances in quantum networks. The authors discuss the rate capacities of constant fidelity entanglement for both elementary and multihop links. In particular, the authors focus on the rate capacity of constant fidelity entanglement in quantum communication networks when the number of nodes in a multihop link tends towards infinity. The authors draw the concepts of classical ad hoc networks to optimize the rate capacity of one typical structure of a quantum repeater. The rate capacities of the recursive entanglement scheme (simultaneous entanglement scheme) and adjacent entanglement scheme are $\Omega(1/e^n)$ and $\Omega(1/n)$, respectively.

We thank all authors for their valuable contributions and all reviewers for their timely and constructive comments on submitted papers. We hope the content of this issue is informative and helpful to all readers.

Location Verification Systems in Emerging Wireless Networks

Shihao Yan and Robert Malaney

(School of Electrical Engineering and Telecommunications, UNSW, Sydney 2052, Australia)

Abstract

As location-based techniques and applications have become ubiquitous in emerging wireless networks, the verification of location information has become more important. In recent years, there has been an explosion of activity related to location-verification techniques in wireless networks. In particular, there has been a specific focus on intelligent transport systems because of the mission-critical nature of vehicle location verification. In this paper, we review recent research on wireless location verification related to vehicular networks. We focus on location verification systems that rely on formal mathematical classification frameworks and show how many systems are either partially or fully encompassed by such frameworks.

Keywords

location verification; wireless networks; likelihood ratio test; decision rule

1 Introduction

As location-based techniques and services have become ubiquitous in emerging wireless networks, the authentication of location information has attracted considerable research interest [1]–[12]. In early wireless positioning systems, accuracy and performance were of utmost importance, and authenticating location information was relegated to a secondary concern. This is now changing. Many current mainstream wireless positioning systems, such as now-ubiquitous Wi-Fi positioning systems, are highly vulnerable to location-spoofing attacks because of their openness and wide public availability [13], [14]. In many configurations, wireless network positioning systems are client-based, which means that only the client (the device whose location is to be verified) can directly obtain its location [15], [16]. The wider communications network can only obtain the client's position by requesting the client to report its location. However, the client can easily spoof or falsify its location. In other configurations, systems that attempt to directly locate a client by using signal metrics, such as received signal strength (RSS) measurements, are vulnerable to manipulation of the signal metric by the client prior to transmission [17]–[20]. In this paper, we review works that attempt to formalize loca-

tion-spoofing. We focus on location verification and assume that the location of the client is the true location and is either publicly announced by the client or a priori publicly known. We refer to this announced or known location as the claimed location. The verification systems we discuss are instructed to use all available signal metrics to classify the client according to whether it is at the claimed location or not [21]–[54]. Location verification (or authentication) defined in this way results in a mathematical problem (and outcome) that is different to more common location acquisition problems [15]–[20]. Location verification is important because spoofed location information can adversely affect a variety of network functions [2], [4], [5], [8], [55]–[62]. For example, in generic wireless networks, spoofed location information can lead to dramatically reduced packet delivery in geographic routing protocols [55], [56]. The performance of location-based access control can also be markedly reduced when locations are spoofed [60]–[62]. Wi-Fi, cellular, and GPS position information in the E911 framework can be easily spoofed by clients in order to maliciously attract emergency services to false locations [47]. However, the adverse effects of location spoofing are arguably even more severe in vehicular ad hoc networks (VANETs) [2], [4], [5], [8].

In VANETs, location spoofing can cause life-threatening traffic accidents. Less critically, a malicious vehicle might spoof its location in order to seriously disrupt other drivers [2], [4], [5] or to selfishly enhance its own functionality within the

This work is supported by the University of New South Wales and the Australian Research Council under grant No. DP120102607.

Location Verification Systems in Emerging Wireless Networks

Shihao Yan and Robert Malaney

network [35], [44]. Authenticating position information within VANETs is the focus of the rest of this paper. We focus on exploiting the physical properties of wireless communication channels to verify a location. Such an approach eliminates (or at least drastically reduces) any dependency on complex higher-layer secrecy techniques, such as encryption or cryptographic key management. Using the properties of the wireless communication channels also allows us to more formally examine the optimal performance expectations for a location verification system (LVS).

In section 2, we describe a generic formal LVS and associated performance evaluation criteria. In section 3, we apply our generic LVS in an emerging VANET scenario. In section 4, we discuss other location verification systems that are not targeted at VANET scenarios but can be adapted to them. In section 5, we draw some conclusions and discuss future research directions.

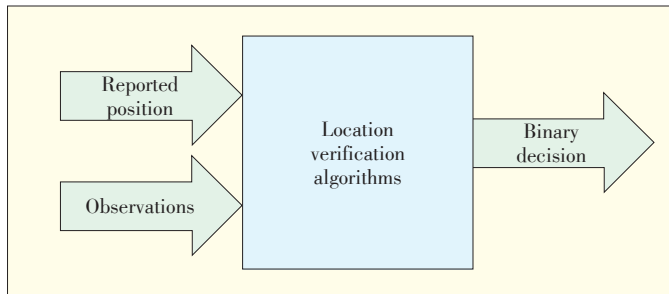
2 Generic Location Verification System

2.1 Binary Decision Rule for an LVS

Location verification is different from locating a user in a wireless network [49]. A key difference between an LVS and a positioning system is that the output of an LVS is usually a binary decision (yes/no) whereas the output of a positioning system is an estimated user location. **Fig. 1** shows a generic LVS. The claimed location is an LVS input provided by the client being verified (the prover).

The observations of the location verifiers are also inputs to the LVS. The LVS aims to verify a prover's claimed location by comparing these inputs and systematically checking whether all inputs are compatible. If they are compatible, a yes decision is returned by the LVS. If they are incompatible, a no decision is returned by the LVS. Because of these binary outputs, location verification can be modeled as a binary decision-theory problem. Thus, a decision rule is embedded in an LVS and can be written as

$$\begin{array}{l} D_1 \\ T \underset{<}{\overset{\geq}{\geq}} \lambda \\ D_0 \end{array} \quad (1)$$



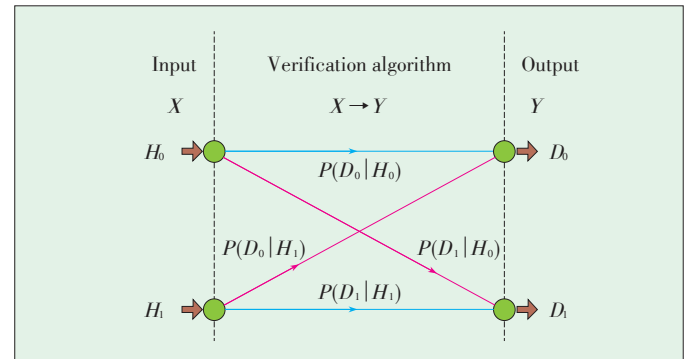
▲ Figure 1. A generic location verification system.

where T is the test statistic, λ is the threshold corresponding to T , and D_0 and D_1 are the binary decisions that infer whether the prover is legitimate or malicious, respectively. The test statistic T is derived from the LVS inputs, the form of which varies according to location verification algorithms.

In an LVS framework, we also have to consider noise (for example, noise in the location acquisition problem results in location error). Noise is usually encapsulated within the classifier logic (i.e. implicit probability distributions) of the LVS. In addition, if the claimed position changes to a claimed area (e.g. a room), the system's implicit probability distributions are altered accordingly.

2.2 ROCs for an LVS

From a statistical decision-theory perspective, an LVS can be modeled as a decision problem (**Fig. 2**). In **Fig. 2**, X is the input of an LVS, and the two realizations are H_0 and H_1 . Here, H_0 represents the case where the prover is at the claimed location (null hypothesis), and H_1 represents the case where a malicious prover is not at the claimed location. In **Fig. 2**, the output Y of an LVS is also binary, and its realizations are D_0 and D_1 . For a given X , the probabilities $P(D_j | H_i)$ ($i = 0, 1, j = 0, 1$) represent the probabilities of deciding on an output Y . The $P(D_j | H_i)$ determines the performance of an LVS [41]. The traditional method for evaluating a detection system involves using the Neyman-Pearson Lemma, which itself is based on the false positive and detection rates. The false positive rate is the probability of deciding incorrectly that a legitimate prover is malicious and is given by $\alpha = P(D_0 | H_0)$. The detection rate is the probability of deciding correctly that a prover is malicious and is given by $\beta = P(D_1 | H_1)$. Both these rates are functions of T and λ . We expect an LVS to provide a high detection rate and low false positive rate, but there is a tradeoff between the false positive and detection rates. The receiver operative curve (ROC) is used to demonstrate this tradeoff and is constructed by plotting β versus α . However, the ROC itself does not provide an optimized setting [41]. The Neyman-Pearson Lemma states that the likelihood ratio test maximizes the detection rate for any given false positive rate [63], [64]. The likelihood ratio is the ratio between the probability density functions of the



▲ Figure 2. Statistical decision theory model for an LVS [4].

measurements under H_0 and H_1 , and the corresponding threshold T is derived by assuming a false positive rate. However, using such a method to determine T does not completely optimize an LVS [63], [64].

2.3 Optimization Frameworks for an LVS

To optimize an LVS, some unique evaluation criterion should be used as the performance metric. The transition probabilities between X and Y determine the performance of an LVS; thus, a unique evaluation criterion should be a function of such transition probabilities.

One widely used metric is Bayes average cost, given by [64]

$$R = \sum_{i=0}^1 \left| \sum_{j=0}^1 C_{ji} P(D_j | H_i) P(H_i) \right| \quad (2)$$

where C_{ji} is the cost assigned to the decision D_j (given the hypothesis H_i), and $P(H_0)$ and $P(H_1)$ are the a priori probabilities of the occurrence of H_0 and H_1 , respectively. In this Bayesian framework, the optimal location verification algorithm is the one that minimizes R . The Bayes average cost requires a priori knowledge of both C_{ji} and $P(H_i)$. If C_{ji} is unknown, the MAP criterion can be used [64]. According to this criterion, the unique cost is given by

$$R_M = C_{10}P(D_1 | H_0)P(H_0) + C_{01}P(D_0 | H_1)P(H_1) \quad (3)$$

Comparing (2) and (3), we can see that R_M is a special case of R , where $C_{00} = C_{11} = 0$, and $C_{10} = C_{01} = 1$. Thus, the MAP criterion is well suited for scenarios where the cost of rejecting a legitimate user is equal to that of accepting a malicious user. In addition, R_M can be reduced to the “total error” when $P(H_0) = P(H_1) = 0.5$ [52].

Although Bayes average cost, MAP, and total error can be used to optimize an LVS, they all possess a weakness in that they all depend on subjective cost values. With Bayes average cost, we have to predetermine the costs for all possible decisions. However, properly determining the true cost to the network for each decision is practically impossible. For example, what is the detailed cost to a VANET when one vehicle spoofs its location information? The true cost is subjective and depends on numerous factors and scenarios. Similarly, C_{10} and C_{01} are both set to one in the MAP criterion and total error, but the cost of accepting a malicious prover is likely much higher than that of rejecting a legitimate prover.

To solve this subjective problem when optimizing an LVS, an information-theoretic framework has been proposed [40], [41]. In this framework, the cost of each possible decision is assigned objectively, not subjectively. The mutual information between the system input and output is used as the optimization criterion. The mutual information between X and Y is defined as

$$I(X; Y) = H(X) - H(X | Y) \quad (4)$$

where $H(X)$ is the input entropy, which measures the uncertainty of the system input (determined by the a priori probabilities); and $H(X | Y)$ is the conditional entropy of X for a given Y . The conditional entropy measures the uncertainty of the input given the output, which is determined by the a priori and transition probabilities. Thus, $I(X; Y)$ measures the uncertainty reduction of the input given the output, and $I(X; Y)$ is maximized by the optimal information-theoretic location verification algorithm. Compared with the Bayesian framework, the information-theoretic framework only assumes knowledge of the a priori probabilities.

Although the likelihood ratio is the optimal test statistic in most frameworks, it is difficult to obtain in practice without making some assumptions about an attacker’s behavior and location. The likelihood function under H_1 is depends on the malicious prover’s attack strategy and true location, both of which are a priori unknown to the LVS. The effect of these key uncertainties with regard to optimizing the LVS is discussed in the following.

3 Location Verification in VANETs

3.1 Location Verification Based on Binary Decision Rules

The authors in [21] exploited specific properties of VANETs, such as high node density and mobility, and proposed an autonomous scheme and cooperative scheme for detecting and mitigating false locations. The acceptance range, mobility grade, and vehicle density were used in the binary decision rule of the autonomous scheme, and the thresholds were based on maximum communication range, maximum velocity, and maximum density, respectively. The test statistics used in the cooperative scheme included neighbor tables and could only be obtained through cooperation between neighboring vehicles. The decision about a prover’s claimed location is made by combining the local decisions with weight factors. The proposed location verification scheme is applied in location-based routing protocols, and it is assumed that a malicious vehicle does not forward the packet to the correct next hop. Therefore, the packet delivery ratio can be a performance criterion.

The proposed schemes in [21] provide the basis of location verification in VANETs. Similarly, the authors of [29] proposed location verification algorithms based on communication range, velocity and density but extended their test statistics to include travelled distance and map location.

The authors of [22] used the timestamp of a packet that had been sent (the claimed location is embedded within this timestamp) in order to detect malicious vehicles that spoof location information in a VANET. The timestamp check ensures that the received packet is neither too old nor too early. In [22], a rate-limiting mechanism was proposed. If the rate of packets originating from a prover exceeds a predetermined maximum

Location Verification Systems in Emerging Wireless Networks

Shihao Yan and Robert Malaney

packet transmission rate, the prover is considered malicious. In the context of location-based routing, the packet delivery ratio can be a performance criterion. However, packet end-to-end delay [21] is also a viable metric in scenarios where a malicious vehicle is assumed to not be forwarding the packet to the correct next hop.

In [24], a secure, no-infrastructure, cooperative LVS was proposed. This LVS was designed to prevent an attacker from falsely claiming it is further away from a verifier than it actually is. In this scheme, the verifier first estimates the prover's location according to time difference of arrival (TDOA) measurements. To do this, the verifier enlists the help of a neighbor that is common to both the verifier and prover. Then, the Euclidean distance error between the estimated and claimed locations of the prover is compared with a distance related to the expected processing delay (assuming a legitimate prover). The packet delivery ratio and end-to-end delay are used to evaluate the proposed location verification algorithm because the routing protocols are location-based [24].

In [23] the authors used onboard radar systems to verify a vehicle's claimed location (obtained through a GPS). Taking noise into account, the authors separately determined the GPS position tolerance shadow and radar position tolerance shadow. The proposed algorithm accepts the prover's claimed location if there is an intersection between the GPS and radar position shadows (or vice versa).

The threshold and performance of the proposed location verification algorithm are determined by the accuracy of the GPS and radar systems. The time required to detect a malicious user is the evaluation criterion. Again, in [23], routing protocols are location-based, and packet end-to-end delay and delivery ratio are also used. In [27], the authors of [23] also proposed a passive location verification algorithm that can work when the onboard radar is not available or cannot work because of obstacles. This passive algorithm creates a track record of location reports by using neighbor tables. A vehicle's neighbor table contains a list of other vehicles' identifications and locations that are within its range. If a prover's claimed location greatly deviates from the track record, the algorithm deems the prover malicious.

In [28], a location-verification algorithm for VANETs with location-based routing was proposed. This algorithm is based on a trusted neighbor (i.e. a vehicle whose location has been verified) and is executed in two steps. First, the time of arrival (TOA) of the challenge-response message between the verifier and prover is used to detect distance reduction attacks. Second, the verifier cooperates with one of its trusted neighbors to verify that the prover is at an intersecting region determined by the verifier and trusted neighbor. The area of the intersecting region is the performance criterion.

In [31], the authors described a scheme in which a verifier measures the time taken for a challenge-response message to travel from the verifier to the prover and back again. Then, the

estimated timeframe is calculated according to the prover's claimed location, and the two timeframes are compared. The authors of [31] conclude that this easily deployable scheme would be reliable in rural, urban, and Manhattan scenarios.

To overcome the non-line-of-sight (NLOS) problem in location verification systems, a cooperative LVS was proposed in [37]. The proposed scheme was designed so that a verifier could verify an NLOS prover. To estimate the distance between the prover and verifier, the protocol requests help from a cooperative vehicle that has LOS communication with both the prover and verifier. The distances between the cooperative vehicle and the prover, and from the cooperative vehicle to the verifier can be estimated using, for example, TDOA or TOA. This then allows for the distance between the prover and verifier to be calculated.

In addition, the distance between the verifier and prover's claimed location can be calculated. The main point of this protocol is its ability to verify the locations of vehicles that could not otherwise be verified because of obstacles.

The authors of [42] proposed a location verification algorithm dedicated to VANETs. A moving verifier (vehicle) can verify a static prover's claimed location without the assistance of roadside units or neighboring vehicles. With this algorithm, the moving verifier measures the TOA of signals transmitted by the static prover at three different locations along the moving verifier's trajectory.

Then, multilateration is used to determine the location of the prover from the three measurements. The Euclidean distance error between the prover's estimated and claimed locations is used as the test statistic, and the corresponding threshold is the average position estimation error. The test statistics and performance criteria used in the location verification algorithms described in this subsection are shown in **Table 1**.

3.2 Location Verification Using ROCs

A location-verification scheme based solely on messages exchanged between neighboring vehicles was proposed in [25]. The authors focused on detecting a malicious vehicle that falsely claims its position is as far away as possible (but within range) from the packet sender. This means that, when geographic routing protocols are used, the vehicle will be selected as the next hop. In [25], it is assumed that each vehicle has two directional antennas—forward and backward—and that each vehicle constructs two corresponding tables of one-hop neighbors. A decision about a prover is made by exchanging and comparing neighbor tables. The theoretic detection rate is derived as a function of the vehicle density. The higher the network density, the higher the probability that malicious vehicles will be detected in the proposed system.

A location-verification algorithm based on a vehicle's one-hop connectivity with other vehicles was proposed in [32]. With this algorithm, one-hop information is exchanged between vehicles so that each vehicle can create a two-hop

▼ **Table 1. Binary-decision, rule-based location verification algorithms for VANET**

Ref.	Test Statistics	Performance Criteria
[21]	acceptance range, mobility grade, maximum density, neighbor tables, etc.	packet delivery ratio
[22]	timestamp, acceptance range, velocity, packet transmit rate	packet end-to-end delay
[23]	error distance between radar estimated location and claimed location	time required to detect a malicious vehicle
[24]	Euclidean distance error between estimated and claimed locations	packet delivery ratio, packet end-to-end delay
[27]	difference between track records and claimed positions, neighbor tables	not provided
[28]	TOA of challenge-response message, acceptance range, roadway map, velocity	area of intersection region
[29]	communication range, speed and density, moved distance	packet delivery ratio
[31]	difference between measured and calculated round trip time	difference between measured and calculated round trip time and distances
[37]	difference between triangulation calculated and claimed distances	channel capacity utilization, packet delivery ratio, response time
[42]	Euclidean distance error between estimated location based on TDOA measurements and claimed location	average location estimation error

neighborhood connectivity diagram. Each vehicle then uses these diagrams to verify the location information being passed to it. Each vehicle constructs a plausibility area. If vehicle A cannot directly hear vehicle B because vehicle B is two hops away, then vehicle A should not be able to directly hear from a prover that claims to be further away than vehicle B. In [34], a map-guided trajectory-based location verification algorithm was proposed. With this algorithm, a plausibility area is constructed by using a prover's historical location and map information (e.g. road dimensions). To prevent a distance-enlarge-ment attack in a VANET, the authors of [38] also proposed a cooperative verification algorithm to verify a prover's claimed location. In this scheme, both the verifier and cooperating party can measure the TOA of the challenge-response messages from a prover.

By using such TOA measurements, both the verifier and cooperating party can locally verify whether the prover launched a distance-reduction attack. Within this location verification algorithm, the test statistic is the difference between the TOA-calculated distance and the distance derived from the prover's claimed location. The threshold is determined by using the processing delay of the challenge-response message. The cooperating party is selected so that the prover is located between the verifier and cooperating party. Therefore, the proposed cooperative algorithm can detect the distance-enlarge-ment attack. In the simulations run in [38], the detection rate is used to evaluate the proposed LVS.

In contrast to the previously reviewed works, which focus on the one-hop location verification, [43] proposes a beacon-based trust management system. This system combines one-hop and multihop verification algorithms to thwart internal attackers in VANETs. The authors used the cosine similarity [23] between the estimated vector (including position and ve-

locity) and claimed vector in order to determine the beacon trustworthiness of a neighboring vehicle. The Tanimoto coefficient between historical beacon messages and received event messages is used to calculate the one-hop event trustworthiness. An algorithm based on this one-hop even trustworthiness is then used to determine the multihop trustworthiness of an event message. Then, the Dempster-Shafer theory [65] is applied to combine all local event trustworthiness and determine the overall trustworthiness of an event message. Finally, an overall decision about the beacon message is made by comparing the overall trustworthiness with a trust threshold. Both the false positive rate and detection rate are performance criteria.

Sybil attacks may also compromise some location-based services in VANETs. A Sybil attack refers to a scenario in which a malicious vehicle illegitimately adopts multiple identities or locations to launch its attack. This type of attack may be launched by a selfish driver to mimic traffic congestion at some location on the road. It may be used to deter other vehicles from transiting along the driver's path. To detect such attacks, two location verification algorithms based on RSS measurements were proposed [44]. In the first algorithm in [44], the verifier estimates the prover's location through the minimum mean-square error on the distribution of RSS measurements. Then, the distance error between the estimated and claimed locations is used as the test statistic. In the second algorithm in [44], the test statistic is derived from the distributions of distance errors under H_0 and H_1 , and the threshold is derived from a given false positive rate. In the simulations run in [44], the detection rate is the performance criterion.

The test statistics and performance criteria used in the location verification algorithms reviewed in this subsection are shown in **Table 2**.

3.3 Information-Theoretic Location Verification Systems

In [40], the verifier uses the maximum likelihood estimator to estimate a prover's location based on RSS measurements. The Mahalanobis distance error between the estimated and claimed locations of the prover is used as the test statistic in the binary decision rule. The corresponding threshold is select-

▼ **Table 2. Location verification algorithms using ROCs for VANET**

Ref.	Test Statistics	Performance Criteria
[25]	number of neighbor vehicles	detection rate, packet delivery ratio, packet end-to-end delay
[32]	two-hop neighbors based plausibility area, RSS measurements	detection rate, false positive rate
[34]	map-guided trajectory based plausibility area, RSS measurements	detection rate, false positive rate
[38]	difference between estimated distance based on TDOA and calculated distance based on claimed location	detection rate, packet delivery ratio
[43]	overall trustworthiness of a message	false positive rate, detection rate, false negative rate, true negative rate
[44]	error distance between estimated and claimed locations, variance of this error distance	false positive rate, detection rate

Location Verification Systems in Emerging Wireless Networks

Shihao Yan and Robert Malaney

ed by maximizing the mutual information between the input and output of the LVS. A threshold selected in this manner does not completely optimize an LVS because the test statistic is not optimized.

The authors of [41] proved that the likelihood ratio is the optimal test statistic in terms of maximizing the mutual information between the input and output of an LVS.

With such a test statistic, an optimal information-theoretic LVS was obtained. To deploy the optimal information-theoretic location verification, three threat models were proposed [41]. In these models, the likelihood functions for RSS measurements could be obtained or approximated in closed forms. The information-theoretic and MAP frameworks lead to the same decision rule (likelihood ratio test with the same threshold) in the special case where $P(H_0) = P(H_1) = 0.5$ and the likelihood functions under H_0 and H_1 follow Gaussian distributions with the same variance.

The authors of [41] showed the objective nature of the optimization metric discussed in subsection 2.3. They also showed another useful property of an information-theoretic framework: The optimized threshold is not very sensitive to the a priori probabilities (Fig. 3). The optimal threshold in the MAP framework, which minimizes R_M for the likelihood ratio test, is a linear function of $P(H_1)$ (Fig. 3). This can be explained by the fact that the optimal threshold for minimizing R_M is $P(H_0) / P(H_1)$ [64].

However, the optimal threshold in the information-theoretic framework that maximizes $I(X; Y)$ for the likelihood ratio test converges to a constant as $P(H_1)$ approaches zero. Knowledge of the a priori probabilities is very difficult to obtain, and in practice, can only be assumed or roughly estimated. In most practical verification scenarios, $P(H_1)$ can be assumed to be quite small. Therefore, the behavior seen in Fig. 3, for the optimal information-theoretic threshold, gives an information-the-

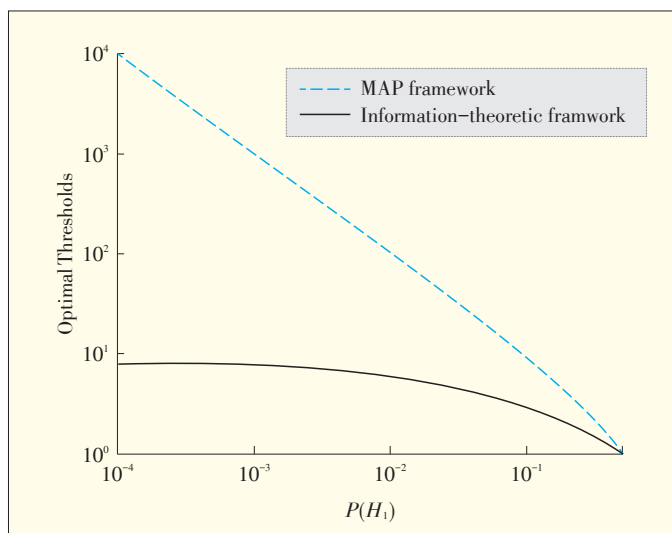
oretic framework a significant advantage over a Bayesian framework.

4 Location Verification Applicable to VANETs

Collecting received signal strengths does not require extra hardware, so many location verification systems for general wireless networks have been developed based on RSS measurements. In [3], the authors proposed an algorithm to detect location-spoofing attacks by matching the input instantaneous measurements with the normal signal fingerprints. From experimental results, the authors of [6] found that received signal strengths follow a mixture of two Gaussian distributions if the prover and verifier both have two antennas. To perform the verification, a likelihood ratio test can be constructed from the instantaneous measurements and expected normal profiles [6]. A location verification algorithm based on RSS fingerprints was proposed in [48]. The authors observed that only analyzing the residual of RSS measurements is not sufficient for robustly detecting location-spoofing attacks. However, if this residual is referenced to a claimed location, the residual can provide a verification algorithm that can resist various forms of attack.

In [52], the location verification was formulated as a statistical significance testing problem. The authors analyzed the spatial correlation of RSS measurements to detect location attacks. They derived theoretic false positive and detection rates in the one-dimensional and two-dimensional physical spaces. The authors of [52] also optimized the threshold in the proposed binary decision rule by minimizing the total error. They proposed a location verification algorithm robust against spoofing and Sybil attacks by using clustering methods [66]. The algorithms in [3], [6], [52], and [48] are similar to many RSS-based wireless local verification algorithms. In principal, they can all be easily adapted to the VANET environment.

Some generic challenge-response-based location verification algorithms for wireless networks have been proposed in [7], [45], and [50]. The well-known Echo protocol is based on the delay of the two challenge-response messages sent through wireless and ultrasonic channels [45]. The relative delay in the two channels is compared with the ideal theoretical delay, which is derived from a prover's claimed location. Applying the Echo protocol in a VANET requires vehicles to have both wireless and ultrasonic hardware for communication. A location verification protocol with hidden or mobile base stations was presented in [50]. Such mobile base stations can securely estimate the distances to the prover because the locations of the hidden or mobile base stations are assumed to be unknown to the prover. The distance error, which is the difference between the estimated and claimed locations of a prover, is compared with a threshold as a means of verification. This algorithm can be used in a VANET if the locations of some verifiers are not publicly known. In [7], several location-verification



▲ Figure 3. Optimal thresholds for information-theoretic and MAP frameworks as functions of $P(H_1)$ [41].

algorithms were proposed. These algorithms use a power-modulated challenge-response method to detect malicious vehicles. Adopting a power-modulated location verification algorithm to a VANET would be straightforward if the verifier in a VANET could adjust its transmit power.

The authors of [51] proposed a probabilistic location verification algorithm for a wireless sensor network (WSN) with high node density. In such networks, the number of hops that a packet sent by a prover must traverse in order to reach a verifier probabilistically depends on the Euclidean distance between the prover and verifier. The algorithm proposed in [51] verifies a prover's claimed location by checking the correlation between the number of hops and Euclidean distance (calculated from the prover's claimed location). In [54], two location verification algorithms were proposed for a WSN with a high node density. These algorithms exploit the inconsistencies between a prover's claimed location and the determination of the verifier's neighbor (one hop from the verifier) that it can hear the prover. The algorithms in [51] and [54] are used in a WSN with high node density. Similarly, these algorithms require the VANET to have a high vehicle density (i.e. they are suitable for urban scenarios).

The algorithms discussed in section 4 are a representative (but not exhaustive) selection of location verification algorithms proposed for other wireless networks. We have classified these algorithms as RSS-based, challenge-response based, or high-node-density based. There are other types of algorithms that could be adapted to VANETs.

5 Conclusion

In this paper, we have outlined the generic frameworks for location verification in VANETs. We have also discussed how much of the exiting literature on location verification for VANETs falls within such frameworks. With intelligent transport systems now becoming a key focus of transport departments worldwide, deployment of actual VANETs is close to reality. A mission-critical component of such networks is location verification. As such, the research reviewed in this paper is likely to be of increasing importance.

References

- [1] R. A. Malaney, "A location enabled wireless security system," in *Proc. IEEE GLOBECOM*, Texas, Nov. 2004, pp. 2196–2200.
- [2] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. of SASN'05*, Alexandria, VA, Nov. 2005, pp. 11–21.
- [3] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signal prints," in *Proc. of WiSe'06: ACM Workshop on Wireless Security*, Los Angeles, Sep. 2006, pp. 43–52.
- [4] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications – assumptions, requirements and principles," in *Proc. ESCAR*, Nov. 2006, pp. 5–14.
- [5] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
- [6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC-layer spoofing using received signal strength," in *Proc. IEEE INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 1768–1776.
- [7] Z. Yu, L. Zang, and W. Trappe, "Evaluation of localization attacks on power-modulated challenge-response systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 259–272, Jun. 2008.
- [8] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.
- [9] L. Bao, "Location authentication methods for wireless network access control" in *Proc. of IEEE International Conf. on Performance, Computing and Communications (IPCCC)*, Dec. 2008, pp. 160–167.
- [10] K. Bauer, D. McCoy, E. Anderson, and M. Breitenback, "The directional attack on wireless localization," in *Proc. IEEE GlobeCom*, Honolulu, Hawaii, Nov. 2009, pp. 1–6.
- [11] R. Zekavat and R. Buehrer, *Handbook of Position Location: Theory, Practice and Advances*. Piscataway: Wiley-IEEE Press, 2012.
- [12] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.
- [13] B. M. Ledvina, M. L. Psiaki, S. P. Powell, and P. M. Kintner, "Bitwise parallel algorithms for efficient software correlation applied to a GPS software receiver," *IEEE Trans. Wirel. Commun.*, vol. 3, no. 5, pp. 1469–1473, Sep. 2004.
- [14] N. O. Tuppenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: attacks on public WLAN – based positioning systems," *SysSec Technical Report*, Swiss Federal Institute of Technology, Swiss, Apr. 2008.
- [15] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, *Global Positioning System: Theory and Practice*, 4th ed., Germany: Springer Verlag, 1997.
- [16] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," *IEEE Pers. Commun.*, vol. 7, no. 5, pp. 28–34, Oct. 2000.
- [17] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN)*, Los Angeles, California, Apr. 2005, pp. 91–98.
- [18] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, Feb. 2006.
- [19] D. Liu, P. Ning, A. Liu, C. Wang, and W. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Information System Security*, vol. 11, no. 4, pp. 1–39, Jul. 2008.
- [20] A. Abu-Mahfouz and G. P. Hancke, "Distance bounding: a practical security solution for real-time location systems," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 16–27, Feb. 2013.
- [21] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.
- [22] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for VANETs," in *Proc. IEEE VTC Fall*, Baltimore, MD, Oct. 2007, pp. 26–30.
- [23] G. Yan, S. Olariu, and M. C. Weigle, "Providing vanet security through active position detection," *Computer Communications*, Vol. 31, no. 12, pp. 2883–2897, Jul. 2008.
- [24] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure location verification for vehicular ad-hoc networks," in *Proc. IEEE GLOBECOM*, New Orleans, LA, Dec. 2008, pp. 1–5.
- [25] Z. Ren, W. Li, and Q. Yang, "Location verification for VANETs routing," in *Proc. IEEE WIMOB*, Marrakech, Morocco, Oct. 2009, pp. 141–146.
- [26] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad-hoc network based on roadside units support," in *Proc. of the IEEE Military Communications Conference (MILCOM)*, Boston, Oct. 2009, pp. 1–7.
- [27] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009.
- [28] X. Xue, N. Lin, J. Ding, and Y. Ji, "A trusted neighbor table based location verification for VANET routing," in *Proc. of IET International Conference on Wireless, Mobile and Multimedia Networks (ICWMNN)*, Sep. 2010, pp. 1–5.
- [29] N. Alsharif, A. Wasef and X. Shen, "Mitigating the effects of position based routing attacks in vehicular ad hoc networks," in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011, pp. 1–5.
- [30] Y. Park, K. Rhee, and C. Sur, "A secure and location assurance protocol for location-aware services in VANETs," in *Proc. of Fifth International Conference*

Location Verification Systems in Emerging Wireless Networks

Shihao Yan and Robert Malaney

- on *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, Seoul, Korea, Jul. 2011, pp. 456–461.
- [31] H. D. Weerasinghe, R. Tackett, and H. Fu, "Verifying position and velocity for vehicular ad-hoc networks," *Security and Communication Networks*, vol. 4, no. 7, pp. 785–791, Jul. 2011.
 - [32] M. Abu-Elkheir, S. A. Hamid, H. S. Hassanein, I. M. Elhenawy, and S. Elmougy, "Position verification for vehicular networks via analyzing two-hop neighbors information," in *Proc. of IEEE Conference on Local Computer Networks (LCN)*, Bonn, Germany, Oct. 2011, pp. 805–812.
 - [33] Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil attack detection for position based applications in privacy preserved VANETs," in *Proc. IEEE GlobeCOM*, Houston, Texas, Dec. 2011, pp. 1–5.
 - [34] M. Abu-Elkheir, H. S. Hassanein, I. M. Elhenawy, and S. Elmougy, "Map-guided trajectory-based position verification for vehicular networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, Paris, France, Apr. 2012, pp. 2538–542.
 - [35] A. Jaeger, N. Bißmeyer, H. Stubing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of ITS Research*, vol. 10, no. 1, pp. 11–21, Jan. 2012.
 - [36] J. Grover, M. S. Gaur, V. Laxmi, and R. K. Tiwari, "Detection of incorrect position information using speed and time span verification in VANET," in *Proc. of the Fifth International Conference on Security of Information and Networks*, Jaipur, India, Oct. 2012, pp. 53–59.
 - [37] O. Abumansoor and A. Boukerche, "A secure cooperative approach for non-line-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 275–285, Jan. 2012.
 - [38] P. Zhang, Z. Zhang, and A. Boukerche, "Cooperative location verification for vehicular ad-hoc networks," in *Proc. IEEE ICC*, Ottawa, Canada, Jun. 2012, pp. 37–41.
 - [39] H. Rasheed, O. Heekuck, and K. Sangjin, "AntiSybil: standing against Sybil attacks in privacy-preserved VANET" in *Proc. of International Conference on Connected Vehicles and Expo (ICCVE)*, Dec. 2012, pp. 108–113.
 - [40] S. Yan, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *Proc. IEEE Globe COM*, Anaheim, California, Dec. 2012, pp. 5415–5420.
 - [41] "Optimal information theoretic wireless location verification," [Online]. Available: <http://arxiv.org/abs/1211.0737>
 - [42] S. Das and M. Saha, "Position verification in vehicular communications," in *Proc. of Fifth International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, Jan. 2013, pp. 1–2.
 - [43] Y. Chen and Y. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.
 - [44] B. Yu, C. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, Jun. 2013.
 - [45] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Workshop Wireless Security (WiSe '03)*, Sep. 2003, pp. 1–10.
 - [46] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, Oct. 2006.
 - [47] R. A. Malaney, "A secure and energy efficient scheme for wireless VoIP emergency service," in *Proc. IEEE GLOBECOM*, San Francisco, California, Nov. 2006, pp. 1–6.
 - [48] R. A. Malaney, "Securing Wi-Fi networks with position verification: extended version," *International J. Security Netw.*, vol. 2, pp. 27–36, Mar. 2007.
 - [49] R. A. Malaney, "Wireless intrusion detection using tracking verification," in *Proc. IEEE ICC*, Glasgow, Jun. 2007, pp. 1558–1563.
 - [50] S. Capkun, K. B. Rasmussen, M. Galaj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.
 - [51] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Ad Hoc Net.*, vol. 6, no. 2, pp. 195–209, Apr. 2008.
 - [52] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
 - [53] J. Chiang, J. Haas, J. Choi, and Y. Hu, "Secure location verification using simultaneous multilateration," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 584–591, Feb. 2012.
 - [54] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 5, pp. 938–950, May. 2013.
 - [55] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Influence of falsified position data on geographic ad-hoc routing," in *Proc. of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Visegrad, Hungary, Jul. 2005, pp. 102–112.
 - [56] T. Leinmüller and E. Schoch, "Greedy routing in highway scenarios: the impact of position faking nodes," in *Proc. WIT*, 2006.
 - [57] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30–39, Nov. 2001.
 - [58] Q. Yang, A. Lim, and P. Agrawal, "Connectivity aware routing in vehicular networks," in *Wireless Communications and Networking Conference*, Mar. 2008, pp. 2218–2223.
 - [59] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2625–2635, Jul. 2012.
 - [60] E. Bertino, B. Catania, M.L. Damiani, and P. Perlasca, "GEO-RBAC: a spatially aware RBAC," in *Proc. of the 10th ACM Symposium on Access Control Models and Technologies*, Pittsburgh, Jun. 2005, pp. 29–37.
 - [61] S. Chen, Y. Zhang, and W. Trappe, "Inverting sensor networks and actuating the environment for spatio-temporal access control" in *Proc. of the fourth ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, Oct. 2006, pp. 1–12.
 - [62] S. Capkun, M. Galaj, G. Karame, and N.O. Tippenhauer, "Integrity regions: authentication through presence in wireless networks," *IEEE Trans. Mob. Comput.*, vol. 9, no. 11, pp. 1608–1621, Nov. 2010.
 - [63] J. Neyman and E. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Phil. Trans. R. Soc. A*, vol. 231, pp. 289–337, Jan. 1933.
 - [64] M. Barkat, Signal Detection and Estimation. Boston, MA: Artech House, 2005.
 - [65] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, Nov. 2005.
 - [66] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning, Data Mining Inference, and Prediction*, New York: Springer-Verlag, 2001.

Manuscript received: June 23, 2013

Biographies

Shihao Yan (shihao.yan@student.unsw.edu.au) is a Ph.D student in the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He received his BS degree in communication engineering and MS degree in communication and information systems from Shandong University, China. His research interests are wireless communications and information theory, including physical layer security, location security and location verification algorithms.

Robert Malaney (r.malaney@unsw.edu.au) received his BS degree in physics from the University of Glasgow, UK. He received his PhD degree in physics from the University of St. Andrews, U.K. He is currently an associate professor in the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He has previously held positions at the California Institute of Technology, Pasadena; the University of California, Berkeley; the US Department of Energy National Laboratories, Washington, DC; and the University of Toronto, Canada. He was a principal research scientist with the Commonwealth Scientific and Industrial Research Organization, Australia. He has authored more than 100 technical publications and holds several patents.

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala
(Research School of Engineering, the Australian National University, Australia)

Abstract

Physical layer security is an emerging technique for improving wireless communication security, which is widely regarded as a complement to cryptographic technologies. To design physical layer security techniques for practical scenarios, uncertainty and imperfections in the channel knowledge need to be taken into account. This paper is a survey of recent research on physical layer security that considers imperfect channel state information (CSI) at communication nodes. We first give an overview of the main information-theoretic measures of secrecy performance with imperfect CSI. Then, we describe several signal processing enhancements in secure transmission designs. These enhancements include secure on-off transmission, beamforming with artificial noise, and secure communication assisted by relay nodes or in cognitive radio systems. Recent studies of physical layer security in large-scale decentralized wireless networks are also summarized. Finally, open problems for on-going and future research are discussed.

Keywords

physical layer security; fading channels; channel uncertainty; imperfect channel state information

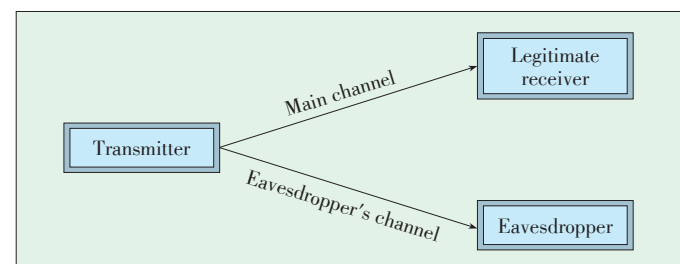
1 Introduction

Secure communication over wireless fading channels becomes a critical issue due to the broadcast nature of wireless networks. Traditionally, key-based cryptographic technologies [1] are used to secure the data transmission. However, the secrecy provided by cryptographic technologies is conditioned on the premise that the eavesdroppers have limited computational capability to decipher the message without the knowledge of secret keys. This premise has become controversial with the rapid development of computing devices. Physical layer security is an emerging research area that explores the possibility of achieving perfect-secrecy data transmission between legitimate network nodes, while malicious nodes eavesdropping the communication obtain zero information [2]. To achieve the secure communication over wireless channels, physical layer security does not rely on the encryption, but studies the time-varying property of fading channels, the smart design on channel codes, and the process on transmitted signals. The information-theoretic foundation of secret communication was laid by Shannon [3]. Wyner's pioneering work introduced the wiretap channel model as a basic framework for physical layer security [4], which was extended to broadcast channels with confidential messages described by Csiszár and Körner [5]. These early works have led to a signifi-

cant amount of recent research in which the fading characteristics of wireless channels has been taken into account. The basic system model of physical layer security over wireless channels is shown in **Fig. 1**.

Most works in this area rely on perfect knowledge of both the legitimate receiver and eavesdropper's channels at the transmitter to enable secure encoding and advanced signaling. However, the assumption of perfect knowing channel state information (CSI) is not realistic. In practical scenarios, there exist many reasons for imperfections in the CSI at the communication nodes. For example,

- No feedback from the eavesdroppers. When the eavesdropper is a passive entity, its CSI or even location is difficult to obtain at the legitimate transmitter. Also, if the eavesdrop-



▲ Figure 1. Basic system model of physical layer security over wireless channels.

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala

pers are malicious users, they will not expose their channel information to the legitimate party.

- Partial CSI feedback from the receivers. Receivers sometimes only provide partial CSI feedback to the transmitter, e.g., limited-rate feedback, channel direction feedback, and signal-to-noise ratio (SNR) feedback.
- Imperfect feedback links between the transmitter and receivers. When the feedback links are not error-free or delay-less, a noise component is added into the feedback information or else the CSI obtained at the transmitter is outdated.
- Channel estimation errors at receivers. Since the estimation of fading channels generally is not error-free, the CSI obtained at the receiver is not perfect.

Over the past few years, increasing attention has been paid to the impact of uncertainty in the CSI on both the legitimate receiver and eavesdropper's channels. The remainder of this paper is devoted to surveying and reviewing the literature on physical layer security with imperfect CSI¹ in wireless communications. We aim to provide a high-level overview of the current research on this field. In addition, this survey focuses on physical layer security research that does not involve the use of a secret key. Some work on physical layer security, e.g., [6]–[10], investigated the secure transmission with the key that can be observed by the eavesdropper over wireless channels.

The remainder of this paper is organized as follows. In Section 2, we discuss research done from the information-theoretic perspective. We present the main performance metrics for secure transmissions with imperfect CSI. In Section 3, we review signal processing secrecy enhancements in the secure transmission design that takes into account the imperfect CSI. Section 4 turns to the research on secrecy with channel uncertainty in large-scale decentralized wireless. Open problems and possible future research directions are described in Section 5. Finally, Section 6 concludes the paper.

2 Characterizations of the Performance Limits

The performance limits of secure transmission systems with full CSI are often characterized by the secrecy capacity. The secrecy capacity for the degraded wiretap channel with additive Gaussian noise (AWGN) is given by [11],

$$C_S = C_M - C_E, \quad (1)$$

where C_M and C_E denote the Shannon capacities of the main (legitimate receiver's) and eavesdropper's channels, respectively. A positive secrecy capacity can be obtained only when the legitimate receiver's channel is better than the eavesdropper's channel. When fading channels are considered, the main and eavesdropper's channels for a specific fading realization can be

regarded as complex AWGN channels. The Shannon capacities of one realization of the quasi-static fading channels are given by

$$C_M = \log_2(1 + \gamma_M), \quad (2)$$

$$C_E = \log_2(1 + \gamma_E), \quad (3)$$

where γ_M and γ_E are the instantaneous SNRs at the legitimate receiver and eavesdropper, respectively. The instantaneous SNR at the legitimate receiver is given by $\gamma_M = P |h_M|^2 / \sigma_M^2$, where P denotes the transmit power, h_M denotes the instantaneous channel gain at the legitimate receiver, and σ_M^2 denotes the receiver noise variance at the legitimate receiver. Also, the instantaneous SNR at the eavesdropper given by $\gamma_E = P |h_E|^2 / \sigma_E^2$, where h_E denotes the instantaneous channel gain at the eavesdropper and σ_E^2 denotes the receiver noise variance at the eavesdropper. Thus, the secrecy capacity for one realization of the quasi-static fading channels can be written as

$$C_S = \begin{cases} \log_2(1 + \gamma_M) - \log_2(1 + \gamma_E), & \text{if } \gamma_M > \gamma_E, \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

Note that, to achieve the secrecy capacity in (4), the transmitter needs perfect knowledge of both γ_M and γ_E .

To measure the performance of secure transmissions over fading channels with imperfect CSI, ergodic secrecy capacity and outage-based characterizations are often adopted. In the following, focusing on these two kinds of characterizations, we provide a review on the information-theoretic aspect of research in the field of physical layer security with imperfect CSI. In addition, we briefly describe the secrecy-degrees of freedom, which applies to systems with pessimistic and strong CSI assumptions.

2.1 Ergodic Secrecy Capacity

Ergodic secrecy capacity applies to delay tolerant systems in which the encoded messages are assumed to span sufficient channel realizations so that the ergodic features of the channel are captured. Ergodic secrecy capacity reveals the capacity limit under the constraint of perfect secrecy. Typical examples of delay tolerant applications are document transmission and e-mail, both of which belong in the category of non-real-time data traffic.

Gopala et al. [12] described ergodic secrecy capacity for both the case of full CSI and the case of only main channel's CSI available at the transmitter. The secrecy capacity for one realization of the quasi-static fading channels is given in (4). Averaged over all fading realizations, the ergodic secrecy capacity of fading channels with full CSI is given by

$$\bar{C}_S^{(F)} = \int_0^\infty \int_0^\infty (\log_2(1 + \gamma_M) - \log_2(1 + \gamma_E)) f(\gamma_M) f(\gamma_E) d\gamma_M d\gamma_E \quad (5)$$

where $f(\gamma_M)$ and $f(\gamma_E)$ are the distribution functions of γ_M and γ_E , respectively. Because the transmitter has full CSI on both channels, the transmitter can make sure that the transmission

¹ The work on systems with imperfect instantaneous CSI often covers the case of a system with no instantaneous CSI, since imperfect instantaneous CSI with very large uncertainty naturally converts to the case of no instantaneous CSI.

occurs only when $\gamma_M > \gamma_E$. When only the channel gain of the legitimate receiver is known at the transmitter, the ergodic secrecy capacity is given by

$$\bar{C}_S^{(M)} = \int_0^\infty \int_0^\infty [\log_2(1+\gamma_M) - \log_2(1+\gamma_E)]^+ f(\gamma_M) f(\gamma_E) d\gamma_M d\gamma_E \quad (6)$$

where $[x]^+ = \max\{x, 0\}$. Gopala et al. [12] also outlined a variable-rate transmission scheme to show the achievability of ergodic secrecy capacity with only main channel information. During a coherence interval with the received SNR at the legitimate receiver, γ_M , the transmitter transmits codewords at a rate of $\log_2(1+\gamma_M)$. This variable-rate scheme relies on the assumption of large coherence intervals and ensures that when $\gamma_M < \gamma_E$, the mutual information between the source and the eavesdropper is upper-bounded by $\log_2(1+\gamma_M)$. When $\gamma_M \geq \gamma_E$, this mutual information is equal to $\log_2(1+\gamma_E)$. Averaged over all the fading states, the achievable perfect secrecy rate is given as (6). The secure message is hidden across different fading states.

Fig. 2 compares the ergodic secrecy capacity of the network with full CSI at the transmitter and that of the network with only main channel CSI at the transmitter. The average channel qualities are $E\{|h_M|^2\} = E\{|h_E|^2\} = 1$, where $E\{\cdot\}$ is the expectation operation. The average power constraint is denoted by $\bar{P} = E\{P\}$. According to (5), the transmission occurs only when $|h_M|^2 > |h_E|^2$. Thus, the constant power level used for transmission with full CSI at the transmitter is $P = \bar{P} / \Pr(|h_M|^2 > |h_E|^2)$, where $\Pr(\cdot)$ denotes the probability measure. Note that $P = 0$ for $|h_M|^2 \leq |h_E|^2$, and hence $E\{P\} = \bar{P}$. On the other hand, the constant power level used for transmission with only main channel CSI at the transmitter is $P = \bar{P}$.

In addition, Khisti and Wornell [13] studied the ergodic secrecy capacity in multiple-input, single-output, multiple-eavesdropper (MISOME) systems. The authors developed upper and lower bounds on the ergodic secrecy capacity when there is perfect legitimate receiver's CSI and imperfect eavesdropper's CSI. The authors also investigated the ergodic secrecy

capacity of fast-fading channel for both high SNR and finitely many antennas, i.e., the number of transmitted antenna is very large. Rezki et al. [14], [15] studied the ergodic secrecy capacity for systems with imperfect CSI on both legitimate receiver and eavesdropper's channels at the transmitter. In [14], the authors presented a framework that characterizes the ergodic secrecy capacity of fast-fading channels when the legitimate receiver's CSI is imperfectly known at the transmitter. In [15], the authors established upper and lower bounds on the ergodic secrecy capacity for a single-input, single-output, single-eavesdropper (SISOSE) system with limited-rate feedback of the legitimate receiver's channel information.

2.2 Outage-Based Characterizations

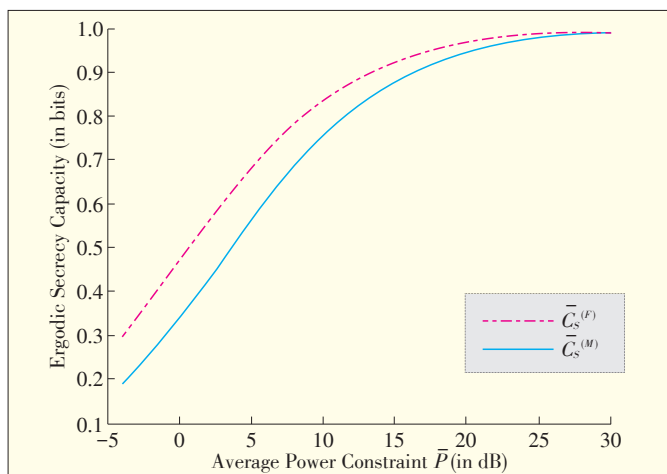
As mentioned before, the ergodic secrecy capacity applies to delay-tolerant systems which allow for the use of an ergodic version of fading channels. However, perfect secrecy cannot always be achieved for systems with stringent delay constraints, and ergodic secrecy capacity is inappropriate to characterize the performance limits of such systems. On the other hand, outage-based characterizations, which measure systems with probabilistic formulations, are more appropriate.

Assuming the fading is quasi-static, Parada and Blahut [16] analyzed the scenario where both legitimate receiver and eavesdropper's CSI is not available at the transmitter. The authors provided an alternative definition of outage probability. According to this definition, the secure communication can be guaranteed for the fraction of time when the legitimate receiver's channel is stronger than the eavesdropper's channel. Barros and Rodrigues [17] provided the first detailed characterization of the secrecy outage capacity where the outage probability, p_{out} , is characterized by the probability that a given target rate, R_s , is greater than the difference between instantaneous main channel capacity, C_M , and instantaneous eavesdropper's channel capacity, C_E . The outage probability is given by

$$p_{\text{out}} = \Pr(C_M - C_E < R_s). \quad (7)$$

The authors also showed that fading alone guarantees that physical layer security is achievable, even when the eavesdropper has a better average SNR than the legitimate receiver. In addition, Bloch et al. [2] characterized the relationship between the upper bound of the outage probability and the variance of the channel estimation error on eavesdropper's channel. The secrecy outage behavior of a multiple-input, single-output, single-eavesdropper (MISOME) fading system was studied in [18], where the authors suggested a relation between the degree of channel knowledge and the tolerable secrecy outage probability.

In [2], [16]–[18], the outage-based formulations capture the probability of having a reliable and secure transmission. Reliability and security are not differentiated, because an outage occurs whenever the transmission is either unreliable or not perfectly secure. Zhou et al. [19] presented an alternative se-



▲ **Figure 2.** Ergodic secrecy capacity versus average power constraint. The average channel qualities are $E\{|h_M|^2\} = E\{|h_E|^2\} = 1$.

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala

crecy outage formulation that directly measures the probability that a transmitted message is not perfectly secure. The alternative secrecy outage is given by

$$p_{so} = \Pr(C_E > R_M - R_S \mid \text{message transmission}), \quad (8)$$

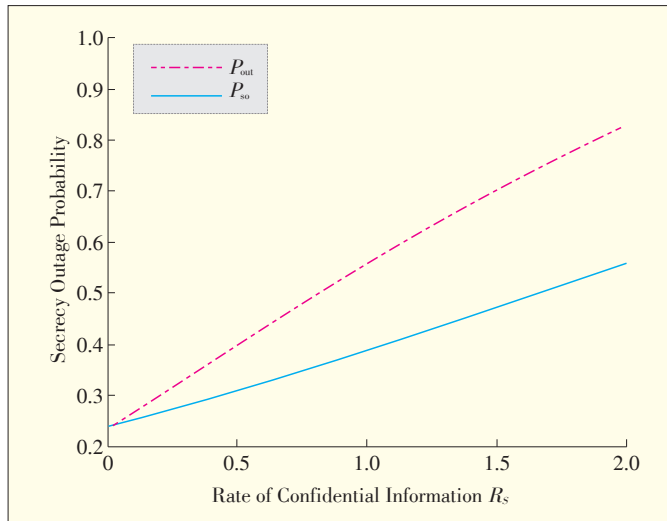
where R_M and R_S are the rate of transmitted codeword and the rate of the confidential information in the wire-tap code, respectively. The outage probability is conditioned on a message actually being transmitted. From (8), we see that the new formulation takes into account the system design parameters, such as the rate of transmitted codewords and the condition under which message transmissions take place. Therefore, the alternative secrecy outage formulation is useful for designing transmission schemes that meet target security requirements.

Fig. 3 compares the secrecy outage probability of not having a reliable and secure transmission, p_{out} in (7), and the secrecy outage probability of not having a secure transmission, p_{so} in (8). The average received SNRs are $E\{\gamma_M\} = E\{\gamma_E\} = 1$. The detailed discussion on the comparison of these secrecy outage probabilities can be found in [19].

2.3 Secrecy Degrees of Freedom

Alongside research on ergodic secrecy capacity and outage-based characterizations, another line of research, e.g., [20]–[24], studies the performance limits of systems with imperfect CSI under a pessimistic but strong assumption that allows the eavesdropper's channel to vary arbitrarily. These work analyzed the so-called secrecy degrees of freedom (SDoF), which is the pre-log of the secrecy capacity at high SNR and reveals the asymptotic behavior of the achievable secrecy rate in a high-SNR regime. The SDoF is formulated as

$$\text{SDoF} = \limsup_{\bar{P} \rightarrow \infty} \frac{R_S}{\log_2(\bar{P})}, \quad (9)$$



▲ **Figure 3.** Secrecy outage probability versus rate of confidential information. The average received SNRs are $E\{\gamma_M\} = E\{\gamma_E\} = 1$.

where \bar{P} denotes the average power constraint on transmitted signals.

The SDoF region for a single-user Gaussian multiple-input, multiple-output (MIMO) wiretap channel was investigated in [20]. The SDoF region of a two-user Gaussian MIMO broadcast channel with arbitrarily varying eavesdropper channel was found in [21]. The SDoF region for a two-user Gaussian MIMO multiple access channel and a Gaussian two-way channel with arbitrarily varying eavesdropper channel were given in [22] and [23], respectively. The SDoF region for a two-user MIMO interference channel with an external eavesdropper was given in [24]. In addition, there is a main limitation in this type of works, i.e., the legitimate receiver is always required to have an advantage over the eavesdropper in terms of the antenna number in order to get positive SDoF.

3 Signal Processing Secrecy Enhancements

In this section, we present signal processing techniques for enhancing secrecy of wireless communications. Specifically, secure on-off transmissions for signal-antenna channels, beamforming with artificial noise for multi-antenna channels, and secure design techniques for relay channel and cognitive radio systems are described in the following three subsections.

3.1 Secure On-off Transmissions for Single-Antenna Channels

Secure on-off transmission policy in wireless network designs generally works in the following way. The transmitter decides whether or not to transmit according to the knowledge of CSI on the legitimate receiver's channel, eavesdropper's channel, or both channels (if applicable). Transmission takes place whenever the estimated instantaneous CSI fulfills the requirements related to some given thresholds, e.g., SNR thresholds. Otherwise, transmission is suspended.

Gopala et al. [12] proposed a low-complexity, on-off power allocation strategy according to the instantaneous CSI on the legitimate receiver's channel, which approaches optimal performance for asymptotically high average SNR. Zhou et al. [19] designed two on-off transmission schemes, each of which guarantees a certain level of security whilst maximizing the throughput. With the statistics of eavesdropper's channel information, the first scheme requires CSI feedback from the legitimate receiver to the transmitter, and the second scheme only requires 1-bit feedback. Rezki et al. [14] studied a system in which the transmitter knows imperfect legitimate receiver's CSI and statistics of eavesdropper's channel. The authors derived the achievable rate of fast-fading channels with a simple on-off scheme and Gaussian input. In addition, under various assumptions on the CSI, He and Zhou [25] proposed several secure on-off transmission schemes, which maximize the throughput subject to a constraint on secrecy outage probability. Both fixed-rate and variable-rate transmissions were pro-

posed. The authors not only considered the imperfect CSI at the transmitter, but also studied the impact of imperfect CSI at the receiver side.

3.2 Beamforming with Artificial Noise for Multi-Antenna Channels

The work by Hero [26] is arguably the first to consider secret communication in a multi-antenna transmission system, and sparked significant efforts to this problem [27]. For multi-antenna channels with imperfect CSI, beamforming with artificial noise is the one of the most widely used techniques to secure the data transmission. Negi and Goel [28], [29] are the first to propose an artificial-noise injection strategy. As well as being allocated to transmitting information signals, part of the transmission power is allocated to generating artificial noise that confuses the eavesdropper. Specifically, the produced artificial noise lies in the null space of the legitimate receiver's channel, and the information signal is transmitted in the range space of the legitimate receiver's channel. This technique relies on the instantaneous CSI on the legitimate receiver's channel, but does not require the instantaneous CSI on the eavesdropper's channel. The legitimate receiver's channel nulls out the artificial noise. Thus, the legitimate receiver is not affected by the noise. The basic idea of beamforming with artificial noise is presented in Fig. 4.

In the following, we discuss the work that came after Negi and Goel's research, which focused on the beamforming with artificial noise in various multi-antenna channel scenarios with different assumptions on the availability of CSI. We first present the literature considering imperfect CSI on the eavesdropper's channel, and then discuss the work which considers the imperfect CSI on both eavesdropper and legitimate receiver's channels.

3.2.1 Imperfect CSI on Eavesdropper's Channel

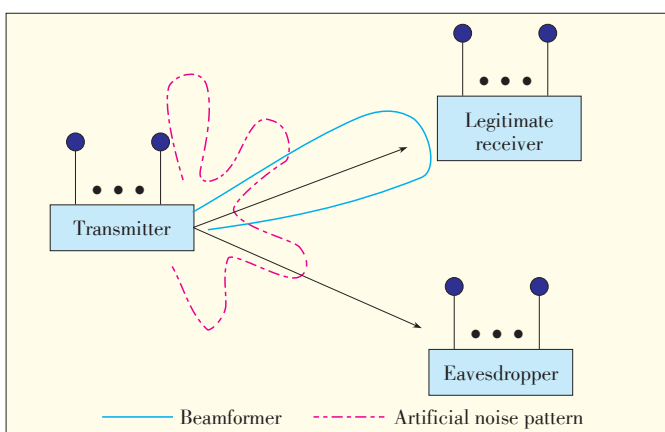
The work of Zhou and McKay [30] studied the optimal power allocation between the information signal and artificial noise in systems with both non-colluding and colluding eavesdrop-

pers. The authors found that, in the case of non-colluding eavesdroppers, the equal power allocation results in nearly the same secrecy rate as if power are optimally allocated. In the case of colluding eavesdroppers, they found that more power should be allocated to transmitting artificial noise as the number of eavesdroppers increases. In [31], Zhang et al. investigated the design of artificial-noise-aided secure multi-antenna transmission in slow-fading channels. The authors provided throughput-maximizing design solutions that include the optimal rate parameters of the wiretap code and the wise power-allocation strategy. Huang and Swindlehurst [32] obtained robust transmit covariance matrices on worst-case secrecy rate maximization under both individual and global power constraints. They investigated both cases of direct transmission and cooperative jamming with a helper. In addition, Gerbracht et al. [18] characterized optimal single-stream beamforming with the use of artificial noise to minimize the outage probability. They pointed out that the solution converges to maximum ratio transmission (MRT) for the case of no CSI to the eavesdropper, and the optimal beamforming vector converges to the generalized eigenvector solution with the growing level of CSI. Lin et al. [33] showed that the artificial noise selected in [29] is suboptimal. According to their study, the eigenvectors of the optimal covariance matrices of both information signals and generalized artificial noise are equal to the right singular vectors of the legitimate receiver's channel. Also, the power of artificial noise should be allocated uniformly over the eigenvectors. The rigorous proofs for these facts were also provided.

In [18], [29]–[33], although the instantaneous CSI on the eavesdropper's channel is not required, the transmitter still needs the statistics of eavesdropper's channel. For the case where no CSI on the eavesdropper's channel (including the statistics) is known at the transmitter, Swindlehurst and Mukherjee [34], [35] proposed a modified water-filling algorithm which balances the required transmit power with the number of spatial dimensions available for jamming the eavesdropper. As described in the modified water-filling algorithm, the transmitter first allocates enough power to meet a target performance criterion, e.g., SNR or rate, at the receiver, and then uses the remaining power to broadcast artificial noise. In [36], the authors also applied the similar algorithm to investigate the multi-user downlink channels in.

3.2.2 Imperfect CSI on Both Eavesdropper and Legitimate Receiver's Channels

The imperfect CSI on the legitimate receiver's channel at the transmitter mainly incurs two problems. First, without knowing the actual instantaneous CSI on the legitimate receiver's channel, the transmitter cannot make sure that the data transmission rate is not larger than the legitimate receiver's channel capacity. Then, a transmitted packet is unable to be decoded by the receiver, i.e., the packet is corrupted, whenever the data transmission rate exceeds the legitimate receiver's channel ca-



▲ Figure 4. An illustration of beamforming with artificial noise.

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala

capacity. Second, when the legitimate receiver's instantaneous CSI is imperfect, the artificial noise leaks into the legitimate receiver's channel, because the beamforming with artificial noise is designed according to the estimated instantaneous CSI rather than the actual instantaneous CSI. Therefore, the artificial noise interferes with the desired user, although it is intended to only confuse the eavesdropper. Naturally, the techniques applying to systems with perfect CSI on the legitimate receiver's channel become not optimal.

Taylor et al. [37] presented the impact of the legitimate receiver's channel estimation error on the performance of an eigenvector-based jamming technique. Their research showed that the ergodic secrecy rate provided by the jamming technique decreases rapidly as the channel estimation error increases. Mukherjee and Swindlehurst [38] also pointed out that the security provided by beamforming approaches is quite sensitive to imprecise channel estimates. The authors proposed a robust beamforming scheme for MIMO secure transmission systems with imperfect CSI of the legitimate receiver. Pei et al. [39] addressed a stochastic time-varying CSI uncertainty model with uplink-downlink reciprocity. Using this model, they proposed a new iterative algorithm to secure the transmission. The algorithm is robust against CSI errors. The authors of [30] investigated the effects of imperfect CSI on optimal power allocation and critical SNR for secure communications. They found that allocating power to the artificial noise for confusing the eavesdropper is better than increasing the signal strength for the legitimate receiver as the channel estimation error increases. Adapting the secrecy beamforming scheme, Liu et al. [40] investigated the joint design of training and data transmission signals for wiretap channels. The ergodic secrecy rate for systems with imperfect channel estimations at both the legitimate receiver and the eavesdropper was derived. The secrecy rate is difficult to be calculated, since the channel estimation errors cause non-Gaussianity of equivalent noise. The authors solved this problem by analyzing a large number of transmit antennas. Based on the achievable ergodic secrecy rate, the optimal tradeoff between the power used for training and data signals can be found. Furthermore, advocating the joint optimization of the transmit weights and artificial noise spatial distribution from a quality-of-service (QoS)-based perspective, Liao et al. [41] proposed a secret-transmit beamforming approach in accordance with the imperfect CSI on both the legitimate receiver and eavesdropper's channels. In [42], Ng et al. addressed a resource-allocation and scheduling optimization problem for orthogonal frequency division multiple access (OFDMA) networks. The optimization problem takes into account artificial noise generation and the effects of imperfect CSI in slow fading. The authors proposed a resource allocation algorithm that accounts for secrecy outage, channel outage, and the potentially detrimental effect of artificial noise generation. Considering the systems with partial CSI feedback, Lin et al. [43] investigated the scenario where only quantized channel

direction information (CDI) of the legitimate receiver's channel is available at the transmitter. Given the transmission power and a fixed number of feedback bits, the authors derived the optimal power allocation between the information signal and the artificial noise so that the secrecy rate is maximized.

In addition, it is necessary to mention that some works (e.g., [33], [44]–[46]) also studied the approaches to provide physical layer security for multi-antenna systems with imperfect CSI, but they did not rely on the use of artificial noise. Li and Petropulu [44] solved optimal input covariance that maximizes the ergodic secrecy rate subject to a power constraint in a MISOSE system with imperfect CSI on eavesdropper's channel. Li and Ma [45] formulated a transmit-covariance optimization problem for secrecy-rate maximization (SRM) of MISOME systems with imperfect CSI on both main and eavesdropper's channels. The authors of [33] analyzed systems with only statistics of the main and eavesdropper's channels at the transmitter. The authors showed that the secure beamforming can still achieve the secrecy capacity in such a scenario, and they proposed the optimal channel input covariance matrix, which fully characterizes the secrecy capacity. The authors also pointed out that artificial noise is not necessary in this case. Geraci et al. [46] studied the secrecy sum-rates achievable by regularized channel inversion (RCI) precoding in MISO systems with imperfect CSI.

3.3 Secure Designs for Relay Channels and Cognitive Radio Systems

Secure communication assisted by relay nodes is often regarded as a natural extension of secure transmission in multi-antenna networks. Physical layer security can be provided by careful signaling at different relays in the system. A virtual beam towards the legitimate receiver can be built by the collaboratively work among relay nodes, which is similar to secure transmission in multi-antenna systems. However, unlike the multiple-antenna transmission, the transmitter cannot directly control the relays. Goel and Negi [29] described a 2-phase protocol for the network of single-antenna wiretap channel with several relays. This protocol was designed to obtain coordination in transmitting artificial noise between the relays. In the first phase, the transmitter and the legitimate receiver both transmit independent artificial noise signals to the relays. Different linear combinations of these two signals are received by the relays and the eavesdropper. In the second phase, the relays replay a weighted version of the received signal, using a publicly available sequence of weights. Meanwhile, the transmitter transmits the confidential information, along with a weighted version of the artificial noise transmitted in the first stage. With the knowledge of the artificial noise component due to the legitimate receiver, the legitimate receiver is able to cancel off the artificial noise and get the confidential information. Assuming global full CSI at every node, the authors in [47] provided a detailed analysis on secure communications of one source-destination pair with the help of multi-

ple cooperating relays in the presence of one or more eavesdroppers. This analysis covered decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ) three different cooperative schemes.

To explore the effects of imperfect CSI in relay systems, researchers often consider the uncertainty of CSI on three kinds of links: relay-destination, relay-eavesdropper, and source-relay. The authors of [48] investigated the effect of imperfect CSI on the relay-eavesdropper channels. They proposed a DF relaying protocols for secure communication, which maximizes the lower bound on the ergodic secrecy capacity under a total relay transmission power constraint. Considering the imperfect CSI on the channels from relay to destination and from relay to eavesdropper, Zhang and Gursoy [49] provided optimization frameworks for the robust DF-based relay beamforming design. Furthermore, Vishwakarma and Chockalingam [50] computed the worst-case secrecy rate when there are imperfections in the CSI on all the links, i.e., relay-destination links, relay-eavesdropper links, and source-relay links.

Cognitive radio (CR) has been widely recognized as an effective technology to improve the utilization of wireless spectrum by allowing secondary users to coexist with primary users and access the spectrum of the prime system. In CR systems with secrecy message broadcasted in the primary links, the signals of secondary links for their users can also serve as the artificial noise for the secure primary link. In order to confuse the eavesdropper overhearing the primary links, the secondary system operates similar to that of the helper nodes, but simultaneously serves their own receivers. The papers that study the imperfect CSI in such cognitive radio systems can be found in [51] and references within. The authors of [51] explored MISO CR systems where the secondary system secures the primary communication in return for permission to use the spectrum. On the other hand, when the secondary user transmitter sends confidential information to a secondary user receiver on the same frequency band as that of a primary user, the requirement of not interfering the primary user is often treated as a power constraint on the transmitted signals in the secondary system. Assuming all CSI is imperfect known, Pei et. al [52] explored an optimal secondary user transmitter design, which maximizes the secure transmission rate of the secondary link while avoiding harmful interference to primary users. The authors proposed two approaches to solving this challenging optimization problem, which is non-convex and semi-infinite.

4 Secrecy in Large-Scale Decentralized Wireless Networks

In the last section, we summarized the research results on physical layer security enhancements for systems consisting of a small number of nodes. We now turn our attention to another very important class of wireless networks: large-scale decentralized wireless networks. In such networks, the CSI of eaves-

droppers is rarely available at legitimate users. Even the locations of eavesdroppers may not be known. The lack of eavesdropper's information makes communication security a challenging problem. Apart from that, the decentralized nature of the network rules out any global optimization approach for secrecy enhancements. Pioneering works on physical layer security in large-scale decentralized wireless networks focused on the connectivity analysis. Specifically, the notion of secrecy graph was introduced in [53] and further developed in [54] to include fading channels. Various secure connectivity improvements were discussed in [55], [56], including multi-antenna sectoring and beamforming. The connectivity in the presence of the location uncertainty of eavesdroppers was studied in [57].

Building on the connectivity analysis of the secrecy graph, the secrecy capacity scaling was analyzed in [58]–[62]. Specifically, the studies in [58], [59] showed that the secrecy requirement does not reduce the capacity scaling of the network, i.e., the capacity scaling law is the same for both insecure message transmission and secure message transmission. Of course, achieving such an optimal scaling law under the secrecy constraint requires very different transmission and access protocols. For example, when eavesdroppers' locations are unknown, various secrecy enhancements such as cooperative jamming and multi-path transmission in conjunction with network coding may be required [61], [62].

Although the scaling law results may provide insights into the asymptotic secrecy throughput performance of large-scale networks, a finer view of throughput is necessary to better understand the impact of key system parameters and transmission protocols, since most of design choices affect the actual (non-asymptotic) throughput but not the scaling behaviors. To this end, a new performance metric named secrecy transmission capacity was developed in [63], [64] to capture the area spectral efficiency of secure transmission. The formulation of such a metric was based on the outage approach in [19] which accommodates a practical scenario where the CSI of the eavesdroppers is unknown to the legitimate nodes.

5 Open Problems and Discussions

Despite the increasing attention paid to the effect of imperfect CSI on physical layer security, research on this area is still at an early stage. In this section, we discuss some open problems in the research area of physical layer security with imperfect CSI.

5.1 Imperfect Channel Estimation at Receivers

For research on physical layer security considering imperfect CSI, most of the existing works investigate the impact of imperfect CSI at the transmitter but assume perfect channel estimation at receivers. Only a few works, e.g., [25], [30], [40], paid attention to the imperfect channel estimation at receivers. Clearly, the assumption of perfect channel estimation at the re-

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala

ceiver is not very practical, since the estimation of fading channels generally is not error-free. In principle, the channel estimation error exists at both the legitimate receiver and the eavesdropper. Assuming perfect estimation at the eavesdropper is more reasonable from the secure transmission design point of view, since it is often difficult or impossible for the transmitter to know the accuracy of the eavesdropper's channel estimate. Nevertheless, in scenarios where the eavesdropper is just an ordinary network user whose performance and other information can be tracked by the transmitter, e.g., [13], [65], [66], the consideration of imperfect channel estimation at the eavesdropper becomes relevant.

5.2 Imperfect Knowledge of Eavesdroppers' Locations

With few exceptions, almost all the existing research on physical layer security assumed that the eavesdropper's location is perfectly known. The validity of such an assumption strongly depends on the application under investigation. For example, when the eavesdropper is a passive entity without transmission, its location is very hard to obtain. Also, in large-scale complex networks, it is very difficult to determine eavesdroppers' locations due to the random deployments or mobility of nodes. Therefore, it is an interesting research direction to consider the secrecy in networks with imperfect or no knowledge of the eavesdropper's location at the transmitter.

6 Conclusions

In this paper, we have reviewed the research on physical layer security with practical assumptions on fading channel information. For the characterizations of performance limits, we described ergodic secrecy capacity suitable for delay tolerant systems, outage-based characterizations for systems with stringent delay constraints, and secrecy degrees of freedom. Also, we surveyed signal processing secrecy enhancements proposed for different transmission scenarios, i.e., secure on-off transmission for signal-antenna channels, beamforming with artificial noise for multi-antenna channels, and other signaling designs for relay channels or cognitive radio systems. In addition, recent findings on secrecy in large-scale decentralized wireless networks were reviewed. Future research directions on physical layer security with imperfect CSI include the imperfect channel estimation at receiver sides and the imperfect knowledge of eavesdroppers' locations.

References

- [1] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.
- [2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
- [4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [6] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.
- [7] —, "Secret-key agreement over unauthenticated public channels—Part II: the simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
- [8] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Proc. IEEE ISIT*, Seoul, Korea, June 2009, pp. 2296–2300.
- [9] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.
- [10] L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multi-commodity flow in networks," in *Proc. IEEE ITW*, Lausanne, Switzerland, Sept. 2012, pp. 627–631.
- [11] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [12] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
- [14] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, Nov. 2011, pp. 952–957.
- [15] —, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE ISIT*, Cambridge, MA, July 2012, pp. 239–243.
- [16] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Adelaide, SA, Sept. 2005, pp. 2152–2155.
- [17] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, July 2006, pp. 356–360.
- [18] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
- [19] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
- [20] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," submitted to *IEEE Trans. Inf. Theory*, July 2010. [Online]. Available: <http://arxiv.org/abs/1007.4801>.
- [21] X. He, A. Khisti, and A. Yener, "MIMO broadcast channel with arbitrarily varying eavesdropper channel: Secrecy degrees of freedom," in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011.
- [22] —, "MIMO multiple access channel with an arbitrarily varying eavesdropper," in *Proc. Allerton Conf. Commun., Control Computing*, Monticello, IL, Sept. 2011.
- [23] X. He and A. Yener, "Gaussian two-way wiretap channel with an arbitrarily varying eavesdropper," in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011.
- [24] —, "The Gaussian interference wiretap channel when the eavesdropper channel is arbitrarily varying," in *Proc. IEEE ISIT*, Cambridge, MA, July 2012.
- [25] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," submitted to *IEEE Trans. Inf. Forensics Security*, Apr. 2013. [Online]. Available: <http://arxiv.org/abs/1304.6485>.
- [26] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
- [27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principle of physical layer security in multiuser wireless networks: A survey," Nov. 2010. [Online]. Available: <http://arxiv.org/abs/1011.3754>.
- [28] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE VTC*, vol. 3, Dallas, TX, Sept. 2005, pp. 1906–1910.
- [29] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.
- [30] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [31] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," to appear in *IEEE Trans. Veh. Technol.*, 2013. [Online]. Available: <http://arxiv.org/abs/1212.364>.

Wireless Physical Layer Security with Imperfect Channel State Information: A Survey

Biao He, Xiangyun Zhou, and Thushara D. Abhayapala

- [32] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
- [33] P.-H. Lin, S.-C. Lin, S.-H. Lai, and H.-J. Su, "On secure beamforming for wiretap channels with partial channel state information at the transmitter," in *Proc. APSIPA ASC*, Hollywood, CA, Dec 2012, pp. 1–5.
- [34] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.
- [35] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE SPAWC Workshop*, Perugia, Italy, June 2009, pp. 344–348.
- [36] —, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton Conf. Commun., Control Computing*, Monticello, IL, Oct. 2009, pp. 1134–1140.
- [37] J. M. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in wireless networks," in *Proc. IEEE CAMAD Workshop*, Kyoto, Japan, June 2011, pp. 122–126.
- [38] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [39] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.
- [40] T.-Y. Liu, S.-C. Lin, T.-H. Chang, and Y.-W. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. IEEE ICC*, Ottawa, ON, June 2012, pp. 4782–4787.
- [41] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
- [42] D. W. K. Ng, E. S. Lo, and R. Schober, "Resource allocation for secure OFDMA networks with imperfect CSIT," in *Proc. IEEE GLOBECOM*, Houston, TX, Dec. 2011, pp. 1–6.
- [43] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
- [44] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 4, no. 10, pp. 1176–1187, Apr. 2011.
- [45] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.
- [46] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Secrecy sum-rates with regularized channel inversion precoding under imperfect CSI at the transmitter," in *Proc. IEEE ICASSP*, May 2013.
- [47] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [48] —, "Secure wireless communications via cooperation," in *Proc. Allerton Conf. Commun., Control Computing*, Urbana-Champaign, IL, Sept. 2008, pp. 1132–1138.
- [49] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical layer security," in *Proc. CISS*, Princeton, NJ, Mar. 2010, pp. 1–6.
- [50] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with imperfect CSI and multiple eavesdroppers," in *Proc. IEEE SPAWC Workshop*, Cesme, June 2012, pp. 439–443.
- [51] T. Kwon, V. W. S. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *Proc. IEEE GLOBECOM*, Anaheim, CA, Dec. 2012, pp. 1236–1241.
- [52] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multi-antenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.
- [53] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE ISIT*, Toronto, ON, July 2008, pp. 539–543.
- [54] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
- [55] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.
- [56] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
- [57] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE ISIT*, Austin, TX, June 2010, pp. 2627–2631.
- [58] S. Vasudevan, D. Goeckel, and D. Towsley, "Security versus capacity tradeoffs in large wireless networks using keyless secrecy," *ACM Mobi-Hoc*, Sept. 2010.
- [59] O. O. Koyluoglu, C. E. Koksul, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
- [60] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE ISIT*, Seoul, Korea, June 2009, pp. 1189–1193.
- [61] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. IEEE INFOCOM*, Orlando, FL, Mar. 2012, pp. 1152–1160.
- [62] C. Capar and D. Goeckel, "Network coding for facilitating secrecy in large wireless networks," in *Proc. CISS*, Princeton, NJ, Mar. 2012, pp. 1–6.
- [63] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [64] X. Zhou, M. Tao, and R. A. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE ICC*, Ottawa, ON, June 2012, pp. 2339–2344.
- [65] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.
- [66] C. Y. Leow, C. C. Capar, D. Goeckel, and K. K. Leung, "Two-way secrecy schemes for the broadcast channel with internal eavesdroppers," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, Nov. 2011, pp. 1840–1844.

Manuscript received: May 28, 2013

Biographies

Biao He (biao.he@anu.edu.au) received the B.E. (hons.) degree in electronic and communication systems from the Australian National University (ANU) in 2012. At the same year, he received the B.E. degree in information engineering from Beijing Institute of Technology (BIT). Currently, he is pursuing his Ph.D. degree in the research school of engineering in ANU. His research interests include physical layer security, wireless communications, and information theory.

Xiangyun Zhou (xiangyun.zhou@anu.edu.au) is a Lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK – University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory and wireless networks. He has a large number of publications in the specific area of physical layer security, including an edited book entitled *Physical Layer Security in Wireless Networks* published by CRC Press in 2013. Dr. Zhou serves on the editorial board of the following journals: *IEEE Communications Letters*, *Security and Communication Networks* (Wiley), and *Ad Hoc & Sensor Wireless Networks*. He has also served as the TPC member of major IEEE conferences. Currently, he is the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

Thushara D. Abhayapala (thushara.abhayapala@anu.edu.au) received the B.E. degree (hons.) in Engineering in 1994 and the Ph.D. degree in Telecommunications Engineering in 1999, both from the Australian National University (ANU), Canberra. He is a Professor and the Director of the Research School of Engineering at ANU. He was the Leader of the Wireless Signal Processing (WSP) Program at the National ICT Australia (NICTA) from November 2005 to June 2007. His research interests are in the areas of spatial audio and acoustic signal processing, space-time signal processing for wireless communication systems, and array signal processing. He has supervised over 30 research students and coauthored over 190 peer-reviewed papers. He is an Associate Editor of *IEEE/ACM Transactions on Audio, Speech, and Language Processing* and the *EURASIP Journal on Wireless Communications and Networking*. He is also a Member of the Audio and Acoustic Signal Processing Technical Committee (2011–2013) of the IEEE Signal Processing Society.

Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics

Syed Taha Ali and Vijay Sivaraman

(School of Electrical Engineering and Telecommunications, University of New South Wales, NSW 2052, Australia)

Abstract

In this article, we give an overview of current research on shared secret-key agreement between two parties. This agreement is based on radio wireless channel characteristics. We discuss the advantages of this approach over traditional cryptographic mechanisms and present the theoretical background of this approach. We then give a detailed description of the key-agreement process and the threat model, and we summarize the typical performance metrics for shared secret-key agreement. There are four processes in shared secret-key agreement: sampling, quantization, information reconciliation, and privacy amplification. We classify prior and current research in this area according to innovation on these four processes. We conclude with a discussion of existing challenges and directions for future work.

Keywords

physical-layer security; secret key generation

1 Introduction

The Diffie-Hellman key exchange protocol is the de facto mechanism for cryptographic secret-key agreement [1]. Relying on the intractability of the discrete logarithm problem, two parties with no prior knowledge of each other are able to exchange public messages over an insecure communications channel and arrive at a shared secret key that is safe from an eavesdropper and that can be used for encrypting communications between themselves. Research interest has recently revived an alternative approach to secret-key agreement. Two parties (Alice and Bob) who are communicating using radios can exploit unique spatio-temporal properties of the wireless channel between them to generate a shared secret. Due to the highly unpredictable and symmetric nature of multipath propagation, the wireless channel that Alice and Bob share is unique to them. It is reciprocal and cannot be deduced in detail by an eavesdropper (Eve). The wireless channel is also highly sensitive to motion and changes in the environment, and variations can be quantized independently by Alice and Bob to yield a shared secret key that Eve has no access to.

This approach has several advantages. First, security implemented at higher layers in the protocol stack can be undermined at the lower layers, and an argument has been made that security should be implemented at multiple layers, if possible. An early research effort in this domain [2] strongly emphasized

that physical layer security can complement existing cryptographic solutions and help build systems that are more secure overall. The physical layer has, thus far, mostly been neglected in the stack. This is unfortunate because the physical wireless link can be a rich source of randomness, (due to signal noise and highly sensitive channel states). The physical wireless link is also a means of deriving shared secrets because of the high correlation in channel characteristics at two ends of a link. These advantages can be easily harnessed because most radios today already have hardware support for performing basic channel estimates, such as measuring radio signal strength.

Second, prevailing cryptographic techniques are based on difficult number theory problems, i.e. these techniques rely on certain assumptions about the adversary's computing power. In contrast, physical layer approaches offer information-theoretic security, also referred to as unconditional security. Even with unlimited computing power, advances in number theory, and the advent of quantum computing, an adversary still cannot break information-theoretic schemes.

Third, traditional cryptographic mechanisms can be resource-intensive and impractical to implement in hardware. This is especially critical for newly emerging computing paradigms, such as Smart Dust, RFID chips, body area networks, and the Internet of Things, which are all based on miniaturized, resource-constrained wireless devices. Devices such as wireless sensors are not typically equipped with secure clocks or powerful pseudorandom number generators, in which case

the Diffie–Hellman key exchange may not lead to truly random keys. Furthermore, research indicates that the Diffie–Hellman key exchange is not very practical to execute on sensor devices [3].

Secret-key agreement using wireless channel characteristics is essentially a four-step process. Alice and Bob first sample the wireless channel to obtain correlated estimates of the channel state. They individually quantize these estimates to yield closely matching bit sequences, or bitstrings. This is followed by an information reconciliation process in which Alice and Bob identify and correct mismatching bits in their bitstrings. Then, there is a privacy amplification step in which a transform operation is used to minimize Eve's knowledge of the shared bitstring. The result is a secret key shared by Alice and Bob that they can use to encrypt communications between themselves. Research in this domain has mostly focused on innovating at different steps of the key-agreement process, and this technique has been validated using different wireless technologies and in various environments.

In section 2, we briefly introduce secret-key agreement using wireless channel characteristics. We discuss the threat model, and we summarize the performance metrics most commonly used. In section 3, we give an overview of existing research in this domain, categorized as per the four steps of the process, i.e. sampling, quantization, information reconciliation, and privacy amplification. In section 4, we discuss alternative methods of using the wireless channel for secret-key agreement. We also discuss potential attacks in this space and outline possible directions for future work. Section 5 concludes the paper.

2 Basic Principles

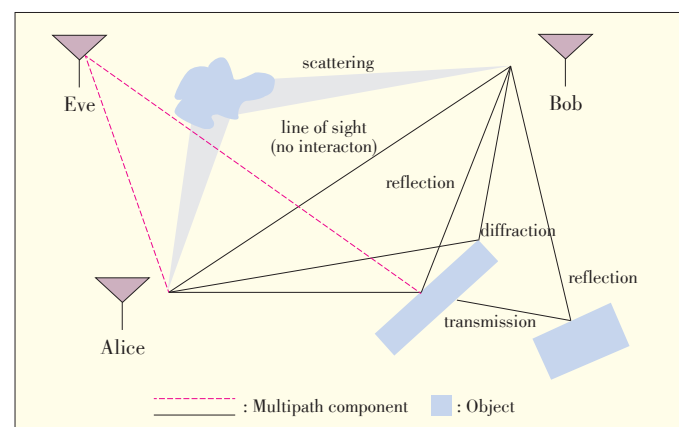
The groundwork for physical layer security was laid in 1975, when Wyner introduced the classic wiretap model [4] and demonstrated that two parties (Alice and Bob) could communicate securely without a shared secret key and assuming that the illegal channel that Eve uses for eavesdropping is a noisier version of the legitimate Alice–Bob channel. The trick here is for Alice and Bob to use sufficiently large code words to encode their messages and to prevent Eve from successfully deciphering the noisier version of data that she receives. In the early nineties, Maurer [5], [6] proved that Alice and Bob could communicate securely with even fewer restrictions. Even if Eve has access to a less noisy channel than the Alice–Bob channel, Alice and Bob can still agree on a shared secret key if they generated correlated random sequences and then harmonized their observations by exchanging public messages on an error-free channel. The process could be devised using obfuscation techniques so that even if Eve were to access these public messages, her knowledge of the shared secret would still be negligible.

The concept of two parties generating correlated random se-

quences, perfected via public discussion and obfuscated from third parties, is very applicable to the wireless medium. The wireless channel has an intrinsic symmetry because of the reciprocity of electromagnetic propagation. If Alice and Bob were to transmit identical signals to each other, using identical transceivers and antennas and in the absence of interference and noise, they would receive perfectly identical signals. Radio signals take multiple paths from the source to the destination where, depending on the particular path, they undergo reflection, diffraction, and scattering. The signals also experience different amounts of delay, attenuation, and phase distortion. Alice and Bob can both therefore measure a set of parameters defined by the cumulative effects of all these paths on the signal at their ends. In ideal conditions, these measurements agree.

If Alice and Bob collect a time series of these channel state measurements over a period of sufficient variation, the channel state profile (or envelope) can be directly quantized into a shared secret key that is unique to their positions in that particular environment at that point in time. If Eve is located more than one radio wavelength away from either Alice or Bob, she will be limited to measuring an entirely different channel and will not be able to deduce the legitimate channel spectra or the shared secret. This concept, is shown in **Fig. 1** and described by a Jake uniform scattering model [7], which is well-known in the field. According to this model, there is a rapid decorrelation in the signal over a distance of approximately half a wavelength, and for a separation of one to two wavelengths or more, the signals can be assumed to be independent. In the 2.4 GHz range, our threat model would require Eve to be situated 6.25 cm or more away from Alice and Bob.

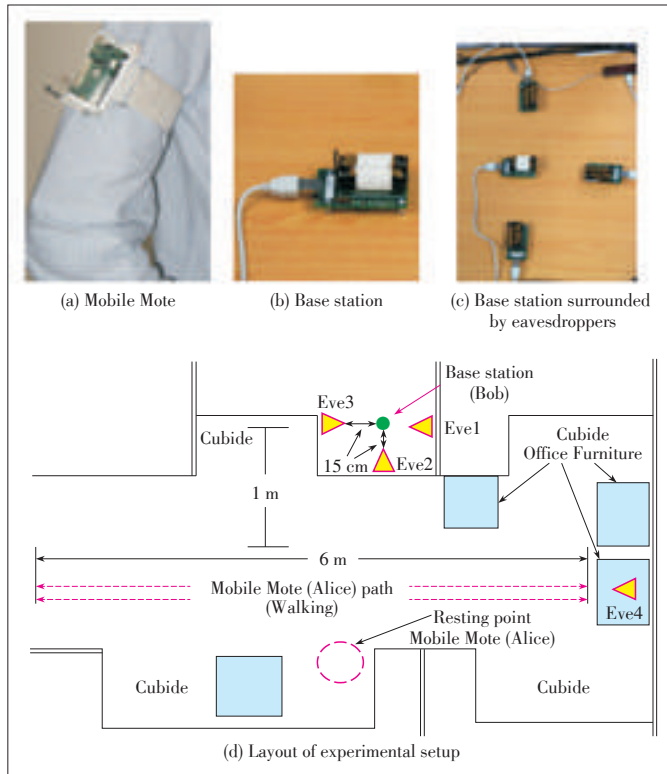
Fig. 2 shows an indoor office environment at the Faculty of Electrical Engineering, University of New South Wales. A base station (Bob) communicates with a wearable mobile device (Alice) walking along the path illustrated. Multiple stationary eavesdroppers (Eve 1 and Eve 4) are in close to the base station, separated by a distance of 15 cm on either side. Alice and Bob send messages at a rate of 1 packet per second, sampling



▲ **Figure 1.** Multipath propagation in indoor setting.

Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics

Syed Taha Ali and Vijay Sivaraman



▲ Figure 2. Mobile node, base station, and experimental layout for indoor environment.

the channel in succession, and all parties record the received signal strength indication (RSSI) as an estimation of the channel state. **Fig. 3** shows the channel state measured over a one minute interval. Alice and Bob are in very good agreement with slight discrepancies with regard to the channel profile. Furthermore, the eavesdroppers drop a large number of packets and are unable to replicate the channel profile in significant detail. This confirms that Alice and Bob can use these measurements to generate shared secret keys.

In practice, all parties experience low-amplitude asymmetric components in their channel measurements because of factors such as random noise, transceiver differences, interference, motion, or sampling delay (caused by half-duplex radios). Quantizing these channel estimations may therefore result in discrepancies in the generated bit sequence. Information-reconciliation protocols are used to resolve these disagreements. In these protocols, Alice and Bob publicly exchange data about their bit sequences (through, for example, parity checks) to identify and correct mismatching bits. This is followed by a privacy amplification step, which eliminates the partial information that Eve has deduced about the shared secret. This step usually involves a transformation operation, such as using a hash function.

Typically, key agreement, secret bit generation rate, entropy, and implementation costs and overheads are the performance metrics used to measure the efficiency of wireless chan-

nel-based key agreement.

Key agreement is the fraction of matching bits in the sequences generated by Alice and Bob. Ideally, this should be 100%, and whatever mismatches occur (due to practical considerations) are resolved using information reconciliation. Very high agreement rates, i.e. greater than 99%, have been achieved in the literature [8]. Eavesdroppers, on the other hand, should match in about 50% of the bits they generate by listening to the Alice-Bob transmissions. The probability of eavesdroppers guessing the right bit is equivalent to a fair coin toss, i.e. there is no advantage at all.

The secret bit generation rate is the average number of usable secret key bits extracted from the wireless channel per unit time. This value depends on various factors, such as the channel sampling rate, quantization parameters, deployment scenario, and channel variability. Bit generation rates in the literature range from 1 bit/s [2] to 40 bits/s [9].

Entropy is a measure of the uncertainty or inherent randomness in the generated bits. Typically, the entropy of a random variable X over a set of n symbols x_1, x_2, \dots, x_n is given by

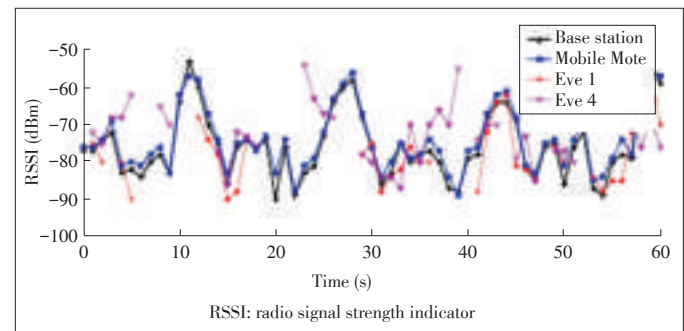
$$H(X) = -\sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (1)$$

where $p(x_i)$ is the probability of the occurrence of symbol x_i . For binary symbols, a value close to 1 indicates high entropy. In the literature, the NIST test suite [10] is typically used to validate the entropy for the generated bits.

Implementation cost and overheads depend on the particular mechanism used to generate bits. Whereas this technique has been demonstrated to work with off-the-shelf hardware, in instances such as that in [11], specialized hardware is required. Furthermore, information reconciliation mechanisms, such as Cascade, require storage and repeated manipulation of large arrays of data. Large-scale data transmission involves significant processing costs [12], which is a serious consideration for resource-constrained devices, such as wireless sensors.

3 Process

In this section, we describe current research on shared se-

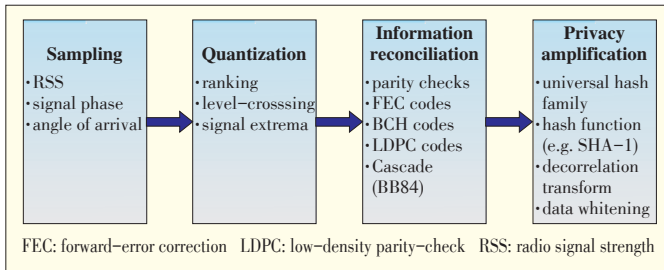


▲ Figure 3. Measurements comparing RSSI in an indoor office environment.

cret key agreement using the wireless channel. A pictorial summary is shown in **Fig. 4**.

3.1 Channel Sampling

Various wireless channel characteristics have been investi-



▲ **Figure 4.** Classification of methodologies for secret-key agreement.

gated in the literature. Radio signal strength (RSS), discussed in [2], [13] and [14], is the most popular characteristic because it already exists in most off-the-shelf radios. Schemes using signal phase [15], angle of arrival [11], and deep fades [16] have also been successfully used for secret-key agreement.

It is imperative that there is sufficient fluctuation in the channel over a period of time so that the generated key has acceptable entropy. This can be a problem in static deployments, and motion on the part of Alice or Bob has been recommended in several research efforts [13], [17]. An alternative approach to generating signal variation in a static setting is channel-hopping. The wireless channel is also frequency-sensitive, so channel characteristics can be measured over a range of frequencies to generate a shared secret [14].

Non-identical hardware may result in Alice and Bob having different channel state measurements. Experiments performed by Jana et al. [13] have shown that heterogeneous hardware may result in a consistent value offset at the two ends, and the resulting channel profile is relatively consistent for Alice and Bob. For this reason, instead of encoding absolute channel measurements, the profile or envelope is quantized to produce secret-key bit sequences.

3.2 Quantization

Quantization is the process by which the sampled channel estimates are mapped to a specific bit sequence. Common approaches to quantizing the channel profile include ranking, level crossing, and using signal extrema. Rank quantization involves “bucketizing” the channel estimates in a manner that ensures an equally probable bit distribution. The buckets can be assigned single or multiple bits, and in the case of the latter, Gray coding is used to demarcate adjacent buckets. Gray coding is a binary numbering system where successive values differ in only one bit. It is used instead of binary coding so that discrepancies in measurements, which may cause a value to be assigned to a different bucket between Alice and Bob, will at most lead to a disagreement in only one bit. This process is

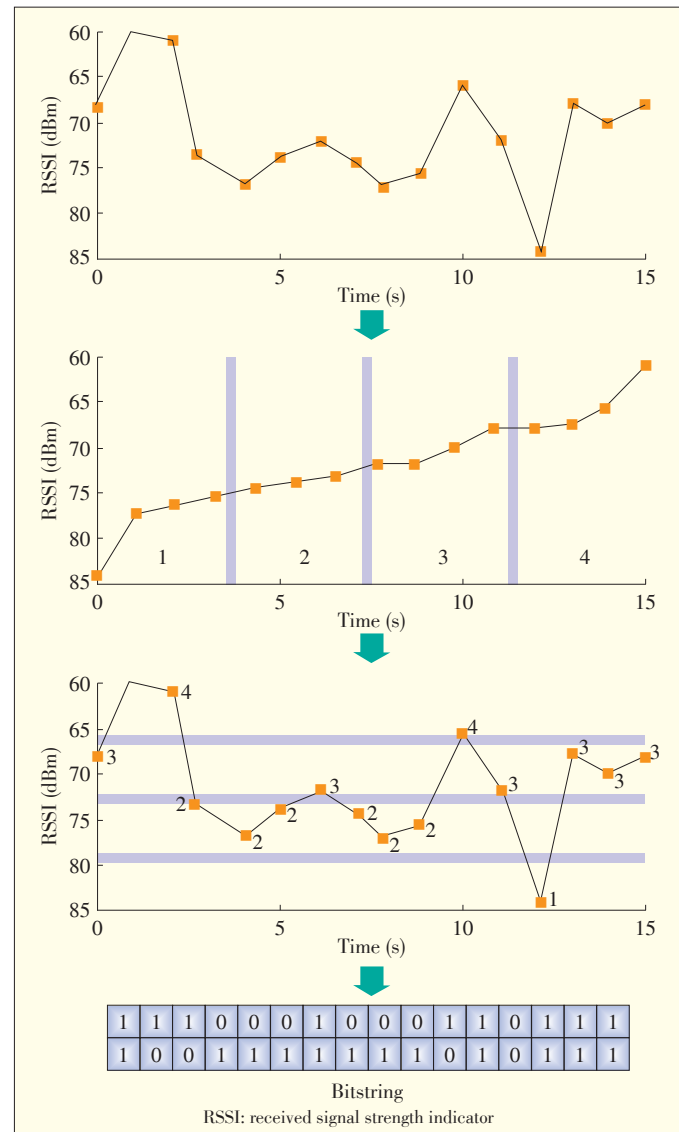
shown in **Fig. 5**. Rank quantization is performed in [17] and [9].

The level-crossing technique involves superimposing certain thresholds onto the channel profile and assigning bit values whenever a threshold is crossed. Variations on this basic concept have been developed to suit application requirements. For example, Mathur et al. [2] propose a quantizer (**Fig. 6**) that uses a moving window in which each block is assigned two threshold values:

$$q+ = \mu + \alpha \cdot \sigma$$

$$q- = \mu - \alpha \cdot \sigma \quad (2)$$

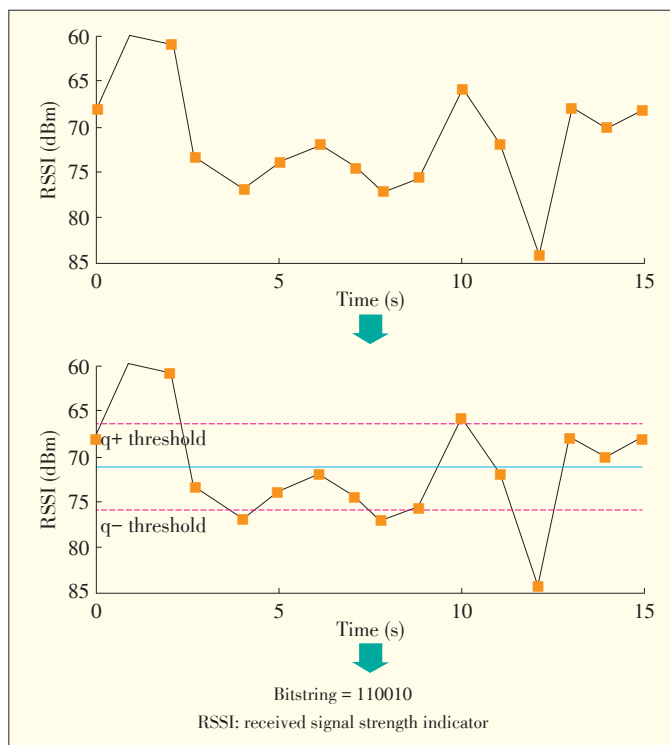
where μ is the mean, σ is the standard deviation, and $\alpha \geq 0$ is an adjustable parameter. If an RSSI reading within a window is greater than $q+$, it is encoded as 1. If an RSSI reading within a window is less than $q-$, it is encoded as 0. The thresholds de-



▲ **Figure 5.** Rank quantization.

Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics

Syed Taha Ali and Vijay Sivaraman



▲ Figure 6. Level-crossing quantization.

fine a censor zone, and values lying within this zone are discarded. This concept is similar to a guard band. The rationale for discarding such values is to filter out random noise effects or asymmetric components that are typically low-amplitude and liable to cause bit disagreement between the two parties.

3.3 Information Reconciliation

Much of the research on information reconciliation has been done in the context of quantum cryptography. Discrepancies in the bitstrings generated over the quantum channel occur because of eavesdropping or imperfections in the transmission media. Researchers have sought secure and efficient mechanisms to reconcile these bitstrings. Information reconciliation attempts a form of error correction using the public channel. To reconcile their bit sequences, Alice and Bob exchange metadata (usually parity information) to identify mismatching bits. At the same time, they simultaneously try to minimize the potential leakage of information to an eavesdropper. If mismatching bits are identified, they are either discarded or corrected. This concept is similar to the cyclic redundancy check used to detect data corruption and is also probabilistic, which means only a specific class of errors can be handled. Various error-correction codes, including BCH [11] and LDPC [18], have been used for reconciliation.

Cascade [19] is the most popular information-reconciliation protocol and works iteratively in an interactive manner. Alice permutes her bit sequence randomly, divides it into blocks, computes the parity on each block, and sends the permutation

and parity information to Bob, who then performs the same process at his end. If parity does not match for certain blocks, Bob performs a binary search to identify the minimum number of bits that he can change to match the parity check. This process is then repeated multiple times with different permutations of the bit sequence to identify which bits need to be corrected. The probability of success can be fine-tuned by specifying an adequate block size and the number of passes of the protocol.

3.4 Privacy Amplification

Privacy amplification is necessary because successive wireless channel estimates may be correlated in time, and this leads to predictability in portions of the bit sequence. Privacy amplification is also necessary because the information reconciliation process may reveal some information about the sequence to eavesdroppers. To effectively decorrelate successive bits in the sequence and nullify any knowledge an eavesdropper may have about parts of the key, an obfuscation operation is performed. Typically, Alice and Bob use universal hash functions chosen from a public set of such functions. This results in smaller, fixed-size bit sequences that can be used as a secret key.

4 Future Directions

In this section, we briefly discuss a few promising directions for future work in secret-key agreement using wireless channel characteristics.

Several research efforts have already resulted in proof-of-concepts for wireless-channel-based secret-key agreement in different environments. Jana et al. [13] investigated the efficacy of this approach in buildings, cafeterias, and tunnels as well as on a lawn or road. The authors also investigated the efficacy of this approach for various modes of activity, such as sitting, walking, or riding a bike. Wilhelm et al. [14] characterize the channel frequency response for static configurations. In [8], we adapted this mechanism for wearable health monitoring devices and presented experimental results.

However, significant work still needs to be done before secret-key agreement using wireless channel characteristics can actually be deployed in everyday, usable technology. Thus far, research on this technique has mostly relied on offline analysis of trace data, and there is a lack of actual prototype solutions implemented on user platforms, such as mobile phones and sensor devices. Running these solutions on user devices would require significant engineering and optimization, which has yet to be done.

Furthermore, wireless channel-based attacks have only just begun to be examined seriously. An early attack, also called a predictable channel attack, was described by Jana et al. in [13]. The authors demonstrated that, in a stationary environment, an attacker may be able to cause predictable variations in RSS by repeatedly blocking the line of sight between Alice

and Bob. Likewise, Mathur et al. [2] discuss an attack where Eve might spoof Alice and Bob. The authors show how that can be detected easily using RSS authenticators. These attacks are relatively simple and can be easily avoided by taking a few precautions. However, some very recent research indicates that multiple eavesdroppers might be able to collude to obtain a greater portion of the quantized bit sequence, even up to approximately 70% agreement with Alice and Bob. This is a serious concern. Such attacks, detailed in [20] and [21], are ad hoc in nature and have so far only been experimentally demonstrated. We suggest there needs to be a thorough inquiry into the theoretical basis for such attacks before solutions can be sought. There also needs to be corresponding research on adequate privacy amplification mechanisms in this domain. So far, this area has been neglected.

5 Conclusion

In this paper, we have briefly introduced current research on wireless channel-based secret-key agreement. We have highlighted the advantages of and challenges related to this technique. We have provided the requisite theoretical background and elaborated on the component processes, sampling, quantization, information reconciliation, and privacy amplification of this technique. We have also summarized certain challenges in this domain, such as the urgent need for practical implementations and the lack of comprehensive theory on threats and attacks. We believe there is great potential for wireless-channel-based secret-key agreement, especially with the advent of new resource-constrained computing paradigms, such as body area networks, mobile computing, and the internet of things.

References

- [1] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
- [2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret Key from an unauthenticated wireless channel," in *ACM MobiCom*, San Francisco, CA, 2008, pp. 128–129.
- [3] E. Blass and M. Zitterbart, "Efficient implementation of elliptic curve cryptography for wireless sensor networks," University at Karlsruhe, Tech. Rep., 2005.
- [4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [6] U. M. Maurer, "Perfect cryptographic security from partially independent channels," in *Proc. STOC'91*, New Orleans, pp. 561–571.
- [7] W. C. Jakes, *Microwave Mobile Communications*, New York: Wiley, 1974.
- [8] S. T. Ali, V. Sivaraman, and D. Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in *Proc. WISEC'12*, Tucson, USA, pp. 39–50.
- [9] J. Croft, N. Patwari, and S. Kaser, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proc. IPSN'10*, Stockholm, Sweden, pp. 70–81.
- [10] L. E. Bassham III, et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Tech. Rep. SP 800–22 Rev. 1a., 2001.
- [11] T. Aono, K. Higuchi, T. Ohira, B. Komiya, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.
- [12] P. Bellot and M. Dang, "BB84 implementation and computer reality," *IEEE RIVE*, Da Nang, Jul. 2009, pp. 1–8.
- [13] S. Jana, S. N. Premnath, M. Clark, S. Kaser, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction using wireless signal strength in real environments," *ACM MobiCom*, Beijing, 2009, pp. 321–332.
- [14] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret keys from entangled sensor nodes: implementation and analysis," *ACM WiSec*, Hoboken, NJ, 2010, pp. 139–144.
- [15] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.
- [16] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," *ACM CCS*, Alexandria, USA, 2007, pp. 401–410.
- [17] N. Patwari, J. Croft, S. Jana, and S. K. Kaser, "High rate uncorrelated bit extraction for shared key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.
- [18] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.
- [19] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. EUROCRYPT'93*, Lofthus, Norway, pp. 410–423.
- [20] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. EUROSEC'11*, Salzburg, Austria, article no. 8.
- [21] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," *Computer Science*, vol. 7459, pp. 235–252, 2012.

Manuscript received: July 11, 2013

Biographies

Syed Taha Ali (taha@unsw.edu.au) received his BSc(Eng) degree from the GIK Institute of Engineering Sciences and Technology, Pakistan, in 2002. He received his MSc from the University of New South Wales, Australia, in 2006. He recently concluded his PhD degree at UNSW, writing a thesis on developing novel security mechanisms for body sensor networks. His research interests include wireless sensor networks, network mobility, software defined networks, and applied network security. His work has appeared at ACM WiSec, IEEE SECON, IEEE BodyNets and IEEE TrustCom. He has been published in journals such as *IEEE Transactions on Mobile Computing* and *Elsevier Future Generation Computer Systems*. He is currently working as a postdoctoral researcher in the School of Electrical Engineering, UNSW.

Vijay Sivaraman (vijay@unsw.edu.au) (M'94) received his BTech. degree from the Indian Institute of Technology, Delhi, in 1994. He received his MS degree from North Carolina State University in 1996. He received his PhD degree from the University of California, Los Angeles, in 2000. He has worked at Bell-Labs and at a Silicon Valley start-up, where he was involved in manufacturing optical switch routers. He is currently an associate professor in the School of Electrical Engineering and Telecommunications, UNSW, and a visiting researcher at the CSIRO ICT Centre. He has considerable experience working with network routing protocols and QoS mechanisms and has initiated and led projects on optical networking, energy-efficient networks, power optimization and security protocols for wearable devices, and sensor networks for air pollution monitoring. His work has appeared at conferences such as IEEE INFOCOM and ACM CoNEXT and has been published in prestigious journals such as *IEEE/ACM Transactions on Networking*, *IEEE Journal of Selected Areas in Communication*, and *IEEE Transactions on Image Processing*.

An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels

Nan Yang¹, Maged ElKashlan², Phee Lep Yeoh³, and Jinhong Yuan¹

(1. The University of New South Wales, NSW 2052, Australia;

2. Queen Mary, University of London, London E1 4NS, UK;

3. The University of Melbourne, VIC 3010, Australia)

Abstract

This paper is a survey of transmit antenna selection—a low-complexity, energy-efficient method for improving physical layer security in multiple-input multiple-output wiretap channels. With this method, a single antenna out of multiple antennas is selected at the transmitter. We review a general analytical framework for analyzing exact and asymptotic secrecy of transmit antenna selection with receive maximal ratio combining, selection combining, or generalized selection combining. The analytical results prove that secrecy is significantly improved when the number of transmit antennas increases.

Keywords

physical layer security; transmit antenna selection; secrecy outage probability; wireless fading

1 Introduction

Information security is vital in wireless communications. The broadcast nature of the wireless channels allows potential eavesdroppers to intercept data transmitted in communication networks. Traditionally, cryptographic protocols provide security in the upper layers (e.g. the network layer), assuming that an error-free link has been created in the physical layer [1]. In wireless networks, distributing and managing secret keys can be expensive and insecure [2]. Therefore, research has recently been done on physical layer security, in which the characteristics of wireless channels are exploited for secure data transmission. Pioneering works on physical layer security describe a wiretap channel with a single antenna at the transmitter, receiver, and eavesdropper [3]–[6]. Perfect secrecy is achieved in wiretap channels when the quality of the transmitter–eavesdropper channel is lower than that of the transmitter–receiver channel [3]–[6].

Physical layer security in multiple-input multiple-output (MIMO) wiretap channels has been motivated by emerging wireless applications with multiple antenna terminals and has recently been addressed from the perspective of information theory [7]–[10]. In [7]–[10], the secrecy capacity of a MIMO wiretap channel was determined. Wireless fading has also been considered [11]–[13]. In [11] and [12], the secrecy outage probability was determined for Rayleigh fading, and in [13] and [14], the secrecy outage probability was determined for Nakagami- m fading. In [15]–[18], transmit beamforming (TBF) in

the direction of the receiver was investigated as a way of securing transmission in the MIMO wiretap channel. In [15], TBF was proposed to minimize the transmit power for a pre-specified signal to interference plus noise ratio (SINR) at the receiver. In [16], artificial noise was incorporated into the beamforming weights to constrain the maximum SINRs of the eavesdroppers. In [17], linear precoding was done at the transmitter, which means a game-theory formulation was used to balance performance and fairness. In [18], codebook-based transmission beamforming was for situations where receiver feedback capacity is limited. These TBF methods require precise information about the main channel and eavesdropper channel. Such information increases feedback overhead and computation during signal processing, especially when there is a large number of transmit antennas [19], [20].

To reduce feedback overhead and computation introduced by TBF, and to increase physical layer security, transmit antenna selection (TAS) can be applied at the multiantenna transmitter [21]–[25]. In [21], TAS secrecy was analyzed for multiple-input, single-output (MISO) wiretap channels where the legitimate receiver has a single antenna. In [22] and [23], the secrecy of TAS with receive maximal-ratio combining (TAS/MRC) or selection combining (TAS/SC) was analyzed for general MIMO wiretap channels. In [24], the effect of antenna correlation at the receiver and eavesdropper on TAS/MRC secrecy was determined. In [25], TAS with receive generalized selection combining (TAS/GSC) was introduced into MIMO wiretap channels, and of TAS/GSC secrecy was then determined.

In this paper, we focus on an important question: Is TAS an effective method for improving physical layer security in MIMO wiretap channels? We provide a survey on TAS and show how TAS benefits transmission security in MIMO wiretap channels. In section 2, we discuss the properties of MIMO wiretap channels and describe the details of TAS for increased security. In section 3, we discuss exact TAS secrecy. In section 4, we discuss asymptotic TAS secrecy. In section 5, we provide figures that show the effect of system parameters on secrecy. Section 6 concludes the paper.

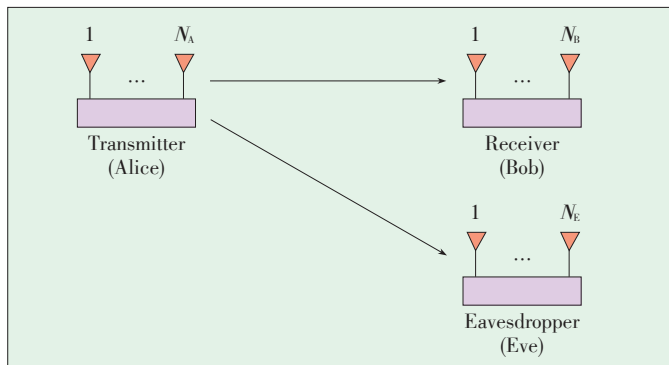
2 MIMO Wiretap Channels with TAS

2.1 MIMO Wiretap Channels

We consider a MIMO wiretap channel as shown in **Fig. 1** [23]. Specifically, the channel between Alice and Bob is the main channel, and the channel between Alice and Eve is the eavesdropper's channel. The eavesdropper is passive, which means there is no channel state information (CSI) feedback between Alice and Eve, and Alice does not know the CSI of the eavesdropper's channel. Alice encodes her messages using wiretap codes and transmits the code words to Bob. Eve overhears the information conveyed by Alice to Bob without inducing any interference in the main channel [26]. We assume that both the main channel and the eavesdropper channel both experience slow block fading and that fading coefficients do not vary during one fading block. We also assume that the block length is sufficiently long to allow for capacity-achieving codes within each block. Furthermore, the main channel and eavesdropper channel are assumed to have the same fading block length. The secrecy capacity is expressed as [6]

$$C_s = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \leq \gamma_E \end{cases} \quad (1)$$

Where $C_B = \log_2(1 + \gamma_B)$ is the capacity of the main channel, and $C_E = \log_2(1 + \gamma_E)$ is the capacity of the eavesdropper channel. In (1), γ_B and γ_E denote the instantaneous signal-to-noise



▲ **Figure 1.** MIMO wiretap channel with N_A , N_B , and N_E antennas at Alice, Bob, and Eve, respectively.

ratios (SNRs) of the main channel and the eavesdropper channel, respectively. In this paper, we focus on a scenario where the main channel and the eavesdropper channel are subject to independent but non-identically distributed (i.n.i.d.) Rayleigh fading.

2.2 Transmit Antenna Selection

Here, we describe a TAS protocol for the MIMO wiretap channel in Fig. 1 [23]. This protocol is designed to boost C_s by increasing C_B relative to C_E . In the main channel, the strongest antenna of N_A available antennas is selected in order to maximize the instantaneous SNR between Alice and Bob and to securely transmit data. Therefore, as N_A increases, C_B also increases. Selecting the strongest antenna at Alice is optimal for secrecy because C_B is maximized, and multiantenna diversity at the transmitter is fully exploited. In the eavesdropper channel, the strongest transmit antenna for Bob is equivalent to a random transmit antenna for Eve. Therefore, as N_A increases, C_E does not increase. The TAS protocol has low feedback overhead because Bob only feeds back to Alice the index of the strongest antenna as well as the channel estimates associated with the strongest antenna. The index allows Alice to select the strongest transmit antenna, and the estimated CSI allows her to determine the size of the codebook with random binning (which is used for secure transmission) [6]. The TAS feedback overhead is lower than TBF feedback overhead because TBF necessitates CSI feedback for N_A transmit antennas.

The TAS protocol is well-suited to passive eavesdropping, where Alice does not know the CSI of the eavesdropper's channel. In such a case, Alice selects a constant code rate R_s . If $C_B - C_E > R_s$, the code words with code rate selected by Alice guarantee secrecy. If $C_B - C_E \leq R_s$, Eve can eavesdrop, and secrecy is not guaranteed. In passive eavesdropping scenarios, secrecy outage probability is a useful metric for assessing security.

At Bob, we focus on three practical diversity-combining techniques: MRC, SC, and GSC. MRC is used to coherently combine the received signals when the number of implemented radio frequency (RF) chains is N_B . SC is used to select the signal with the highest instantaneous SNR when there is only one RF chain (because of size and complexity constraints). GSC is used to select and combine the signals of L_B strongest antennas out of N_B available antennas when the number of implemented RF chains is L_B for $1 < L_B < N_B$. The $N_B \times 1$ channel vector between the n th transmit antenna at Alice and N_B antennas at Bob is given by $\mathbf{h}_{n,B} = [h_{n,1}, h_{n,2}, \dots, h_{n,N_B}]^T$, where $[\cdot]^T$ denotes the transpose operation. The antennas at Bob have independent and identically distributed (i.i.d.) Rayleigh fading entries. When MRC is used at Bob, the index of the selected antenna is given by [23]

$$n_{\text{MRC}}^* = \underset{1 \leq n \leq N_A}{\operatorname{argmax}} \|\mathbf{h}_{n,B}\| \quad (2)$$

An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels

Nan Yang, Maged Elkashlan, Phee Lep Yeoh, and Jinhong Yuan

where $\|\cdot\|$ denotes the Euclidean norm. When SC is used at Bob, the index of the selected antenna is given by [23]

$$n_{SC}^* = \underset{1 \leq n \leq N_A, 1 \leq m \leq N_B}{\operatorname{argmax}} |h_{n,m}| \quad (3)$$

When GSC is used at Bob, $|h_{n,1}|^2 \geq |h_{n,2}|^2 \geq \dots \geq |h_{n,N_B}|^2$ is the order statistics derived from arranging $\{|h_{n,m}|^2\}_{m=1}^{N_B}$ in descending order of magnitude. We also give the definition

$\theta_j = \sum_{m=1}^{N_B} |h_{n,m}|^2$. The index of the selected antenna is then given by [25]

$$n_{GSC}^* = \underset{1 \leq n \leq N_A, 1 \leq m \leq N_B}{\operatorname{argmax}} \theta_j \quad (4)$$

The combining technique used at Eve depends on the number of RF chains at Eve. MRC is optimal at Eve because the benefits of N_E antennas are fully exploited, and the probability of successful eavesdropping is maximized.

3 Analyzing Exact Secrecy

3.1 Secrecy Outage Probability

Here, we give closed-form expressions for the exact probability of secrecy outage using TAS. This is the probability that the achievable secrecy rate C_s is less than a predetermined secrecy transmission rate R_s . When C_s is less than R_s , secure transmission is not guaranteed. The secrecy outage probability is given by [6]

$$P_{\text{out}}(R_s) = \Pr[C_s < R_s] \quad (5)$$

We proceed to the generalized framework for analyzing the secrecy outage probability. From (5), the secrecy outage probability can also be given as [23]

$$\begin{aligned} P_{\text{out}}(R_s) &= \Pr[C_s < R_s \mid \gamma_B > \gamma_E] \Pr[\gamma_B > \gamma_E] + \\ &\quad \Pr[C_s < R_s \mid \gamma_B \leq \gamma_E] \Pr[\gamma_B \leq \gamma_E] = \\ &\quad \Pr[C_s < R_s \mid \gamma_B > \gamma_E] \Pr[\gamma_B > \gamma_E] + \Pr[\gamma_B \leq \gamma_E] = \\ &\quad \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E + \\ &\quad \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E = \\ &\quad \int_0^\infty \int_0^{2^{R_s}(1+\gamma_E)^{-1}} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E, \end{aligned} \quad (6)$$

where $f_{\gamma_B}(\gamma_B)$ is the probability density function (PDF) of γ_B , and $f_{\gamma_E}(\gamma_E)$ is the PDF of γ_E . Given the properties of Rayleigh fading channels and the diversity combining techniques used at Bob and Eve, $f_{\gamma_B}(\gamma_B)$ and $f_{\gamma_E}(\gamma_E)$ can be easily obtained.

Here, we give the secrecy outage probabilities of TAS/MRC, TAS/SC, and TAS/GSC. In these expressions, we assume that Bob and Eve use the same diversity combining techniques. For TAS/MRC (TAS is used at Alice, and MRC is used at both Bob and Eve), the secrecy outage probability is given by [22]

$$\begin{aligned} P_{\text{out, MRC}}(R_s) &= 1 - \frac{\bar{\gamma}_B^{N_E}}{\Gamma(N_E)} \sum_{p=1}^{N_A} \binom{N_A}{p} (-1)^{p-1} e^{-\frac{\rho(2R_s-1)}{\bar{\gamma}_B}} \prod_{u=1}^{N_B-1} \left[\sum_{i_u=0}^{i_{u-1}} \binom{i_{u-1}}{i_u} \left(\frac{1}{i_u!} \right)^{i_u-i_{u+1}} \right] \times \\ &\quad \sum_{q=0}^{\psi_u} \binom{\psi_u}{q} 2R_s q \frac{(2R_s-1)^{\psi_u-q} \Gamma(N_E+q) \bar{\gamma}_E^q}{(2R_s p \bar{\gamma}_E + \bar{\gamma}_B)^{N_E+q} \bar{\gamma}_B^{\psi_u-q}} \end{aligned} \quad (7)$$

Where $\bar{\gamma}_B$ and $\bar{\gamma}_E$ are the average per-antenna received SNR at Bob and Eve, respectively. In (7), $\psi_u = \sum_{i_u=1}^{N_B-1} i_u$ for $i_0 = p$, and $i_{N_B} = 0$. To obtain (7), we substitute $f_{\gamma_B}(\gamma_B)$ and $f_{\gamma_E}(\gamma_E)$ into (6); we use [27, eq. (1.111)] to expand the binomial; and we use [28, eq. (9)] to expand the resulting polynomial. Then, we solve the resulting integrals using [27, eq. (3.326.2)]. If we follow this same procedure, the secrecy outage probability of TAS/SC (TAS is used at Alice, and SC is used at both Bob and Eve) is given by [22]

$$\begin{aligned} P_{\text{out, SC}}(R_s) &= 1 - \frac{N_E}{\bar{\gamma}_E} \sum_{p=1}^{N_A} \binom{N_A N_B}{p} (-1)^{p-1} \\ &\quad e^{-\frac{\rho(2R_s-1)}{\bar{\gamma}_B}} \sum_{q=0}^{N_B-1} \binom{N_B-1}{q} (-1)^q \left(\frac{2R_s p}{\bar{\gamma}_B} + \frac{q+1}{\bar{\gamma}_E} \right) \end{aligned} \quad (8)$$

The secrecy outage probability of TAS/GSC (TAS is used at Alice, and GSC is used at both Bob and Eve) is given by [25]

$$\begin{aligned} P_{\text{out, GSC}}(R_s) &= \sum_{l_E=0}^{L_E} \frac{s_{l_E} (l_E-1)}{\Gamma(l_E)} \sum_{S_k \in S} \sum_{\eta=0}^{\beta_k} \Xi \Gamma(\eta+l_E-1) \left(\frac{2R_s \delta_k}{\bar{\gamma}_B} + \frac{1}{\bar{\gamma}_E} \right)^{-(\eta+l_E-1)} - \\ &\quad \sum_{l_E=0}^{L_E} \frac{s_{l_E}}{\Gamma(l_E) \bar{\gamma}_E} \sum_{S_k \in S} \sum_{\eta=0}^{\beta_k} \Xi \Gamma(\eta+l_E) \left(\frac{2R_s \delta_k}{\bar{\gamma}_B} + \frac{1}{\bar{\gamma}_E} \right)^{-(\eta+l_E)} - \\ &\quad \sum_{l_E=L_E+1}^{N_E} \frac{s_{l_E} l_E}{\Gamma(l_E) \bar{\gamma}_E} \sum_{S_k \in S} \sum_{\eta=0}^{\beta_k} \Xi \Gamma(\eta+1) \left(\frac{2R_s \delta_k}{\bar{\gamma}_B} + \frac{l_E}{L_E \bar{\gamma}_E} \right)^{-(\eta+1)} \end{aligned} \quad (9)$$

where $S = \{S_k \mid \sum_{n=0}^N n_{k,n} = N_A\}$ with $n_{k,n} \in Z^+$ and

$$\Xi = \alpha_k \binom{\beta_k}{\eta} (2R_s-1)^{\beta_k} e^{-\frac{\delta_k(2R_s-1)}{\bar{\gamma}_B}} \left(\frac{2R_s}{2R_s-1} \right)^\eta \quad (10)$$

The definition of s_{l_E} in (9) can be found in [29, eq. (3)]. The definitions of α_k , β_k , and δ_k in (10) can be found in [29, eq. (6)–(8)]. The secrecy outage probability expressions in (7), (8), and (9) are closed-form expression and apply to arbitrary numbers of antennas and arbitrary average SNRs.

3.2 Probability of Nonzero Secrecy Capacity

Here, we describe the condition for non-zero secrecy capacity. From (1), the probability of nonzero secrecy capacity is [6]

$$\Pr[C_s > 0] = \Pr[\gamma_B > \gamma_E] = \int_0^\infty \int_0^{\gamma_B} f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) d\gamma_E d\gamma_B \quad (11)$$

From (6) and (11), the relationship between $P_{\text{out}}(R_s)$ and $\Pr[C_s > 0]$ is $\Pr[C_s > 0] = 1 - P_{\text{out}}(0)$. The probabilities of nonzero

secrecy capacity for TAS/MRC, TAS/SC, and TAS/GSC are obtained from (7), (8) and (9), respectively.

3.3 ε -Outage Secrecy Rate

The ε -outage secrecy rate R_s^{\max} is the maximum secrecy rate when the secrecy outage probability is less than ε [12]. This rate is given by $\varepsilon = P_{\text{out}}(R_s^{\max})$. The ε -outage secrecy rates for TAS/MRC, TAS/SC, and TAS/GSC can be obtained by applying numerical root-finding to (7), (8) and (9), respectively.

4 Analyzing Asymptotic Secrecy

4.1 Asymptotic Secrecy Outage Probability

We introduce the asymptotic secrecy outage probability to characterize secrecy outage probability when the average SNR of the main channel is sufficiently high; that is, when $\bar{\gamma}_B \rightarrow \infty$. This corresponds to a scenario where Bob is much closer to Alice than Eve (which is an interesting practical scenario). The asymptotic secrecy outage probability allows us to determine the effects of antenna correlation on secrecy outage diversity order and secrecy outage array gain. The secrecy outage diversity order is the slope of the secrecy outage probability curve and describes how fast secrecy outage probability decreases with average SNR. The secrecy outage array gain is the horizontal shift of the secrecy outage probability curve. This gain describes the SNR advantage of a secrecy outage probability curve relative to the reference curve with the same secrecy outage diversity order.

To introduce the asymptotic probability, we show the first nonzero order expansion of the cumulative distribution function of γ_B . This gives $F_{\gamma_B}^{\infty}(\gamma_B)$. Specifically, the first nonzero order expansion can be obtained by using the first order Maclaurin series expansion from [27, eq. (1.211.1)] and neglecting the higher-order terms. Using the expansion $f_{\gamma_E}(\gamma_E)$ and (6), the asymptotic secrecy outage probability is given by [22]

$$P_{\text{out}}(R_s) = (G_a \bar{\gamma}_B)^{-G_d} + o(\bar{\gamma}_B^{-G_d}) \quad (12)$$

where G_d is the secrecy outage diversity order and G_a is the secrecy outage array gain. For TAS/MRC, $G_{d,\text{MRC}} = N_A N_B$ and [22]

$$G_{a,\text{MRC}} = \left(\frac{(2R_s - 1)^{N_A N_B}}{(N_B!)^{N_A} \Gamma(N_E)} \sum_{p=0}^{N_A N_B} \binom{N_A N_B}{p} \left(\frac{2R_s \bar{\gamma}_E}{2R_s - 1} \right)^p \Gamma(N_E + p) \right)^{-\frac{1}{N_A N_B}} \quad (13)$$

For TAS/SC, we have $G_{d,\text{SC}} = N_A N_B$ and [22]

$$G_{a,\text{SC}} = \left(N_E (2R_s - 1)^{N_A N_B} \sum_{p=0}^{N_A N_B} \binom{N_A N_B}{p} \left(\frac{2R_s \bar{\gamma}_E}{2R_s - 1} \right)^p \sum_{q=0}^{N_E-1} \binom{N_E-1}{q} \left(\frac{2R_s \bar{\gamma}_E}{2R_s - 1} \right)^q \frac{(-1)^q \Gamma(p+1)}{(q+1)^{p+1}} \right)^{-\frac{1}{N_A N_B}} \quad (14)$$

For TAS/GSC, $G_{d,\text{GSC}} = N_A N_B$ and [25]

$$G_{a,\text{GSC}} = \left(\frac{(2R_s - 1)^{N_A N_B}}{(L_B^{N_B} L_E^{N_A})^{N_A}} \sum_{p=0}^{N_A N_B} \binom{N_A N_B}{p} \left(\frac{2R_s \bar{\gamma}_E}{2R_s - 1} \right)^p \left(-p \sum_{l_E=1}^{L_E} \frac{\varepsilon_{l_E} \Gamma(p+1-l_E)}{\Gamma(l_E) \bar{\gamma}_E^{1-l_E}} - \sum_{l_E=L_E+1}^{N_E} \frac{\varepsilon_{l_E} \Gamma(p+1) L_E^p}{L_E^p} \right) \right)^{-\frac{1}{N_A N_B}} \quad (15)$$

In light of these asymptotic results, we can make the following points about the use of TAS with MRC, SC, or GSC in the wiretap channel:

- The secrecy outage probability approaches zero as γ_B approaches infinity.
- TAS/MRC, TAS/SC, and TAS/GSC achieve the same secrecy outage diversity order of $N_A N_B$. This diversity order depends entirely on the main channel.
- The secrecy outage diversity order of TAS/MRC, TAS/SC, and TAS/GSC is not affected by the eavesdropper channel. Moreover, the secrecy outage diversity order of TAS/GSC is not affected by the choice of L_B or L_E .

4.2 Secrecy Performance Tradeoff

Here, we discuss the secrecy outage tradeoff between TAS/GSC, TAS/SC, and TAS/MRC at the legitimate receiver. The asymptotic results show that this tradeoff is characterized solely by secrecy outage SNR gain. When the same diversity combining technique is used at the eavesdropper, the SNR gap between TAS/GSC and TAS/SC in the main channel is given by [25]

$$\Delta_1 = \frac{10}{N_B} \log(L_B^{N_B} L_E) \text{ dB} \quad (16)$$

As L_B increases, $\Delta_1 > 0$ and the SNR gap increases. The SNR gap between TAS/GSC and TAS/MRC is given by [25]

$$\Delta_2 = \frac{10}{N_B} \log\left(\frac{L_B^{N_B} L_E}{N_B!}\right) \text{ dB} \quad (17)$$

As L_B increases, the SNR gap decreases. By observing Δ_1 and Δ_2 , we find that these SNR gaps depend entirely on N_B and L_B . They are not affected by N_E and L_E .

5 Numerical Results

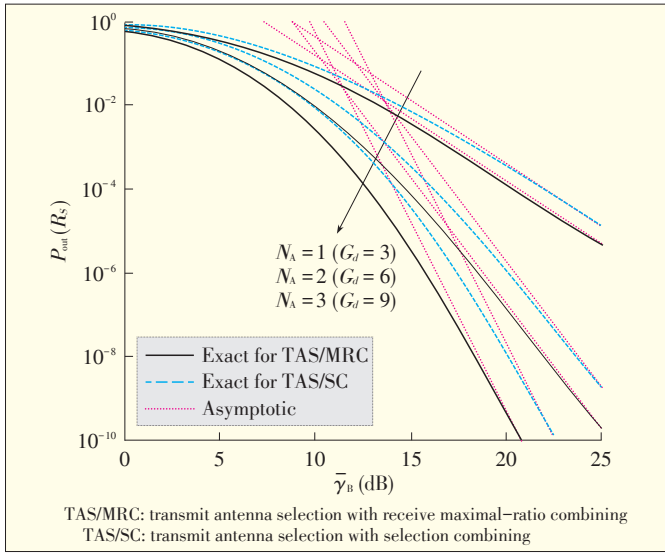
We now give numerical results that show how the number of antennas and average SNR affect secrecy. We normalize the variance of the fading coefficients to unity.

In Fig. 2 [22], secrecy outage probability is plotted against $\bar{\gamma}_B$ to show the effect of N_A on secrecy. There is a significant decrease in the secrecy outage probability when N_A increases because N_A increases the secrecy diversity order through $N_A N_B$. This means that the secrecy outage probability quickly approaches zero as N_A increases, and the probability of secure transmission is sufficiently high.

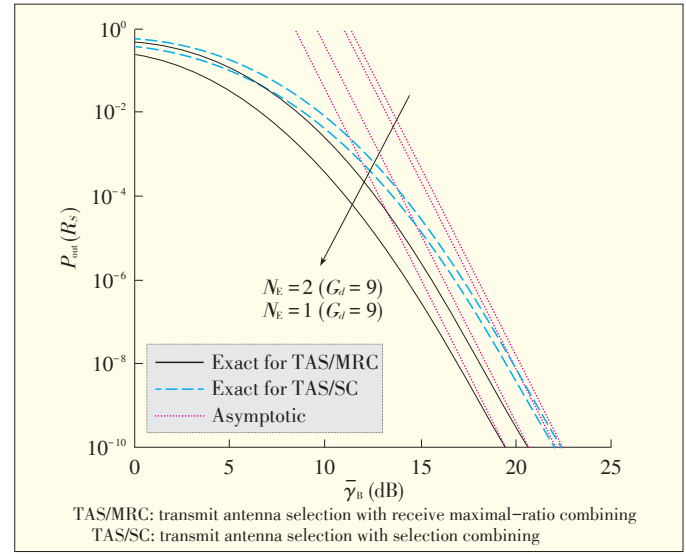
In Figs. 3 and 4 [22], secrecy outage probability is plotted against $\bar{\gamma}_B$ to show the effect of N_B and N_E on secrecy, respectively. In Fig. 3, secrecy outage probability significantly decreases as N_B increases because secrecy diversity order increases as N_B increases. In Fig. 4,

An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels

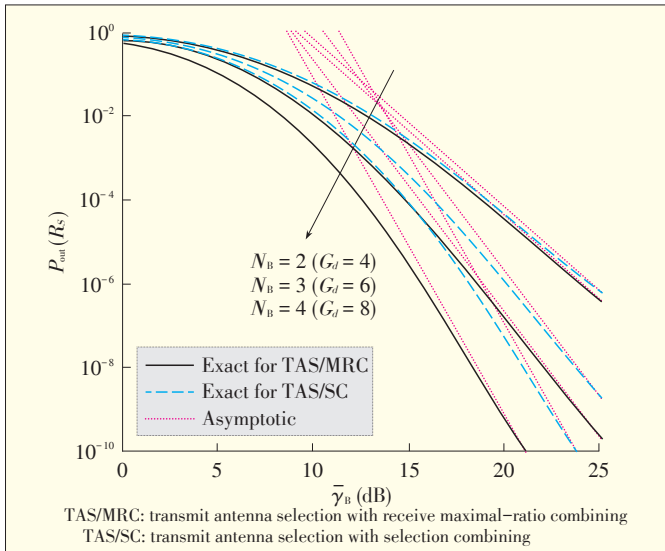
Nan Yang, Maged Elkashlan, Phee Lep Yeoh, and Jinhong Yuan



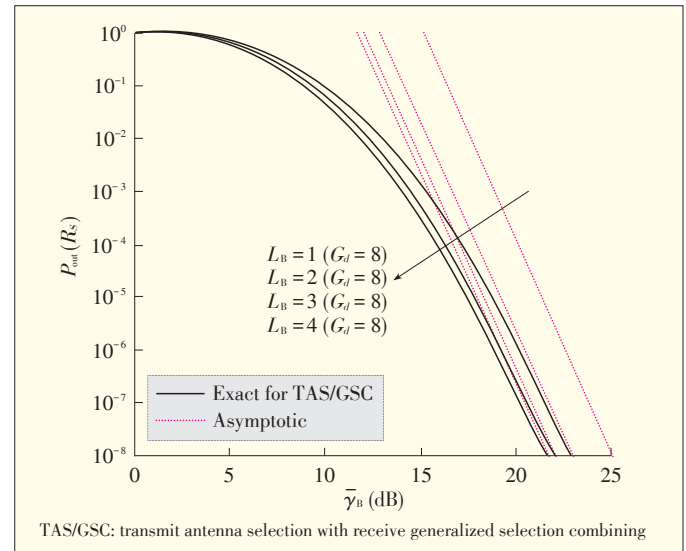
▲ Figure 2. Secrecy outage probability versus $\bar{\gamma}_B$ for $R_s = 0.1$, $\bar{\gamma}_E = 5$ dB, $N_B = 3$, and $N_E = 2$.



▲ Figure 4. Secrecy outage probability versus $\bar{\gamma}_B$ for $R_s = 0.1$, $\bar{\gamma}_E = 5$ dB, $N_A = 3$, and $N_E = 3$.



▲ Figure 3. Secrecy outage probability versus $\bar{\gamma}_B$ for $R_s = 0.1$, $\bar{\gamma}_E = 5$ dB, $N_A = 2$, and $N_E = 2$.



▲ Figure 5. Secrecy outage probability versus $\bar{\gamma}_B$ for $R_s = 1$, $\bar{\gamma}_E = 5$ dB, $N_A = 2$, $N_B = 4$, $N_E = 3$, and $L_E = 2$.

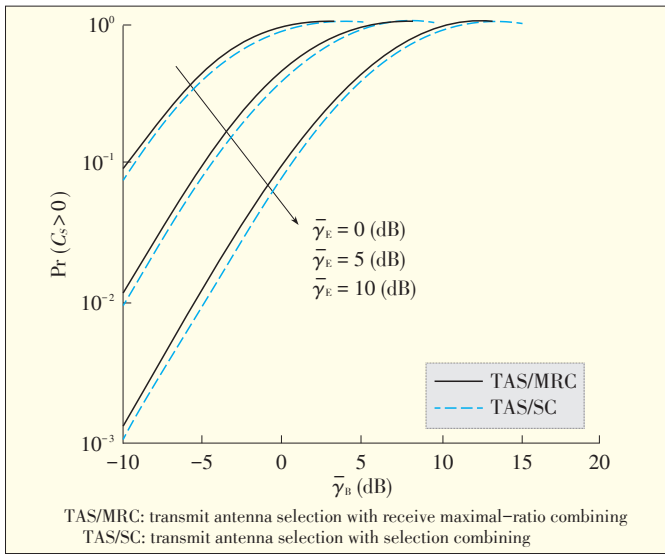
secrecy outage probability increases as N_E increases. This increase only occurs in the secrecy array gain because secrecy diversity order is not affected by N_E (indicated by the parallel slopes of the asymptotes).

In Fig. 5 [25], secrecy outage probability is plotted against $\bar{\gamma}_B$ to show the effect of L_B on secrecy. In Fig. 5, secrecy outage probability decreases as L_B increases. TAS/GSC provides a greater SNR advantage than TAS/SC and provides comparable secrecy outage to that of TAS/MRC. GSC is less complex than MRC but more complex than SC, so there is a cost-performance tradeoff with TAS/GSC in terms of physical layer security.

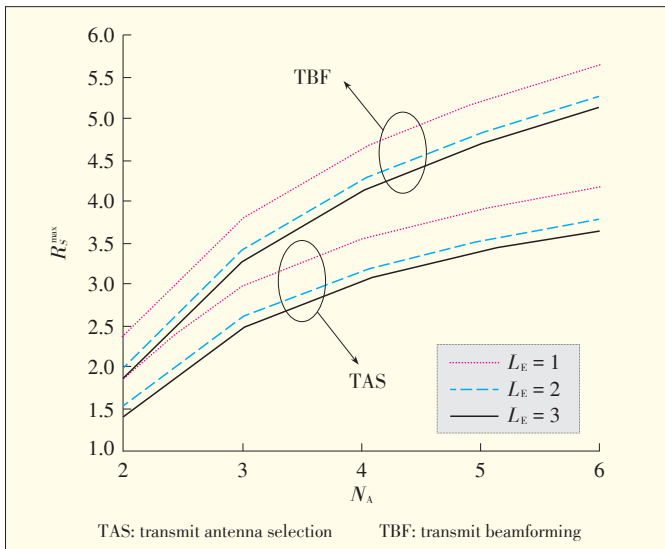
In Fig. 6 [22], the probability of non-zero secrecy capacity

is plotted against $\bar{\gamma}_B$. For a fixed $\bar{\gamma}_B$, $\Pr[C_S > 0]$ increases as $\bar{\gamma}_B$ increases. Moreover, $\Pr[C_S > 0]$ decreases as $\bar{\gamma}_E$ increases. Non-zero secrecy capacity exists even when the eavesdropper's channel is statistically better than the main channel, that is, when $\bar{\gamma}_E > \bar{\gamma}_B$.

Fig. 7 [25] shows TAS and TBF ε -outage secrecy rates against N_A for $\varepsilon = 0.01$. The TBF is the same as that in [18]. Maximal-ratio transmission is used at Alice, and a single antenna is installed at Bob. In Fig. 7, $N_B = 1$ for a fair comparison. The secrecy outage probability of TBF with GSC at the eavesdropper is derived from [25, eq. (17)]. Fig. 7 shows that, for both TAS and TBF, R_s^{\max} increases as N_A increases. TAS R_s^{\max} approximates TBF R_s^{\max} when N_A is small. Also, the rate



▲ Figure 6. Probability of nonzero secrecy capacity versus $\bar{\gamma}_B$ for $N_A = 4$, $N_B = 3$, and $N_E = 2$.



▲ Figure 7. ϵ -outage secrecy rate between TAS and TBF versus N_A for $\bar{\gamma}_B = 20$ dB, $N_B = 1$, $\bar{\gamma}_E = 0$ dB, and $N_E = 3$.

advantage of TBF over TAS increases as N_A increases. However, with TBF, this advantage comes at the cost of higher feedback and overhead. TBF feedback and overhead increases as N_A increases; however, TAS feedback and overhead is unchanged.

6 Conclusion

In this paper, we have reviewed TAS, which is designed to increase physical layer security in MIMO wiretap channels. A general analytical framework has been described that allows us to accurately determine the asymptotic secrecy of TAS/MRC, TAS/SC, and TAS/GSC. The asymptotic results show that TAS/

MRC, TAS/SC, and TAS/GSC have the same secrecy outage diversity order. The tradeoff of TAS/GSC relative to TAS/SC and TAS/MRC is characterized by their respective secrecy outage SNR gains.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, pp. 656–715, Oct. 1949.
- [2] B. Schneier, "Cryptographic design vulnerabilities," *Comput.*, vol. 31, no. 9, pp. 29–33, Sep. 1998.
- [3] A. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [6] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [7] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.
- [8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part I: the MISOE wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
- [9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: the MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [11] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.
- [12] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with MIMOME eavesdroppers: characterization of the outage probability and ϵ -outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.
- [13] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. 2009 ACSSC*, pp. 829–833.
- [14] M. Z. I. Sarkar and T. Ratnarajah, "On the secrecy mutual information of Nakagami-m fading SIMO channel," in *Proc. 2010 IEEE ICC*, pp. 1–5.
- [15] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [16] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
- [17] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.
- [18] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.
- [19] T. Gucluoglu and T. M. Duman, "Performance analysis of transmit and receive antenna selection over flat fading channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3056–3065, Aug. 2008.
- [20] N. Yang, P. L. Yeoh, M. Elkashlan, J. Yuan, and I. B. Collings, "Cascaded TAS/MRC in MIMO multiuser relay networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3829–3839, Oct. 2012.
- [21] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012.
- [22] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Secure transmission via transmit antenna selection in MIMO wiretap channels," in *Proc. IEEE Globecom 2012*, Anaheim, CA, Dec. 2012, pp. 1–6.

An Introduction to Transmit Antenna Selection in MIMO Wiretap Channels

Nan Yang, Maged El Kashlan, Phee Lep Yeoh, and Jinhong Yuan

- [23] N. Yang, P. L. Yeoh, M. El Kashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
- [24] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
- [25] N. Yang, P. L. Yeoh, M. El Kashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: A secure transmission using transmit antenna selection and receive generalized selection combining," to appear in *IEEE Communications Letters*.
- [26] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
- [27] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th edition. Academic, 2007.
- [28] S. Choi and Y.-C. Ko, "Performance of selection MIMO systems with generalized selection criterion over Nakagami-m fading channels," *IEICE Trans. Commun.*, vol. E89-B, no. 12, pp. 3467–3470, Dec. 2006.
- [29] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.

Manuscript received: August 14, 2013

Biographies

Nan Yang (nan.yang@unsw.edu.au) received his PhD degree in electronic engineering from Beijing Institute of Technology in 2010. From 2008 to 2010, he was a visiting PhD student at the School of Electrical Engineering and Telecommunications, University of New South Wales, Australia. From 2010 to 2012, he was a postdoctoral research fellow at the CSIRO Wireless and Networking Technologies Laboratory, Australia. He joined the School of Electrical Engineering and Telecommunications, University of New South Wales, in 2012 and is currently a postdoctoral research fellow there. He has published more than 40 papers in IEEE journals and conference proceedings. He co-authored three papers that won Best Paper Awards in IEEE VTC 2013 Spring. His research interests include communications theory and signal processing, specifically, cooperative communications, MIMO systems, resource allocation, and physical layer security.

Maged El Kashlan (maged.elkashlan@cecs.qmul.ac.uk) received his PhD degree in electrical engineering from the University of British Columbia, Canada, in 2006. From 2006 to 2007, he was with the Laboratory for Advanced Networking, University of British Columbia. From 2007 to 2011, he worked at the CSIRO Wireless and Networking Technologies Laboratory, Australia. From 2008–2011, he also held an adjunct position at the University of Technology Sydney. In 2011, he joined the School of Electronic Engineering and Computer Science, Queen Mary University, London. He also holds visiting faculty appointments at the University of New South Wales, Australia; and Beijing University of Posts and Telecommunications. He has co-authored three papers that won Best Paper Awards in IEEE VTC 2013 Spring. His research interests include distributed wireless networks, cooperative wireless networks, MIMO systems, cognitive radio, and physical layer security. He has been a member of the Technical Program Committee for several IEEE conferences, including IEEE International Conference on Communications (ICC) and IEEE Global Communications Conference (GLOBECOM).

Phee Lep Yeoh (phee.yeoh@unimelb.edu.au) received his PhD degree from the University of Sydney, Australia, in 2012. From 2008 to 2012, he worked at the Telecommunications Laboratory at the University of Sydney and the CSIRO Wireless and Networking Technologies Laboratory, Sydney. In 2012, he joined the Department of Electrical and Electronic Engineering, University of Melbourne, Australia. He won Best Paper award at IEEE VTC-Spring 2013 and Best Student Paper award at IEEE AusCTW 2013. He has been a member of the Technical Program Committee for international IEEE conferences, including GLOBECOM, ICC, and VTC. His research interests include cooperative communications, MIMO, cross-layer optimization, and physical layer security.

Jinhong Yuan (j.yuan@unsw.edu.au) received his BE and PhD degrees in electronics engineering from Beijing Institute of Technology, in 1991 and 1997. From 1997 to 1999, he was a research fellow at the School of Electrical Engineering, University of Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, and is currently a professor of telecommunications at that school. He has published two books, two book chapters, more than 200 papers in telecommunications journals and conference proceedings, and 40 industry reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check (LDPC) codes. He co-authored three papers that have won Best Paper awards and one Best Poster award. His publications are available at <http://www2.ee.unsw.edu.au/wcl/JYuan.html>. He is currently the chair of the IEEE NSW Chair of joint Communications/Signal Processions/Ocean Engineering Chapter and an associate editor of *IEEE Transactions on Communications*. His research interests include error control coding and information theory, communication theory, and wireless communications.

ZTE to Provide Disaster Recovery Solution to U Mobile Malaysia

4 October 2013, Shenzhen—ZTE has been selected by U Mobile Sdn Bhd to provide a disaster recovery system to make Malaysia's most dynamic and innovative 3G mobile network more resilient and robust.

U Mobile will deploy ZTE's DR solution in the core network, increasing the backup capabilities of the network infrastructure. The agreement between U Mobile and ZTE was signed today in Kuala Lumpur. ZTE's DR solution will be implemented on U Mobile's core transmission and IPCORE equipment and will significantly reduce service recovery times and improve network stability and reliability.

The DR system, which is expected to be completed in

2014, will enhance U Mobile's ability to provide uninterrupted internet and mobile services to subscribers. After the project is completed, U Mobile will explore subsequent upgrades and purchases depending on capacity requirements.

"We are glad to be partnering with ZTE once again for the deployment of DR systems as we believe their expertise in telecommunications equipment and network solutions will add value to our company," said Wong Heang Tuck, acting CEO and COO of U Mobile. "This is one of U Mobile's many major collaborations with ZTE and we look forward to greater partnerships and work synergies ahead."

(ZTE Corporation)

Reducible Discord in Generic Three-Qubit Pure W States

Zhengjun Xi¹, Zhihui Li² and Yongming Li¹

(1.College of Computer Science, Shaanxi Normal University, Xi'an 710062, China;

2.College of Mathematics & Information Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract

Quantum discord is the most prominent of quantum correlations, but it does not have unique generalizations to the multipartite case. W states are especially useful for secure communication. In this paper, we propose that the quantum correlation in generic three-qubit pure W states can be given by the two-qubit discords of these states.

Keywords

quantum discord; W state; quantum correlation

1 Introduction

In many-particle physics and quantum information science, classifying and quantifying correlations in a multipartite quantum state is a fundamental problem. The amount of knowledge about the quantum system that can be acquired from subsystems has also yet to be determined. Quantum science asks whether a multipartite quantum state can be determined uniquely if all its reduced-density matrices are specified [1],[2]. Generic N -party pure quantum states are uniquely determined by the reduced states of just over half the parties [3]. In [4], the N -qubit pure W states are determined by their bipartite reduced density matrices. Thus, N -party correlations in W state are reducible to two-party correlations. In the simplest case, the entanglement of the generalized three-qubit W state has maximum robustness against the loss of one qubit. This means that the bipartite entanglement left in the system can still be used to perform information-theoretic tasks, even without the cooperation of a third party. Moreover, a third party cannot destroy the residual entanglement, which makes the W state particularly useful for secure communication [6]–[9]. Almost all three-party pure quantum states can be determined by two-party reduced states [10]–[12]. In [1], [10] and [11], the total quantum correlations in the N -qubit pure W states should be characterized by the bipartite quantum correlation within them. In this paper, we discuss two-qubit quantum discord in generic three-qubit pure W states [13]. We propose two-qubit quantum discord as a figure

of merit for quantum correlation in the bipartite state.

2 Quantum Discord

Here, we discuss the concepts and properties of total, quantum, and classical correlations in the bipartite quantum system. The total correlation in a bipartite quantum state ρ^{AB} is given by the mutual information:

$$I(\rho^{AB}) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \quad (1)$$

where $S(\rho)$ is the von Neumann entropy, given by $-\text{Tr}(\rho \log_2 \rho)$. The reduced density matrices of ρ^{AB} are denoted ρ^A and ρ^B and are obtained by tracing out B and A, respectively. The classical correlation is the amount of information about subsystem B that can be obtained by measuring subsystem A [14]. The classical correlation is given by

$$C(\rho^{AB}) = \max_{\{E_i^A\}} [S(\rho^B) - \sum_i p_i S(\rho_i^B)] \quad (2)$$

where $\{E_i^A\}$ is the positive-operator valued measure (POVM)

performed on A, and $\rho_i^B = \frac{1}{p_i} \text{Tr}_A(E_i^A \otimes I^B \rho^{AB})$ is the remaining state of B after obtaining outcome i on A. The probability of outcome i is given by $p_i = \text{Tr}(E_i^A \otimes I^B \rho^{AB})$, where I^B is the identity operator on the subsystem B.

Quantum discord is the difference between total and classical correlations [13]:

$$D(\rho^{AB}) = I(\rho^{AB}) - C(\rho^{AB}) \quad (3)$$

Quantum states without entanglement but with nonzero

Reducible Discord in Generic Three-Qubit Pure W States

Zhengjun Xi, Zhihui Li, and Yongming Li

quantum discord can still be used to perform useful quantum tasks [15]. Quantum discord is essential in a wide variety of quantum information and quantum computations [16].

The definition of classical and quantum correlations involves an optimization process to minimize the term $\sum_{i=1}^n \rho_i S(\rho_i^B)$, which is considered the quantum version of the conditional entropy [13]. For a two-qubit system, the optimal POVM is a one-dimensional projective measurement [17]. In general, it is difficult to calculate the analytic expression for the quantum discord [16], [18]–[22]. Analytic results have only been obtained for a few specific cases of quantum discord: Many studies of quantum discord rely on numerical results. However, the results from [20] and [21] are sufficient for us to achieve our aims in this paper.

3 Quantum Discord for a Generic Three-Qubit W State

We consider only the case of a three-qubit W state, given by

$$|W_3\rangle = a_1|001\rangle + a_2|010\rangle + a_3|100\rangle \quad (4)$$

where $\sum_{i=1}^3 |a_i|^2 = 1$ and a_i are real numbers. Without a loss of generality, we assume positive parameters a_j for $j = 1, 2, 3$. From the results in [1], [4], [5], [10], [11], the three-qubit pure W state is determined by bipartite reduced density matrices. The total correlation in W state should be characterized by the bipartite correlations. Then, all the two-qubit reduced density matrices of the three-qubit pure W state (4) are given by

$$\rho^{JK} = \begin{pmatrix} 1 - |a_{4-J}|^2 - |a_{4-K}|^2 & 0 & 0 & 0 \\ 0 & |a_{4-K}|^2 & a_{4-K}a_{4-J} & 0 \\ 0 & a_{4-K}a_{4-J} & |a_{4-J}|^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (5)$$

where $J < K$. The one-qubit reduced density matrices $\rho^{J(k)}$ are given by

$$\rho^J = \begin{pmatrix} 1 - |a_{4-J}|^2 & 0 \\ 0 & |a_{4-J}|^2 \end{pmatrix}, \quad \rho^K = \begin{pmatrix} 1 - |a_{4-K}|^2 & 0 \\ 0 & |a_{4-K}|^2 \end{pmatrix} \quad (6)$$

Here, we discuss quantum discord in all the two-qubit reduced density matrices of the three-qubit pure W state. The reduced density matrix (5) satisfies the condition

$|\sqrt{\rho_{00}\rho_{33}} - \sqrt{\rho_{11}\rho_{22}}| = |\rho_{12}| + |\rho_{03}|$, where $\rho_{00} = 1 - |a_{4-J}|^2 - |a_{4-K}|^2$, $\rho_{03} = \rho_{33} = 0$ and $\rho_{12} = a_{4-K}a_{4-J}$, $\rho_{11} = |a_{4-K}|^2$ and $\rho_{22} = |a_{4-J}|^2$. Then, from the results in [20] and [21], quantum discord $D^J(\rho^{JK})$ has a simple form derived from measuring J . Quantum discord is given by

$$D^J(\rho^{JK}) = S(\rho^J) + S(\rho^K | \Pi^J) - S(\rho^{JK}) \quad (7)$$

where $S(\rho^K | \Pi^J)$ is the conditional entropy $p_1 S(\rho_1^K) + p_2 S(\rho_2^K)$.

For each outcome i on J , the remaining state of K is given by

$$\rho_i^K = \begin{pmatrix} 1 - |a_{4-K}|^2 & (-1)^{i-1} a_{4-K} a_{4-J} \\ (-1)^{i-1} a_{4-K} a_{4-J} & |a_{4-K}|^2 \end{pmatrix} \quad (8)$$

For each outcome, $\rho_i = \frac{1}{2}$. Quantum discord is asymmetric when J and K systems are exchanged. Therefore, by measuring K for all the two-qubit density matrices (5), the quantum discord can be derived:

$$D^K(\rho^{JK}) = S(\rho^K) + S(\rho^J | \Pi^K) - S(\rho^{JK}). \quad (9)$$

where $S(\rho^J | \Pi^K)$ is the conditional entropy $p_1 S(\rho_1^J) + p_2 S(\rho_2^J)$. For each outcome i on K , the remaining state of J is given by

$$\rho_i^J = \begin{pmatrix} 1 - |a_{4-J}|^2 & (-1)^{i-1} a_{4-K} a_{4-J} \\ (-1)^{i-1} a_{4-K} a_{4-J} & |a_{4-J}|^2 \end{pmatrix} \quad (10)$$

For each outcome, $\rho_i = \frac{1}{2}$. Then, we can list all two-qubit quantum discords in the three-qubit pure W state:

$$\{D^1(\rho^{12}), D^2(\rho^{23}), D^1(\rho^{13}), D^2(\rho^{12}), D^3(\rho^{23}), D^3(\rho^{13})\} \quad (11)$$

This set completely determines the quantum correlations in the three-qubit pure W state (4). In this paper, we compute the two-qubit discord in the one-parametric three-qubit pure W state. Without a loss of generality, we assume positive

parameters $a_1 = a_3 = a$ and $a_2 = \sqrt{1-2a^2}$ ($0 \leq a \leq \frac{1}{\sqrt{2}}$). Then,

$S(\rho^1) = S(\rho^3) = S(\rho^{12}) = S(\rho^{23})$, $S(\rho^{13}) = S(\rho^2)$. After some manipulation, all two-qubit discords in one-parametric three-qubit pure W state are reduced to

$$\{D^1(\rho^{12}), D^2(\rho^{23}), D^1(\rho^{13})\} \quad (12)$$

where

$$\begin{aligned} D^1(\rho^{12}) &= S(\rho^2 | \Pi^1), \\ D^2(\rho^{23}) &= S(\rho^2) + S(\rho^3 | \Pi^2) - S(\rho^{23}), \\ D^1(\rho^{13}) &= S(\rho^1) + S(\rho^3 | \Pi^1) - S(\rho^{13}) \end{aligned} \quad (13)$$

The following cases are shown in **Fig. 1**:

When $a = 0$ and $|W_3\rangle = |010\rangle$, the reduced density matrices are product states and $D^1(\rho^{12}) = D^2(\rho^{23}) = D^1(\rho^{13}) = 0$.

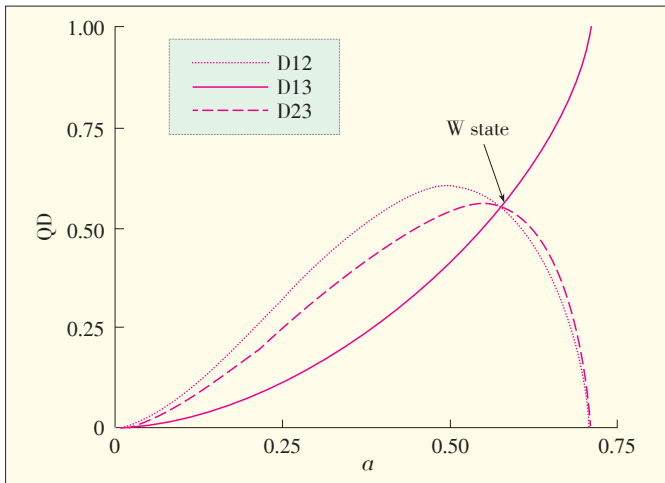
When $a = \frac{1}{\sqrt{2}}$, $|W_3\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |100\rangle)$, and $\rho^{13} = |\Phi\rangle\langle\Phi|$,

where $|\Phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, then $D^1(\rho^{13}) = 1$ and $D^1(\rho^{12}) = D^2(\rho^{23}) = 0$.

when $a = \frac{1}{\sqrt{3}}$, $|W_3\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, and the reduced density matrices are the same, then $D^1(\rho^{12}) = D^2(\rho^{23}) = D^1(\rho^{13}) \approx 0.55$.

Reducible Discord in Generic Three-Qubit Pure W States

Zhengjun Xi, Zhihui Li, and Yongming Li



▲ Figure 1. Reducible discord in one-parametric three-qubit pure W states. Here, the parameter $a_1 = a_3 = a \in [0, \frac{1}{2}]$.

When $0 < a < \frac{1}{3}$, then $D^1(\rho^{12}) > D^2(\rho^{23}) > D^1(\rho^{13})$.

When $\frac{1}{3} < a < \frac{1}{2}$, then $D^1(\rho^{13}) > D^2(\rho^{23}) > D^1(\rho^{12})$.

At first, it might seem that $\{D^1(\rho^{12}), D^2(\rho^{23}), D^1(\rho^{13})\}$ conflicts with the conclusions in [4] and [5]. However, the reduced density matrices ρ^{12} and ρ^{23} are unitary equivalents and have the same information. In this sense, the matrices have the same position to determine the W state [4], but their discords are different.

4 Conclusion

We have described how quantum correlations in generic three-qubit pure W states can be given by the two-qubit discords of these states. Our results show that reducing discord in the generalized three-qubit pure W state is complicated. The results in this paper might also be useful in a general scenario. For example, our results could be used to verify the monogamy and entropy uncertainty relationship.

References

- [1] D. L. Zhou, "Irreducible Multiparty Correlations in Quantum States without Maximal Rank," *Phys. Rev. Lett.*, vol. 101, pp. 1–4, Oct. 31, 2008.
- [2] P. Parashar and S. Rana, "Reducible correlations in Dicke states," *J. Phys. A: Math. Theor.* vol. 42, pp. 1–11, Oct. 28, 2009.
- [3] N. S. Jones and N. Linden, "Parts of quantum states," *Phys Rev A*, vol. 71, pp. 1–7, Jan. 18, 2005.
- [4] P. Parashar and S. Rana, "N-qubit W states are determined by their bipartite marginals," *Phys Rev A*, vol. 80, pp. 1–4, July. 17, 2009.
- [5] P. Parashar and S. Rana, "Optimal reducibility of all W states equivalent under stochastic local operations and classical communication," *Phys Rev A*, vol. 84, pp. 1–7, Nov. 29, 2011.
- [6] V. Scarani and N. Gisin, "Quantum Communication between N Partners and Bell's Inequalities," *Phys. Rev. Lett.*, vol. 87, pp. 1–4, Aug. 24, 2001.
- [7] V. Scarani and N. Gisin, "Quantum key distribution between N partners: Optimal eavesdropping and Bell's inequalities," *Phys. Rev. A*, vol. 65, pp. 1–8, Dec. 12, 2001.
- [8] N. R. Zhou, L. J. Wang, L.H. Gong, X. W. Zuo, and Y. Liu, "Quantum deterministic key distribution protocols based on teleportation and entanglement swapping," *Opt. Comm.*, vol. 284, pp. 4836–4842, Sept. 1, 2011.
- [9] A. Sen(De), U. Sen, M. Wieśniak, D. Kaszlikowski, and M. Zukowski, "Multiqubit W states lead to stronger nonclassicality than Greenberger–Horne–Zeilinger states," *Phys Rev A*, vol. 68, pp. 1–7, Dec. 9, 2003.
- [10] N. Linden, S. Popescu, and W. K. Wootters, "Almost Every Pure State of Three Qubits Is Completely Determined by Its Two-Particle Reduced Density Matrices," *Phys. Rev. Lett.*, vol. 89, pp. 1–4, Oct. 24, 2002.
- [11] N. Linden and W. K. Wootters, "The Parts Determine the Whole in a Generic Pure Quantum State," *Phys. Rev. Lett.*, vol. 89, pp. 1–4, Dec. 20, 2002.
- [12] L. Diósi, "Three-party pure quantum states are determined by two two-party reduced states," *Phys. Rev. A*, vol. 70, pp. 1–2, July. 20, 2004.
- [13] H. Ollivier and W. H. Zurek, "Quantum Discord: A Measure of the Quantumness of Correlations," *Phys. Rev. Lett.*, vol. 88, pp. 1–4, Dec. 14, 2001.
- [14] L. Henderson and V. Vedral, "Classical, quantum and total correlations," *J. Phys. A: Math. Gen.* vol.34, pp. 6899–6905, Aug. 24, 2001.
- [15] A. Datta, A. Shaji, and C. M. Caves, "Quantum Discord and the Power of One Qubit," *Phys. Rev. Lett.*, vol. 100, pp. 1–4, Feb. 5, 2008.
- [16] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, "The classical-quantum boundary for correlations:Discord and related measures," *Rev. Mod. Phys.*, vol. 84, pp. 1655–1707, Nov. 26, 2012.
- [17] S. Hamieh, R. Kobes, and H. Zaraket, "Positive-operator-valued measure optimization of classical correlations," *Phys. Rev. A*, vol. 70, pp. 1–6, Nov. 29, 2004.
- [18] S. L. Luo, "Quantum discord for two-qubit systems," *Phys. Rev. A*, vol. 77, pp. 1–6, Apr. 3, 2008.
- [19] M. Ali, A. R. P. Rau, and G. Alber, "Quantum discord for two-qubit X states," *Phys. Rev. A*, vol. 81, pp. 1–7, Apr. 12, 2010.
- [20] X. M. Lu, J. Ma, Z. J. Xi, and X. G. Wang, "Optimal measurements to access classical correlations of two-qubit states," *Phys. Rev. A*, vol. 83, pp. 1–7, Jan. 31, 2011.
- [21] Q. Chen, C. J. Zhang, S. X. Yu, X. X. Yi, and C. H. Oh, "Quantum discord of two-qubit X states," *Phys. Rev. A*, vol. 84, pp. 1–5, Oct. 6, 2011.
- [22] Y. C. Huang, "Computational complexity of quantum correlation: quantum discord is NP-complete [online]. Available: <http://arxiv.org/abs/1305.5941>

Manuscript received: July 28, 2013

Biographies

Zhengjun Xi (xizhengjun@snnu.edu.cn) received his PhD in computer science from Shaanxi Normal University, Xi'an, China, in 2012. He is currently a lecturer in the College of Computer Science, Shaanxi Normal University. His research interests include quantum information theory and quantum computation. He has published more than 20 papers.

Zhihui Li (lizhihui@snnu.edu.cn) received his PhD from Northwestern Polytechnical University, Xi'an, China, in 2002. She is currently a professor in the College of Mathematics and Information Science, Shaanxi Normal University. She has published more than 60 papers.

Yongming Li (liyongm@snnu.edu.cn) received his PhD from Sichuan University, Chengdu, China, in 1996. He is currently a professor in the College of Computer Science, Shaanxi Normal University. His research interests include computation theory, fuzzy control theory, fuzzy automata theory, fuzzy and quantum logic, and topology over lattices. He has published more than 150 papers.

Two-Way Cooperative Quantum Communication with Partial Entanglement Analysis

Yunkai Deng, Zhujun Gao, and Ying Guo

(Central South University, Changsha 410083, China)

Abstract

In this paper, we describe an improved cooperative two-way quantum communication scheme that works in a forward-and-backward fashion. In this scheme, partial entanglement analysis based on five-qubit entangled Brown state allows for the simultaneous exchange of arbitrary unknown states between Alice and Bob (with the help of trusted Charlie). Security is guaranteed because opposing unknown states are transmitted by performing the suitable recovery operations in a deterministic way or, in the case of irregularities, no results are generated. The current two-way quantum communication scheme can also be extended to transmit arbitrary unknown states. This is done in a probabilistic way by using two-way quantum teleportation based on the generalized Brown-like state.

Keywords

quantum teleportation; two-way communication; brown state; bell states; entanglement

1 Introduction

Entanglement has been widely applied in quantum information theory and quantum computation [1]. An elegant application of entanglement is quantum teleportation (QT) [2], [3], in which an arbitrary unknown state is transmitted without distributing the quantum carrier itself. QT was first proposed by C.H. Bennett et al. in 1993. Since then, QT has been theoretically and experimentally investigated [4]. Several schemes with different entanglement states have been reported. These states include Bell states [5]–[7], Greenberger–Horne–Zeiling (GHZ) states [8], and W states [9], [10]. Two-qubit entanglement states can be transmitted via quantum teleportation based on four-qubit entanglement states [11]–[13]. All QT schemes allow one-way, point-to-point transmission of single-qubit or multi-qubit entanglement states.

In practical applications, problems arise when two participants (Alice and Bob) exchange unknown states in a small quantum network. To solve this problem, Mishra et al. [14] propose a two-way quantum communication scheme in which unknown single-qubit states can be exchanged. This exchange is based on the six-qubit entanglement state established between Alice and Bob (with the help of a third party, Charlie). Without Charlie, Alice and Bob could not recover the required states in a deterministic way because they do not know which channel will be established between them.

Recently, much research has been done on the multi-qubit entanglement state. In [15], the Brown state is described. This five-qubit maximally entangled state is achieved by using a numerical optimization procedure. Because it is highly entangled, this state can be used for QT [16], quantum secret sharing, superdense coding, secure communication [17], and information splitting [18]. In [19], Sreraman et al. [19] proposed a one-way QT for transmitting unknown states based on the Brown state.

In a quantum computation network, information may be simultaneously transmitted from Alice to Bob and from Bob to Alice. Consequently, two one-way QT schemes (one from Alice to Bob and one from Bob to Alice) may be switched on. However, a network becomes insecure or dishonest when Bob achieves Alice's unknown states but fails to send his Bell state measurements (BSMs) to Alice. Alice needs to recover Bob's unknown states at the same time Bob receives Alice's unknown because QT needs the BSM results from sender to receiver to recover unknown states. To solve this problem, QT must simultaneously transmit Alice's unknown states to Bob and Bob's unknown states to Alice. Also, QT must either exchange unknown states or, in the case of irregularities, generate no results. In this paper, we describe a two-way QT scheme in which partial entanglement analysis is performed. This scheme makes use of two local BSMs that are based on the Brown state rather than the Bell states usually used in standard QT schemes.

In section 2, we describe an improved cooperative two-way QT scheme that uses the help of a trusted third party, Charlie. We analyze this scheme using partial entanglement analysis based on the Brown state. In section 3, we propose a general two-way QT scheme for transmitting unknown states backward and forward. This transmission occurs in a probabilistic way, and the unknown states are assumed to be Brown-like states. Section 4 concludes the paper.

2 Cooperative Two-Way QT Based on Brown States

Alice, Bob and Charlie prepare a five-qubit entanglement Brown state $|j_{Bri12345}\rangle$ as the information carrier in a small quantum network. The subscript pairs 1 and 2, and 4 and 5 refer to the modes entangled with Alice and Bob, respectively. The subscript 3 refers to the mode entangled with Charlie. This mode is given by

$$|Br\rangle_{12345} = \frac{1}{2}(|001\rangle|\Psi^-\rangle + |010\rangle|\Phi^-\rangle + |110\rangle|\Psi^+\rangle + |111\rangle|\Phi^+\rangle) \quad (1)$$

where $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ are four standard Bell states given by

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (2)$$

Suppose Alice sends an arbitrary unknown state in mode 0, i.e. $|\varphi_a\rangle_0 = \alpha|0\rangle + \beta|1\rangle$, to Bob. At the same time, Bob sends another arbitrary unknown state in mode 6, i.e. $|\varphi_b\rangle_6 = \gamma|0\rangle + \delta|1\rangle$, to Alice. Alice and Bob both obtain the required states or, if there is a discrepancy, do not obtain the required states. Here, the coefficients are real and satisfy the two constraints $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$. The direct-product state is given as

$$|\Psi_{ab}\rangle_{06} = |\varphi_a\rangle_0 \otimes |\varphi_b\rangle_6 = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \quad (3)$$

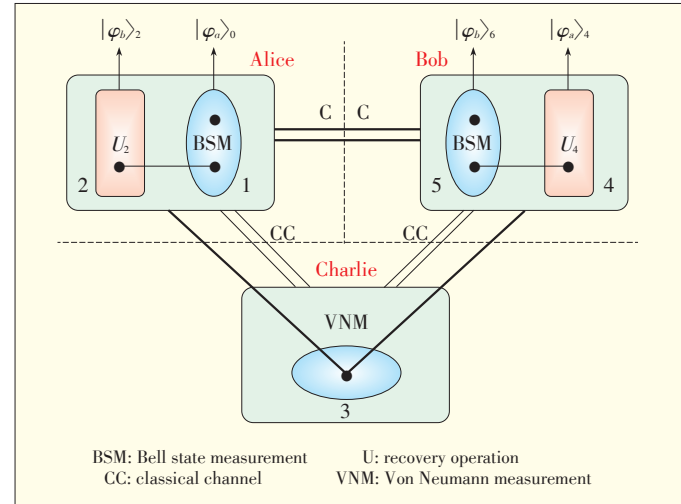
Therefore, the combined quantum system is given by

$$|\Delta\rangle_{0123456} = |\varphi_a\rangle_0 \otimes |Br\rangle_{12345} \otimes |\varphi_b\rangle_6 \quad (4)$$

which can be rewritten as

$$\begin{aligned} |\Delta\rangle_{0123456} = & \frac{\alpha\gamma}{4\sqrt{2}} [(|\Phi^+\rangle + |\Phi^-\rangle)(|010\rangle - |101\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) + (|100\rangle - |011\rangle)(|\Phi^+\rangle + |\Phi^-\rangle) + \\ & (|\Psi^+\rangle + |\Psi^-\rangle)(|000\rangle - |111\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) + (|001\rangle + |110\rangle)(|\Phi^+\rangle + |\Phi^-\rangle)] + \\ & \frac{\alpha\delta}{4\sqrt{2}} [(|\Phi^+\rangle + |\Phi^-\rangle)(|010\rangle - |101\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) - (|011\rangle - |100\rangle)(|\Psi^+\rangle + |\Psi^-\rangle) + \\ & (|\Psi^+\rangle + |\Psi^-\rangle)(|000\rangle + |111\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) + (|001\rangle + |110\rangle)(|\Psi^+\rangle + |\Psi^-\rangle)] + \\ & \frac{\beta\gamma}{4\sqrt{2}} [(|\Psi^+\rangle - |\Psi^-\rangle)(|010\rangle - |101\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) - (|011\rangle - |100\rangle)(|\Phi^+\rangle + |\Phi^-\rangle) + \\ & (|\Phi^+\rangle - |\Phi^-\rangle)(|000\rangle + |111\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) + (|001\rangle + |110\rangle)(|\Phi^+\rangle + |\Phi^-\rangle)] + \\ & \frac{\beta\delta}{4\sqrt{2}} [(|\Psi^+\rangle - |\Psi^-\rangle)(|010\rangle - |101\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) - (|011\rangle - |100\rangle)(|\Psi^+\rangle + |\Psi^-\rangle) + \\ & (|\Phi^+\rangle - |\Phi^-\rangle)(|000\rangle + |111\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) + (|001\rangle + |110\rangle)(|\Psi^+\rangle + |\Psi^-\rangle)] \end{aligned} \quad (5)$$

If Alice and Bob want to exchange unknown states, a secure, cooperative two-way communication scheme can be used. This scheme is implemented with the help of Charlie via two-hop QT based on the Brown state (**Fig.1**).



▲ Figure 1. Cooperative two-way QT scheme based on the Brown state.

First, Alice measures the Bell states of the photons in modes 0 and 1. At the same time, Bob measures the Bell states of the photons in modes 5 and 6. Both Alice and Bob convey their BSMs $M_A, M_B \in \{00, 01, 10, 11\}$ to the trusted Charlie. These BSMs are sent through the classic channels. The yielded state $|\Omega\rangle_{234}$ is achieved in modes $\{2, 3, 4\}$ (**Table 1**). Then, Charlie calculates $C_m = M_A \otimes M_B = M_A + M_B \bmod 2$. After that, he uses the von Neumann measurement (VNM) on the photon in mode 3, with $\{|0\rangle, |1\rangle\}$ as the basis of this measurement. The result of the VNM conforms to $M_c \in \{00, 01\}$, which means that $M_c = 00/01$. This corresponds to the VNM $|0\rangle/|1\rangle$. Then, Charlie calculates D_m , given by

$$D_m = \begin{cases} C_m \otimes \{M_c = 00\}, & \text{for } C_m \in \{00, 01\} \\ C_m \otimes \{M_c = 01\}, & \text{for } C_m \in \{10, 11\} \end{cases} \quad (6)$$

Finally, Charlie broadcasts D_m to Alice and Bob through the classic channels.

Alice and Bob obtain M_B and M_A , respectively, when they decode M_c from the received D_m . If $D_m \in \{00, 01\}$, then Alice obtains $M_c = 00$; otherwise, she obtains $M_c = 01$. Alice decrypts Bob's M_B according to her own M_A , which is derived from C_m . Similarly, Bob securely obtains Charlie's M_c and Alice's M_A from D_m . Finally, Alice and Bob recover the opposite unknown

Two-Way Cooperative Quantum Communication with Partial Entanglement Analysis

Yunkai Deng, Zhujun Gao, and Ying Guo

▼ Table 1. Relationship between Alice's BSM and the photons in modes 0 and 1, relationships between Bob's BSM and the photons in modes 5 and 6, and the entanglement states yielded in modes {2; 3; 4}

BSM _A	BSM _B	$ \Omega\rangle_{234}$
$ \Phi^+\rangle$	$ \Phi^+\rangle$	$\alpha\gamma(100\rangle- 011\rangle)+\alpha\delta(010\rangle- 101\rangle)+\beta\gamma(001\rangle+ 110\rangle)+\beta\delta(000\rangle+ 111\rangle)$
	$ \Phi^-\rangle$	$\alpha\gamma(100\rangle- 011\rangle)+\alpha\delta(010\rangle- 101\rangle)+\beta\gamma(001\rangle+ 110\rangle)-\beta\delta(000\rangle+ 111\rangle)$
	$ \Psi^+\rangle$	$\alpha\gamma(010\rangle- 101\rangle)+\alpha\delta(100\rangle- 011\rangle)+\beta\gamma(000\rangle+ 111\rangle)+\beta\delta(001\rangle+ 110\rangle)$
	$ \Psi^-\rangle$	$\alpha\gamma(010\rangle- 101\rangle)+\alpha\delta(100\rangle- 011\rangle)-\beta\gamma(000\rangle+ 111\rangle)+\beta\delta(001\rangle+ 110\rangle)$
$ \Phi^-\rangle$	$ \Phi^+\rangle$	$\alpha\gamma(100\rangle- 011\rangle)+\alpha\delta(010\rangle- 101\rangle)-\beta\gamma(001\rangle+ 110\rangle)-\beta\delta(000\rangle+ 111\rangle)$
	$ \Phi^-\rangle$	$\alpha\gamma(100\rangle- 011\rangle)+\alpha\delta(010\rangle- 101\rangle)-\beta\gamma(001\rangle+ 110\rangle)+\beta\delta(000\rangle+ 111\rangle)$
	$ \Psi^+\rangle$	$\alpha\gamma(010\rangle- 101\rangle)+\alpha\delta(100\rangle- 011\rangle)-\beta\gamma(000\rangle+ 111\rangle)-\beta\delta(001\rangle+ 110\rangle)$
	$ \Psi^-\rangle$	$\alpha\gamma(010\rangle- 101\rangle)+\alpha\delta(100\rangle- 011\rangle)+\beta\gamma(000\rangle+ 111\rangle)-\beta\delta(001\rangle+ 110\rangle)$
$ \Psi^+\rangle$	$ \Phi^+\rangle$	$\alpha\gamma(001\rangle+ 110\rangle)+\alpha\delta(000\rangle+ 111\rangle)+\beta\gamma(100\rangle- 011\rangle)+\beta\delta(010\rangle- 101\rangle)$
	$ \Phi^-\rangle$	$\alpha\gamma(001\rangle+ 110\rangle)-\alpha\delta(000\rangle+ 111\rangle)+\beta\gamma(100\rangle- 011\rangle)+\beta\delta(010\rangle- 101\rangle)$
	$ \Psi^+\rangle$	$\alpha\gamma(000\rangle+ 111\rangle)+\alpha\delta(001\rangle+ 110\rangle)+\beta\gamma(010\rangle- 101\rangle)+\beta\delta(100\rangle- 011\rangle)$
	$ \Psi^-\rangle$	$-\alpha\gamma(000\rangle+ 111\rangle)+\alpha\delta(001\rangle+ 110\rangle)+\beta\gamma(101\rangle- 010\rangle)+\beta\delta(100\rangle- 011\rangle)$
$ \Psi^-\rangle$	$ \Phi^+\rangle$	$\alpha\gamma(001\rangle+ 110\rangle)+\alpha\delta(000\rangle+ 111\rangle)+\beta\gamma(011\rangle- 100\rangle)+\beta\delta(101\rangle- 010\rangle)$
	$ \Phi^-\rangle$	$\alpha\gamma(001\rangle+ 110\rangle)-\alpha\delta(000\rangle+ 111\rangle)+\beta\gamma(011\rangle- 100\rangle)+\beta\delta(101\rangle- 010\rangle)$
	$ \Psi^+\rangle$	$\alpha\gamma(000\rangle+ 111\rangle)+\alpha\delta(001\rangle+ 110\rangle)+\beta\gamma(101\rangle- 010\rangle)+\beta\delta(011\rangle- 100\rangle)$
	$ \Psi^-\rangle$	$-\alpha\gamma(000\rangle+ 111\rangle)+\alpha\delta(001\rangle+ 110\rangle)+\beta\gamma(010\rangle- 101\rangle)+\beta\delta(011\rangle- 100\rangle)$
BSM: Bell state measurement		

states $|\varphi_b\rangle$ and $|\varphi_a\rangle$, respectively, after performing suitable recovery operations in modes 2 and 4 (Table 2).

If Alice and Bob's BSMs are both $|\Phi^+\rangle$, i.e. $M_A = M_B = 00$, and if Charlie's VNM is $|0\rangle$, i.e. $M_C = 00$, then the resulting state in modes 2 and 4 is

$$|\varphi_{24}^{(1)}\rangle = \alpha\gamma|10\rangle - \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|00\rangle \quad (7)$$

To achieve the unknown direct-product state in modes 2 and 4, and expressed in (3), Alice and Bob perform the controlled-phase operation Z in modes 2 and 4, respectively, and obtain the state

$$|\varphi_{24}^{(2)}\rangle = \alpha\gamma|10\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|00\rangle \quad (8)$$

Then, Alice applies the unitary operation σ_x in mode 2. This results in

$$|\varphi_{24}^{(3)}\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \quad (9)$$

Subsequently, Alice and Bob perform the controlled-NOT operation, $C(2, 4)$, on the photons in modes 2 and 4, where mode 2 is the control qubit, and mode 4 is the target qubit. Finally, Alice and Bob obtain the direct-product state, given by

$$|\varphi_{24}\rangle = (\gamma|0\rangle + \delta|1\rangle)_2 \otimes (\alpha|0\rangle + \beta|1\rangle)_4 \quad (10)$$

From (10), Alice can determine Bob's unknown state $|\varphi_b\rangle_2$ in mode 2, and Bob can determine Alice's unknown state $|\varphi_a\rangle_4$ in mode 4 by

disentangling [1].

The controlled-phase operation performed in modes 2 and 4, is denoted Z , i.e., $Z|00\rangle = |00\rangle$, $Z|01\rangle = |01\rangle$, $Z|10\rangle = |10\rangle$, $Z|11\rangle = -|11\rangle$. An identity operation is denoted I , and Pauli operations are denoted σ_x and σ_z . The controlled-NOT gate, denoted $C(2,4)$, designates the control qubit in mode 2 and target qubit in mode 4. For simplicity, the normalization of the resulting states is omitted.

The operations performed by Alice and Bob to exchange unknown states are depend entirely on M_C of Charlie. To improve the security of the two-way QT, M_A , M_B and M_C need to be encrypted by Charlie before being broadcast to Alice and Bob. Without the help of Charlie, Alice and Bob cannot exchange their unknown states. Furthermore, if either Alice or Bob fails to convey M_A or M_B , then Charlie will break off communication without transmitting any information to Bob or Alice. In this scenario, we designate the secure two-way QT via the partial entanglement analysis in for-

▼ Table 2. Recovery operations $U_{24} = U_2 \otimes U_4$ performed in modes 2 and 4 and based on Alice and Bob's BSMs, respectively

BSM	BSM	VNM	Yielded states in modes 2 and 4	Recovery operation U_{24}
$ \Phi^+\rangle_A$	$ \Phi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 10\rangle-\alpha\delta 11\rangle+\beta\gamma 01\rangle+\beta\delta 00\rangle$	$Z, \sigma_x \otimes I, C(2, 4)$
		$ 1\rangle_3$	$-\alpha\gamma 01\rangle+\alpha\delta 00\rangle+\beta\gamma 10\rangle+\beta\delta 11\rangle$	$I \otimes \sigma_x, \sigma_x \otimes \sigma_x, Z, C(2, 4)$
	$ \Phi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 10\rangle+\alpha\delta 11\rangle+\beta\gamma 01\rangle-\beta\delta 00\rangle$	$\sigma_x \otimes I, C(2, 4), Z$
		$ 1\rangle_3$	$-\alpha\gamma 01\rangle-\alpha\delta 00\rangle+\beta\gamma 10\rangle-\beta\delta 11\rangle$	$I \otimes \sigma_x, Z, C(2, 4)$
	$ \Psi^+\rangle_B$	$ 0\rangle_3$	$-\alpha\gamma 11\rangle+\alpha\delta 10\rangle+\beta\gamma 00\rangle+\beta\delta 01\rangle$	$Z, \sigma_x \otimes \sigma_x, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 00\rangle-\alpha\delta 01\rangle+\beta\gamma 11\rangle+\beta\delta 10\rangle$	$\sigma_x \otimes I, \sigma_x \otimes I, C(2, 4)$
	$ \Psi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 11\rangle+\alpha\delta 10\rangle-\beta\gamma 00\rangle+\beta\delta 01\rangle$	$I \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$-\alpha\gamma 00\rangle-\alpha\delta 01\rangle-\beta\gamma 11\rangle+\beta\delta 10\rangle$	$C(2, 4), Z$
$ \Phi^-\rangle_A$	$ \Phi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 10\rangle-\alpha\delta 11\rangle-\beta\gamma 01\rangle-\beta\delta 00\rangle$	$\sigma_x \otimes I, \sigma_x \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$-\alpha\gamma 01\rangle+\alpha\delta 00\rangle-\beta\gamma 10\rangle-\beta\delta 11\rangle$	$\sigma_x \otimes \sigma_x, Z$
	$ \Phi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 10\rangle+\alpha\delta 11\rangle-\beta\gamma 01\rangle+\beta\delta 00\rangle$	$\sigma_x \otimes I, Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 00\rangle-\alpha\delta 01\rangle-\beta\gamma 11\rangle-\beta\delta 10\rangle$	$I \otimes \sigma_x, C(2, 4), Z$
	$ \Psi^+\rangle_B$	$ 0\rangle_3$	$-\alpha\gamma 11\rangle+\alpha\delta 10\rangle-\beta\gamma 00\rangle-\beta\delta 01\rangle$	$\sigma_x \otimes \sigma_x, I \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 00\rangle-\alpha\delta 01\rangle-\beta\gamma 11\rangle-\beta\delta 10\rangle$	$\sigma_x \otimes \sigma_x, Z, C(2, 4)$
	$ \Psi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 11\rangle+\alpha\delta 10\rangle+\beta\gamma 00\rangle-\beta\delta 01\rangle$	$\sigma_x \otimes \sigma_x, C(2, 4), Z$
		$ 1\rangle_3$	$-\alpha\gamma 00\rangle-\alpha\delta 01\rangle+\beta\gamma 11\rangle-\beta\delta 10\rangle$	$Z, C(2, 4)$
$ \Psi^+\rangle_A$	$ \Phi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 01\rangle+\alpha\delta 00\rangle+\beta\gamma 10\rangle-\beta\delta 11\rangle$	$Z, I \otimes \sigma_x, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 10\rangle+\alpha\delta 01\rangle-\beta\gamma 01\rangle+\beta\delta 00\rangle$	$\sigma_x \otimes I, Z, C(2, 4)$
	$ \Phi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 01\rangle-\alpha\delta 00\rangle+\beta\gamma 10\rangle+\beta\delta 11\rangle$	$I \otimes \sigma_x, I \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 10\rangle-\alpha\delta 01\rangle-\beta\gamma 01\rangle-\beta\delta 00\rangle$	$\sigma_x \otimes I, Z, \sigma_x \otimes I, C(2, 4)$
	$ \Psi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 00\rangle-\alpha\delta 01\rangle+\beta\gamma 11\rangle+\beta\delta 10\rangle$	$Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 11\rangle+\alpha\delta 10\rangle+\beta\gamma 00\rangle-\beta\delta 01\rangle$	$\sigma_x \otimes \sigma_x, C(2, 4), Z$
	$ \Psi^-\rangle_B$	$ 0\rangle_3$	$-\alpha\gamma 00\rangle+\alpha\delta 01\rangle+\beta\gamma 11\rangle+\beta\delta 10\rangle$	$\sigma_x \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$-\alpha\gamma 11\rangle+\alpha\delta 10\rangle-\beta\gamma 00\rangle-\beta\delta 01\rangle$	$\sigma_x \otimes \sigma_x, I \otimes \sigma_x, Z, C(2, 4)$
$ \Psi^-\rangle_A$	$ \Phi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 01\rangle+\alpha\delta 00\rangle-\beta\gamma 10\rangle+\beta\delta 11\rangle$	$I \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 10\rangle+\alpha\delta 01\rangle+\beta\gamma 01\rangle+\beta\delta 00\rangle$	$\sigma_x \otimes I, C(2, 4)$
	$ \Phi^-\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 01\rangle-\alpha\delta 00\rangle-\beta\gamma 10\rangle-\beta\delta 11\rangle$	$I \otimes \sigma_x, \sigma_x \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$\alpha\gamma 10\rangle-\alpha\delta 01\rangle+\beta\gamma 01\rangle+\beta\delta 00\rangle$	$Z, \sigma_x \otimes I, C(2, 4)$
	$ \Psi^+\rangle_B$	$ 0\rangle_3$	$\alpha\gamma 00\rangle+\alpha\delta 01\rangle+\beta\gamma 11\rangle-\beta\delta 10\rangle$	$C(2, 4), Z$
		$ 1\rangle_3$	$\alpha\gamma 11\rangle+\alpha\delta 10\rangle-\beta\gamma 00\rangle+\beta\delta 01\rangle$	$\sigma_x \otimes \sigma_x, Z, C(2, 4)$
	$ \Psi^-\rangle_B$	$ 0\rangle_3$	$-\alpha\gamma 00\rangle+\alpha\delta 01\rangle-\beta\gamma 11\rangle-\beta\delta 10\rangle$	$I \otimes \sigma_x, Z, C(2, 4)$
		$ 1\rangle_3$	$-\alpha\gamma 11\rangle+\alpha\delta 10\rangle+\beta\gamma 00\rangle+\beta\delta 01\rangle$	$Z, \sigma_x \otimes \sigma_x, C(2, 4)$
BSM: Bell state measurement U: recovery operation VNM: Von Neumann measurement				

ward-and-backward quantum channels.

3 Extended Cooperative Two-Way QT with the Brown-Like State

Here, we extend the two-way QT scheme. This scheme is extended in order so that unknown states, based on entangled Brown-like states established between Alice, Bob, and Charlie, can be exchanged. Alice and Bob's unknown states can be represented as the direct-product state in (3). However, the five-qubit entanglement state prepared as a quantum channel for QT is not maximally entangled. This is called the Brown-like state $|\varpi\rangle_{12345}$ and is given by

$$|\varpi\rangle_{12345} = a|001\rangle|\Psi^-\rangle + b|010\rangle|\Phi^-\rangle + c|110\rangle|\Psi^+\rangle + d|111\rangle|\Phi^+\rangle \quad (11)$$

where the photons in modes 1 and 2, and 4 and 5 are kept by Alice and Bob, respectively. The photon in mode 3 is kept by the trusted Charlie. The coefficients are real and satisfy the constraint $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

Before designating the extended two-way QT scheme, Alice and Bob prepare an unknown state $|\varphi_a\rangle_0$ in mode 0 and an unknown state $|\varphi_b\rangle_6$ in mode 6. The five-qubit entanglement state ϖ needs to be established between Alice, Bob and Charlie in advance. Then, the whole quantum system becomes

$$\begin{aligned} |\Gamma\rangle &= |\varphi_a\rangle_0 \otimes |\varpi\rangle_{12345} \otimes |\varphi_b\rangle_6 = \\ & \frac{\alpha\gamma}{2\sqrt{2}} [(|\Phi^+\rangle + |\Phi^-\rangle)(|a|010\rangle - |b|101\rangle)(|\Psi^-\rangle - |\Psi^+\rangle) + (|a|100\rangle - |b|011\rangle)(|\Phi^+\rangle + |\Phi^-\rangle) + \\ & (|\Psi^+\rangle + |\Psi^-\rangle)(|c|000\rangle - |d|111\rangle)(|\Psi^-\rangle - |\Psi^+\rangle) + (|c|001\rangle + |d|110\rangle)(|\Phi^+\rangle + |\Phi^-\rangle)] + \\ & \frac{\alpha\delta}{2\sqrt{2}} [(|\Phi^+\rangle + |\Phi^-\rangle)(|a|010\rangle - |b|101\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) - (|a|011\rangle - |b|100\rangle)(|\Psi^+\rangle + |\Psi^-\rangle) + \\ & (|\Psi^+\rangle + |\Psi^-\rangle)(|c|000\rangle + |d|111\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) + (|c|001\rangle + |d|110\rangle)(|\Psi^+\rangle + |\Psi^-\rangle)] + \\ & \frac{\beta\gamma}{2\sqrt{2}} [(|\Psi^+\rangle - |\Psi^-\rangle)(|a|010\rangle - |b|101\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) - (|a|011\rangle - |b|100\rangle)(|\Phi^+\rangle + |\Phi^-\rangle) + \\ & (|\Phi^+\rangle - |\Phi^-\rangle)(|c|000\rangle + |d|111\rangle)(|\Psi^+\rangle - |\Psi^-\rangle) + (|c|001\rangle + |d|110\rangle)(|\Phi^+\rangle + |\Phi^-\rangle)] + \\ & \frac{\beta\delta}{2\sqrt{2}} [(|\Psi^+\rangle - |\Psi^-\rangle)(|a|010\rangle - |b|101\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) - (|a|011\rangle - |b|100\rangle)(|\Psi^+\rangle + |\Psi^-\rangle) + \\ & (|\Phi^+\rangle - |\Phi^-\rangle)(|c|000\rangle + |d|111\rangle)(|\Phi^+\rangle - |\Phi^-\rangle) + (|c|001\rangle + |d|110\rangle)(|\Psi^+\rangle + |\Psi^-\rangle)] \end{aligned} \quad (12)$$

Two-way communication in the extended system flows in a similar way to that in the previous system. Alice takes a BSM in modes 0 and 1, and this measurement is denoted M'_A . At the same time, Bob takes a BSM in modes 5 and 6, and this measurement is denoted M'_B . Alice and Bob both convey their BSMs to Charlie, who takes a VNM in mode 3. The basis of this measurement is $\{|0\rangle, |1\rangle\}$, and the measurement is denoted M'_C (from $C_m = M'_A \otimes M'_B$). After that, Charlie broadcasts $D_m = C_m \otimes M'_C$ to Alice and Bob through the classic channels. Bob decrypts M'_A using the received D_m and his own M'_B . Similarly, Alice obtains M'_B by using the received D_m and her own M'_A . Finally, Bob and Alice exchange unknown states by performing the suitable recovery operations.

Without a loss of generality, we consider a case in which two pairs of photons in modes 0 and 1, and 5 and 6 have collapsed into $|\Phi^+\rangle$, and the VNM of Charlie is $M'_C = 00$. According to the previously mentioned process, the resulting state in modes 2 and 4 is

$$|\varphi'\rangle_{24} = b\alpha\gamma|10\rangle - b\alpha\delta|11\rangle + c\beta\gamma|01\rangle + c\beta\delta|00\rangle \quad (13)$$

After applying the controlled phase gate Z in modes 2 and 4, Bob prepares an ancillary qubit $|0\rangle_{4'}$ in mode $4'$. Then, he performs the entangling operation $C(2, 4')$ in modes 2 and $4'$, and obtains

$$\begin{aligned} |\varphi'\rangle_{244'}^{(1)} &= b\alpha\gamma|101\rangle + b\alpha\delta|111\rangle + c\beta\gamma|010\rangle + c\beta\delta|000\rangle = \\ & \frac{\gamma}{2} ((\alpha|10\rangle + \beta|01\rangle) \otimes (b|1\rangle + c|0\rangle) + \\ & (\alpha|10\rangle - \beta|01\rangle) \otimes (b|1\rangle - c|0\rangle)) + \\ & \frac{\delta}{2} ((\alpha|11\rangle + \beta|00\rangle) \otimes (b|1\rangle + c|0\rangle) + \\ & (\alpha|11\rangle - \beta|00\rangle) \otimes (b|1\rangle - c|0\rangle)) \end{aligned} \quad (14)$$

A state discrimination measurement can be taken to distinguish $b|1\rangle + c|0\rangle$ and $b|1\rangle - c|0\rangle$ in mode $4'$ [1]. If this measurement is $b|1\rangle + c|0\rangle$, the yielded state in modes 2 and 4 is given by

$$|\varphi'\rangle_{24}^{(1)} = \frac{\gamma}{2} (\alpha|10\rangle + \beta|01\rangle) + \frac{\delta}{2} (\alpha|11\rangle + \beta|00\rangle) \quad (15)$$

Otherwise, the yielded state is given by

$$|\varphi'\rangle_{24}^{(2)} = \frac{\gamma}{2} (\alpha|10\rangle - \beta|01\rangle) + \frac{\delta}{2} (\alpha|11\rangle - \beta|00\rangle) \quad (16)$$

For the state $|\varphi'\rangle_{24}^{(1)}$, operation σ_x is performed in mode 2, and operation $C(2, 4)$ is performed in modes 2 and 4 to obtain the direct-product state $|\varphi\rangle_{24}$ in (10). For the state $|\varphi'\rangle_{24}^{(2)}$, operation σ_x is performed in mode 2, and operation $C(2, 4)$ is performed in modes 2 and 4. Finally, Alice achieves Bob's unknown state $|\varphi_b\rangle_2$ in mode 2. Meanwhile, Bob obtains Alice's state $|\varphi_a\rangle_4$ in mode 4 after jointly applying the disentangling operations.

To enhance the security of two-way QT, Alice and Bob need to sample a large number of Brown states and compare their measurements, which are based on the entanglement of the states in the eavesdropper-detection phase. As in [20], if Eve uses an intercept-resend attack to eavesdrop on the entangled channels, she may fail to resend the intercepted state. This will be detected by the legal participants in the communication [21]. Similarly, the entangled channels established between Alice, Bob and Charlie should be made much secure by using known eavesdropper detection approaches. Effective eavesdropper attacks include intercept-resend [21]; entanglement swapping [22]; teleportation [23]; dense coding [24]; channel loss [25], denial-of-service (DoS) [26], [27]; correlation-ex-

Two-Way Cooperative Quantum Communication with Partial Entanglement Analysis

Yunkai Deng, Zhujun Gao, and Ying Guo

tract ability [28]; and Trojan horse [29], [30]. These attacks need to be understood to design secure two-way QT using partial entanglement analysis in imperfect channels. In addition, authenticating [31] and signing [32]–[36] a message can secure it from illegitimate eavesdropper.

4 Conclusion

In this paper, we have investigated an improved cooperative two-way QT scheme that makes use of partial entanglement analysis of Brown or Brown-like states. We have described how to transfer arbitrary unknown states in a secure and cooperative manner. Such transference involves encryption by trusted Charlie and combining BSM and VNM with suitable local operations. This is an alternative way of transmitting unknown states with the help of Charlie in forward-and-backward channels. Encryption is critical in quantum repeaters to secure a quantum computation network.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (60902044, 61172184), the New Century Excellent Talents in University (NCET-11-0510), and partly by the World Class University R32-2010-000-20014-0 NRF, and Fundamental Research 2010-0020942 NRF, Korea.

References

- [1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.
- [2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Press, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, 1993.
- [3] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Phys. Rev. Lett.*, vol. 80, pp. 1121–1125, 1998.
- [4] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology*. New York: Crypto 82 Plenum Press, 1982.
- [5] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature (London)*, vol. 390, pp. 575–579, 11 December 1997.
- [6] C.-Y. Lu, T. Yang, and J.-W. Pan, "Experimental Multiparticle Entanglement Swapping for Quantum Networking," *Phys. Rev. Lett.*, vol. 103, no. 2, Jul. 2009.
- [7] M. Riebe, et al., "Deterministic quantum teleportation with atoms," *Nature (London)*, vol. 429, pp. 734–737, 17 June 2004.
- [8] A. Karlsson and M. Bourennane, "Quantum teleportation using three-particle entanglement," *Phys. Rev. A*, vol. 58, no. 6, pp. 4394–4400, 1998.
- [9] P. Agrawal and A. Pati, "Perfect teleportation and superdense coding with W states," *Phys. Rev. A*, vol. 74, no. 6, 062320, 2006.
- [10] V. N. Gorbachev, A. I. Trubilko, and A. A. Rodichkina, "Can the states of the W-class be suitable for teleportation?" *Phys. Lett. A*, vol. 314, no. 4, pp. 267–271, Aug. 2003.
- [11] J. Lee, H. Min and S. D. Oh, "Multiparticle entanglement for entanglement teleportation," *Phys. Rev. A*, vol. 66, no. 5, 052318, 2002.
- [12] G. Rigolin, "Quantum teleportation of an arbitrary two-qubit state and its relation to multiparticle entanglement," *Phys. Rev. A*, vol. 71, 032303, 2005.
- [13] Y. Yeo and W. K. Chua, "Teleportation and Dense Coding with Genuine Multiparticle Entanglement," *Phys. Rev. Lett.*, vol. 96, 060502, 2006.
- [14] M. K. Mishra, A. K. Maurya, and H. K. Prakash, J., "Two-way quantum communication: 'secure quantum information exchange,'" *Phys. B: At. Mol. Opt. Phys.*, vol. 44, no. 11, 115504, 2011.
- [15] S. Muralidharan and P. K. Panigrahi, "Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit

state," *Phys. Rev. A*, vol. 77, 032321, 2008.

- [16] X. W. Wang and Z. H. Peng, "Scheme for Implementing Teleporting an Arbitrary Tripartite Entangled State in Cavity QED," *Int. J. Theor. Phys.*, vol. 48, pp. 2786–2792, 2009.
- [17] X. M. Xiu, L. Dong, Y. J. Gao, and F. Chi, "Controlled deterministic secure quantum communication using five-qubit entangled states and two-step security test," *Opt. Commun.*, vol. 282, pp. 333–337, 2009.
- [18] Y. Nie, Y. Li, and Z. Wang, "Semi-quantum information splitting using GHZ-type states," *Quantum Inf. Process.*, vol. 12, pp. 437–448, 2013.
- [19] M. Sreeraman and P. K. Prasanta, "Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state," *Phys. Rev. A*, vol. 77, 032321, 2008.
- [20] S. Kaoru, T. Kiyoshi, and F. Hiroyuki, "Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair," *Phys. Rev. A*, vol. 80, 022323, 2009.
- [21] F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, "Comment on 'Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection,'" *Phys. Rev. Lett.*, vol. 101, 208901, 2008.
- [22] Y. S. Zhang, C. F. Li, and G. C. Guo, "Comment on 'Quantum key distribution without alternative measurements,'" *Phys. Rev. A*, vol. 63, 036301, 2001.
- [23] F. Gao, Q. Wen, and F. Zhu, "Teleportation attack on the QSDC protocol with a random basis and order," *Chin. Phys. B*, vol. 17, no. 9, 3189, 2008.
- [24] S. Qin, F. Gao, Q. Wen, and F. Zhu, "Improving the security of multiparty quantum secret sharing against an attack with a fake signal," *Phys. Lett. A*, vol. 357, pp. 101–103, 2006.
- [25] A. Wojcik, "Eavesdropping on the 'Ping-Pong' Quantum Communication Protocol," *Phys. Rev. Lett.*, vol. 90, 157901, 2003.
- [26] Q. Y. Cai, "The 'ping-pong' protocol can be attacked without eavesdropping," *Phys. Rev. Lett.*, vol. 91, 109801, 2003.
- [27] F. Gao, F. Z. Guo, Q. Y. Wen and F. C. Zhu, "Consistency of shared reference frames should be reexamined," *Phys. Rev. A*, vol. 77, 014302, 2008.
- [28] F. Gao, S. Qin, Q. Wen, and F. Zhu, "Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state," *Opt. Commun.*, vol. 283, no. 1, pp. 192–195, Jan. 2010.
- [29] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, *Phys. Rev. A* 73, 022320 (2006).
- [30] F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, "Improving the security of multiparty quantum secret sharing against Trojan horse attack," *Phys. Rev. A*, vol. 72, 044302, 2005.
- [31] M. Curty, D. J. Santos, E. Perez, and P. Garcia-Fernandez, "Qubit authentication," *Phys. Rev. A*, vol. 66, 022301, 2002.
- [32] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Phys. Rev. A*, vol. 65, 042312, 2002.
- [33] G. Zeng, "Reply to 'Comment on 'Arbitrated quantum-signature scheme,'" *Phys. Rev. A*, vol. 78, 016301, 2008.
- [34] Q. Li, W. H. Chan and D. Y. Long, "Arbitrated quantum signature scheme using Bell states," *Phys. Rev. A*, vol. 79, 054307, 2009.
- [35] X. Zou and D. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes," *Phys. Rev. A*, vol. 82, 042325, 2010.
- [36] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, "Cryptanalysis of the arbitrated quantum signature protocols," *Phys. Rev. A*, vol. 84, 022344, 2011.

Manuscript received: August 6, 2013

Biographies

Yunkai Deng received his BS degree from Central South University, China, in 2004. He began working toward his MSc degree at Central South University in 2012. His research interests include quantum information processing, mobile communications, and high-speed communication networks.

Zhujun Gao received his BS degree from Qufu Normal University, China, in 2004. He began working toward his MSc degree at Central South University in 2013. His research interests include technology education, modern mobile communications, and high-speed communication networks.

Ying Guo (yingguo@csu.edu.cn) received his MS degree from Kunming University of Science and Technology, China, in 2003. He received his PhD degree from Shanghai Jiaotong University in 2006. His research interests include quantum information processing and communications, wireless communication. He is now a professor at Central South University, China.

A Coding and Automatic Error-Correction Circuit Based on the Five-Particle Entangled State

Xi Chen, Pei Zhang, and Xiaoqing Zhou

(College of Physics and Mechatronics Engineering, Jishou University, Jishou 416000, China)

Abstract

In this paper, we discuss the concepts of quantum coding and error correction for a five-particle entangled state. Error correction can correct bit-reverse or phase-flip errors of one and two quantum states and is no longer limited to only one quantum state. We encode a single quantum state into a five-particle entangled state before being transferred to the sender. We designed an automatic error-correction circuit to correct errors caused by noise. We also simplify the design process for a multiple quantum error-correction circuit. We compare error-correction schemes for five and three entangled particles in terms of efficiency and capabilities. The results show that error-correction efficiency and fidelity are improved.

Keywords

quantum communication; channel coding; five-particle entangled state; fidelity

1 Introduction

Quantum information transmitted from sender to receiver is affected by the environment and decays exponentially over time [1]. De-coherence is associated with the development of quantum theory and has had a negative impact on quantum theory [2]–[5]. To reduce and correct errors caused by noise interference in a channel, channel coding has been introduced on the sender side. A single quantum state can be encoded into a five-particle entangled state before transmission, and corrections can be made automatically during transmission. With a decoder at the receiver, a quantum state with no more than two error conditions can be corrected. This eases retransmission pressure in the information channel. The best way to reduce the probability of errors in quantum coding is to introduce quantum channel coding error correction [3]. In 1995, the Shore coding scheme was designed. In 1996, Stenae, Calderbank and Shor created CSS code [6]–[9]. The same year, Bennett et al. proposed quantum error-correcting codes [10], [11]. Gottesman and Calderbank proposed the stabilizer system [6], [7], [12], [13] and constructed quantum Hamming-bound saturated quantum error-correction codes [14]–[16]. With these codes, the error of one quantum state can be corrected using three quantum state or five quantum state coding [6], [7], [14]. In 2010, Lv Hongjun proposed a 3, 5, 7 quantum error-correction circuit that made quantum network communication be-

tween sites possible [2]. Recently, Zhou Nanrun et al. proposed a quantum synchronous communication protocol [15]–[17]. Zhou Xiaoqing et al. have also proposed a model of a token-ring quantum transmission network using three-particle entangled state [18]. They also calculated the fidelity of this model [19]. In [20], the interconnection and routing strategy of point quantum teleportation network was described. To minimize transmission errors caused by environmental factors, a five-particle entangled quantum state encoding and error-correction circuit was designed. This circuit can correct an error of up to two quantum states. It was no longer confined to the situation of one quantum error. A more simplified error-correction circuit was designed.

2 Channel Coding

In a classical channel, noise affects transmission. Flip errors sometimes occur in the received bit. The sent bit may be 1, but the received bit is 0. In the transmission of quantum information, errors are easily caused by noise and quantum incoherence. Quantum information errors may be more complicated than those that affect classic information. There are three categories of error that affect quantum information: reverse turn, phase reversal, and reverse turn with phase [5]. As in classical information science, quantum information science also uses channel coding. By structuring the state of information that repeats itself and increasing redundancy, the system can auto-

A Coding and Automatic Error-Correction Circuit based on the Five-Particle Entangled State

Xi Chen, Pei Zhang, and Xiaoqing Zhou

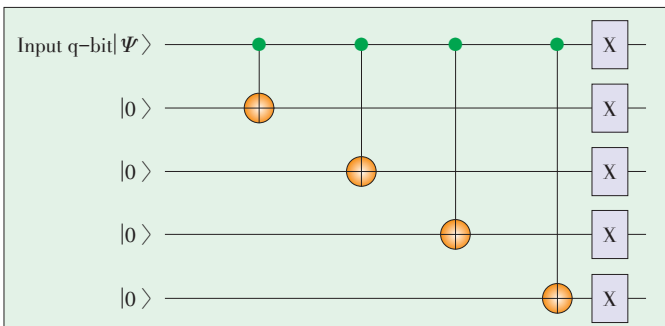
atically correct errors and ensure that information is correct [1]. We assume that the input qubit signal of an information channel is $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and that classical bit coding is used to reduce the error rate as much as possible. More than 1 bit is encoded to transfer the information. Quantum information can be transmitted by an encoder, and quantum states are $|\Psi\rangle = \alpha|00000\rangle + \beta|11111\rangle$, that is, code one qubit with five qubits. This also creates the possibility for quantum correction (Fig. 1).

2.1 Five-Particle Bit-Reversal Error Correction

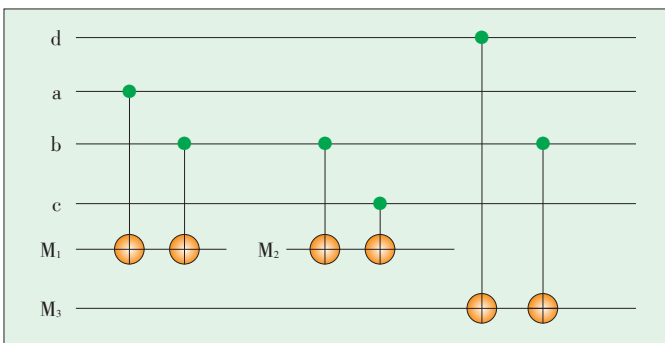
According to the basic principles of quantum mechanics, measurement leads to the collapse of the quantum state, and information carried by quantum state is lost [17]. Therefore, it is important to find a corrective measure without quantum bit flip. Here, we only consider an error of no more than two bits, and the error coding state can be corrected without the need for measuring by introducing redundant qubits [20]. Collapse of the quantum state due to measurement is avoided. To reduce the quantum auxiliary bits and quantum logic gates, we use three quantum bit error-correction method [2] to design a five-particle entangled state bit inversion error-correction circuit. Fig. 2 shows the error situation of a, b, c, and d.

For example, M_1 is 0; M_2 is 1; and M_3 is a, b are both incorrect. The variety of error conditions is shown in Table 1.

No more than two qubit error conditions are corrected, and these error conditions determine the quantum bit inversion operation. Then, the five entangled particle error-correction circuit is used.



▲ Figure 1. Five-particle encoder.



▲ Figure 2. Measuring the error condition of a, b, c.

▼ Table 1. Inversion error rule of a, b, c

M_1	M_2	M_3	Result
0	0	0	no inversion error
0	0	1	d error
0	1	0	c error
0	1	1	a, b error
1	0	0	a error
1	0	1	b, c error
1	1	0	a, c error
1	1	1	b error

From Fig. 2, the error conditions of qubit a, b, c can be corrected, then we anticipate that the qubits of a, b, c are correct. Therefore, these qubits can help correct d and e to concert and assist the qubit. In this way, no more than two quantum bits are error-corrected. The five entangled particle bit-reversal error-correction circuit is shown in Fig. 3.

Because of environmental factors, the quantum state and auxiliary bit quantum state of the sender has changed from 00000 000000 to 10010 000000.

Before position 1, a, b and c are control bits that control the NOT operation, the auxiliary bit δ , is $|0\rangle$; the auxiliary bit β is $|1\rangle$; and the output is 10010 010000.

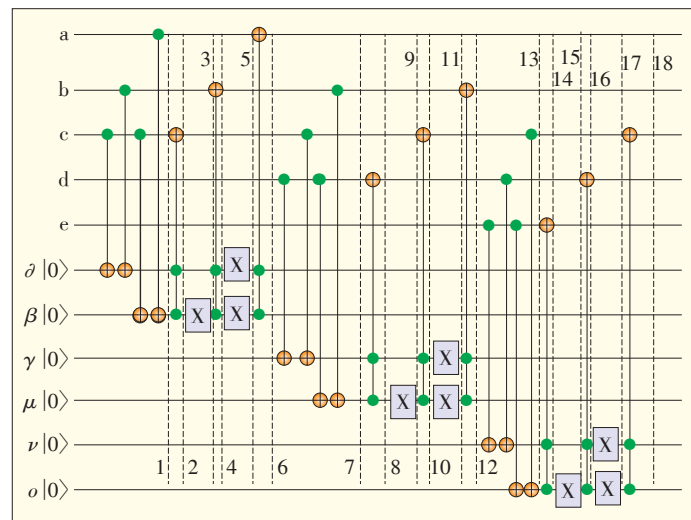
Before position 2, the auxiliary bits δ , β are control bits; c is the target bit that operates the Toffoli gate and remains unchanged; and the output is 10010 010000.

Before position 3, the target bit is β and operates the NAND gate; β is $|0\rangle$; and the output is 10010 000000.

Before position 4, the auxiliary bits δ , β are control bits; b is the target bit that operates the Toffoli gate and remains unchanged; and the output is 10010 000000.

Before position 5, the target bits are δ , β and operate the NAND gate; δ is $|1\rangle$; β is $|1\rangle$; and the output is 10010 110000.

Before position 6, the auxiliary bits δ , β are control bits; a is the target bit that operates the Toffoli gate; a is $|0\rangle$ by rever-



▲ Figure 3. Five particle bit-reversal error-correction circuit.

sion; and the output is 00010 110000.

Before position 7, b , c and d are control bits that control the NOT operation; the auxiliary bit γ is $|0\rangle$; the auxiliary bit μ is $|1\rangle$; and the output is 00010 111100.

Before position 8, the auxiliary bits γ and μ are control bits; d is the target bit that operates the Toffoli gate; d is $|0\rangle$ by reversion; and the output is 00000 111100.

Before position 9, the target bit is μ and operates the NAND gate; μ is $|0\rangle$; and the output is 00000 111000.

Before position 10, the auxiliary bits γ and μ are control bits; c is the target bit that operates the Toffoli gate and remains unchanged; and the output is 00000 111000.

Before position 11, the target bits γ and μ operate the NAND gate; γ is $|0\rangle$; μ is $|1\rangle$; and the output is 00000 110100.

Before position 12, the auxiliary bits γ and μ are the control bits; b is the target bit that operates the Toffoli gate and remains unchanged; and the output is 00000 110100.

Before position 13, c , d and e are control bits that control the NOT operation; the auxiliary bit ν is $|0\rangle$; and the output is 00000 110100.

Before position 14, the auxiliary bits ν and o are control bits; e is the target bit that operates the Toffoli gate, and the output is 00000 110100.

Before position 15, the target bit o operates the NAND gate; o is $|1\rangle$; and the output is 00000 110101.

Before position 16, the auxiliary bits ν and o are control bits; d is the target bit that operates the Toffoli gate and remains unchanged; and the output is 00000 110101.

Before position 17, the target bits ν and o operate the NAND gate; ν is $|1\rangle$; o is $|0\rangle$; and the output is 00000 110110.

Before position 18, the auxiliary bits ν and o are control bits; c is the target bit that operates the Toffoli gate and remains unchanged; and the output is 00000 110110.

Error-correction results are shown in **Table 2**.

The five quantum entanglement error-correction code can correct errors of no more than two qubits without completely destroying the encoded state. In the received $|abcde\rangle$, a represents 0 or 1. We measure the number of 1 in a , b , c , d , e and decode $|abcde\rangle$ into $|00000\rangle$. In contrast, $|abcde\rangle$ is decoded to $|11111\rangle$. This means that $|D$ determines the means of decoding [18]:

$$D\{|00000\rangle |00001\rangle |00010\rangle |00100\rangle |01000\rangle |10000\rangle |11000\rangle |10100\rangle |10010\rangle |10001\rangle |01100\rangle |01010\rangle |01001\rangle |00110\rangle |00101\rangle |00011\rangle\} = |00000\rangle$$

$$D\{|11111\rangle |11110\rangle |11101\rangle |11011\rangle |10111\rangle |01111\rangle |00111\rangle |01011\rangle |01101\rangle |01110\rangle |10011\rangle |10101\rangle |10110\rangle |11001\rangle |11010\rangle |11100\rangle\} = |11111\rangle$$

2.2 Five Particle Phase-Flip Error Correction

Assuming $|00000\rangle + |11111\rangle$ flips through channels

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ the received information is } |00000\rangle - |11111\rangle$$

because of the phase reversal of the first qubit. In this case,

▼ **Table 2.** A variety of input and output

Input	Output
00000 000000	00000 101010
00001 000000	00000 101001
00010 000000	00000 100110
00100 000000	00000 011010
01000 000000	00000 001010
10000 000000	00000 111010
11000 000000	none
10100 000000	none
10010 000000	00000 110110
10001 000000	00000 111001
01100 000000	none
01010 000000	00000 000110
01001 000000	00000 001001
00110 000000	00000 010110
00101 000000	00000 011001
00011 000000	00000 100101
11111 000000	11111 101010
11101 000000	11111 101001
11110 000000	11111 100110
11011 000000	11111 011010
10111 000000	11111 001010
01111 000000	11111 111010
00111 000000	none
01011 000000	none
01101 000000	11111 110110
01110 000000	11111 111001
10011 000000	none
10101 000000	11111 000110
10110 000000	11111 100101
11001 000000	11111 010110
11010 000000	11111 011001
11100 000000	11111 001001

the previous method cannot be used for correction. Thus, we use the phase-inverted channel error-correction method. The Hadamard transform is given by [1]

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (1)$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2)$$

$$H^2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (3)$$

$$HZH = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X \quad (4)$$

We define:

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (5)$$

$$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad (6)$$

A Coding and Automatic Error-Correction Circuit based on the Five-Particle Entangled State

Xi Chen, Pei Zhang, and Xiaoqing Zhou

Let $|+\rangle$ flip through channels which has a phase flip

$$Z|+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |-\rangle \quad (7)$$

$$Z|-\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = |+\rangle \quad (8)$$

For example, $\alpha|0\rangle + \beta|1\rangle$ turns into $\alpha|+\rangle + \beta|-\rangle$ after a Hadamard transform, and the occur phase flip is equal to the operation of $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ with the result $\alpha|-\rangle + \beta|+\rangle$. The error of the phase flip was converted into bit-flip errors **Fig. 4**.

The result of phase flip $|+\rangle$ and $|-\rangle$ is similar to the preceding phase-flip error. This provides the basis for correcting the phase flip. We only need to flip through the phase error of the H gate logic circuit, which can be converted into bit-flip errors for processing. The phase-inversion error-correction circuit in **Fig. 5** can be used to correct the reversal error. A phase reversal is turned into a phase inversion. The results can be referred to the inversion error correction. Phase inversion error is shown in Fig. 5.

3 Efficiency of Five Particle Error Correction

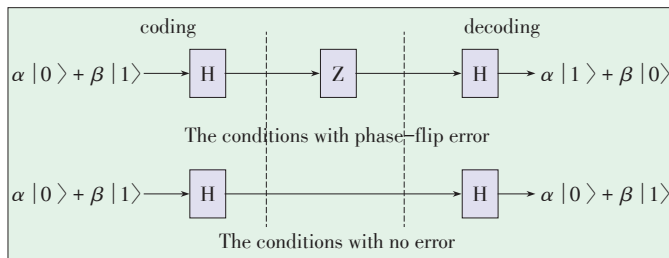
We assume that the qubit is $|\varphi\rangle$, the decoded qubit is $|\varphi'\rangle$, and fidelity is

$$F = E|\langle\varphi'|\varphi\rangle|^2 \quad (9)$$

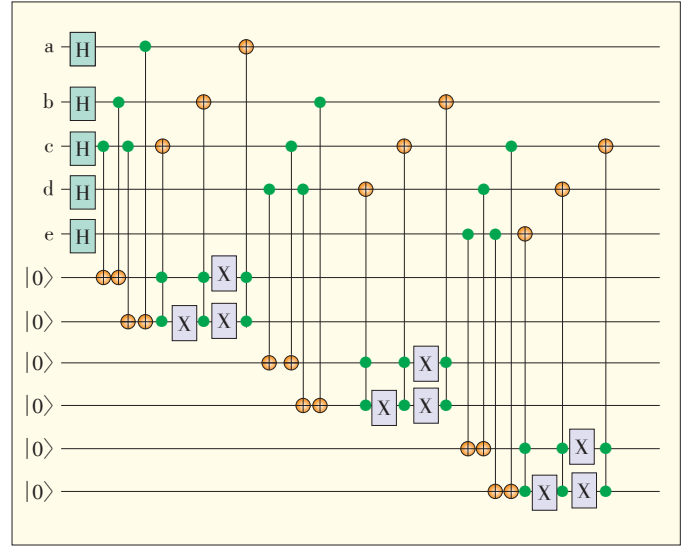
After using 3 quantum states $|000\rangle + |111\rangle$ to encode, the probability of the decoding results is $\alpha|0\rangle + \beta|1\rangle$, which is equal to the probability of a qubit inversion, i.e. $(1-p)^3 + 3p(1-p)^2$. The probability of a decoding error is equal to the probability of more than 2 qubit reversal, i.e. $3p^2(1-p) + p^3$. The fidelity F is given by

$$\begin{aligned} F &= [(1-p)^3 + 3p(1-p)^2] |(\alpha\langle 0| + \beta\langle 1|)(\alpha|0\rangle + \beta|1\rangle)|^2 \\ &\quad + [3p^2(1-p) + p^3] |(\alpha\langle 1| + \beta\langle 0|)(\alpha|0\rangle + \beta|1\rangle)|^2 \quad (10) \\ &= [(1-p)^3 + 3p(1-p)^2] (|\alpha|^2 + |\beta|^2)^2 + [3p^2(1-p) + p^3] (\alpha^*\beta + \beta^*\alpha)^2 \end{aligned}$$

We obtain $\min F_3 \geq [(1-p)^3 + 3p(1-p)^2] = 1 - 3p^2 + 2p^3$ with the



▲ Figure 4. Schematic diagram of phase flip converted into bit-flip by H transform.



▲ Figure 5. Five particle phase-inversion error-correction circuit.

normalization condition $|\alpha|^2 + |\beta|^2 = 1$ and $(\alpha^*\beta + \beta^*\alpha)^2 \geq 0$.

Then, $F > 1-p$ because $0 < p < \frac{1}{2}$, i.e. the loyalty of the channel is increased. Similarly, an error rate of no more than two quantum states can be corrected after five entangled particle encoding. The loyalty F is given by $\min F_5 \geq (1-p)^5 + 5p(1-p)^4 + 10p^2(1-p)^3$. We can see that $\min F_5 \geq F_3$ by $0 < p < \frac{1}{2}$, and the phase-flip error can be corrected by turning into error. Therefore, its fidelity algorithm is also similar to the fidelity algorithms of a bit-flip.

In the process of quantum error correction, the error probability of a quantum bit is T/N , where T is the time of error correction and N is the number of error corrections. The larger N is, the smaller the interval and bit error rate is. The error probability of the remainder of the quantum bit is proportional to $T/2N$ after the first operation.

As a consequence of this, the error probability of quantum qubit is proportional to $N(T/2N)$ [1]. It illustrates that the error rate of system is reduced while the number of operation is larger. For example, If $p = 0.1$, the probability of the condition which there is no more than one qubit inversion error occurs in three qubits is

$$(1-p)^3 + 3p(1-p)^2 = 0.972 \quad (11)$$

The probability when there are no more than two qubit errors in a five entangled particles is

$$(1-p)^5 + 5p(1-p)^4 + 10p^2(1-p)^3 = 0.99144 \quad (12)$$

The comparison of error correction efficiency and fidelity between five and three quantum states can illustrate that the efficiency and fidelity have been improved while use five quantum

A Coding and Automatic Error-Correction Circuit based on the Five-Particle Entangled State

Xi Chen, Pei Zhang, and Xiaoqing Zhou

states encoding for transmitting information.

4 Conclusion

In this paper, we proposed an encoding and decoding scheme for channel transmission with five-particle entangled state. With this scheme, the quantum state is not collapsed by measurement, and errors of no more than two quantum bits are automatically corrected. In this paper, the quantum channel coding and error correction of five-particle entangled state was described. Error correction is no longer limited to only one quantum error. Using our scheme, errors can be corrected for two quantum states. We compared the transmission efficiency and error-correction capability of five qubits and three qubits in the channel. Transmission efficiency and fidelity of the channel were improved. To minimize the error rate, the transmission information must be encoded into more quantum states before transmission. This paper provides new ideas for designing and optimizing an error-correction circuit for multipartite quantum states.

References

- [1] H. W. Chen, *Quantum Information and Quantum Computation Simple Tutorial*. NanJing, China: Southeast University Press, 2006, pp. 86–94.
- [2] D. H. Tan, "The Research of Quantum Error Coding," M.S. thesis, Dept., Southwest Univ., Chongqing, China, 2007.
- [3] L. C. Cai, "Study of Quantum Error Correcting Code," *Journal of Sichuan University of Science & Engineering (Natural Science Edition)*, vol. 17, no. 3, pp. 163–168, Dec. 2004.
- [4] L. C. Cai, "The Construction of Quantum Error Correcting Codes," M.S. thesis, Dept. Quantum, The PLA Information Engineering Univ., Henan, China, 2010.
- [5] H. J. Lv, K. K. Du, D. Gao, and G. J. Xie, "Design and optimization of quantum error-correction circuit with module," *Chinese Journal of Quantum Electronics*, vol. 27, no. 6, pp. 700–704, Jun. 2010.
- [6] Z. Li, "Research on the Some Topics of Quantum Codes," Ph.D. dissertation, Dept. Quantum, Xian Univ. Xian, China, 2008.
- [7] L. J. Xing, "Study of quantum convolutional codes—Construction, encoding and decoding," Ph.D. dissertation, Dept. Quantum, Xian Univ. Xian, China, 2008.
- [8] A. M. Steane, "Multiple particles interference and quantum error correction," *Proc. R. Soc. (London) A*, vol. 452, no. 3, pp. 2551–2557, Nov. 1996.
- [9] A. R. Calderbank, and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.
- [10] R. Laflamme, C. Miguel, J. P. Paz, et al., "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, pp. 198–201, Jul. 1996.
- [11] C. H. Bennett, D. P. Divincenzo, J. A. Smolin, et al., "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, Nov. 1996.
- [12] D. Gottesman, "A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound," *Phys. Rev. A*, vol. 54, no. 5, pp. 1862–1862, Jul. 1996.
- [13] F. Y. Xiao and H. W. Chen, "Error correction and decoding for quantum stabilizer codes," *Acta Phys. Sin.*, vol. 60, no. 8, pp. 1–7, Dec. 2011.
- [14] L. J. Xing, Z. Li, B. M. Bai, and X. M. Wang, "Encoding and Decoding of CSS-Type Quantum Convolution Codes," *Journal of Beijing University of Posts and Telecommunications*, vol. 31, no. 6, pp. 121–124, Dec. 2008.
- [15] N. R. Zhou, G. H. Zeng, F. C. Zhu, et al., "The Quantum Synchronous Communication Protocol for Two-army Problem," *J. Shanghai Jiaotong University*, vol. 40, no. 11, pp. 1885–1889, Dec. 2006.
- [16] N. R. Zhou and G. H. Zeng, "Quantum communication protocol for data link layer based on entanglement," *Acta Physica Sinica*, vol. 56, no. 9, pp. 5066–5070, Sep. 2007.
- [17] N. R. Zhou, B. Y. Zeng, L. J. Wang, et al., "Selective automatic repeat quantum synchronous communication protocol based on quantum entanglement," *Acta Physica Sinica*, vol. 59, no. 4, pp. 2193–2199, Apr. 2010.
- [18] X. Q. Zhou and Y. W. Wu, "Discussion on building the net of quantum teleportation using three-particle entangled state," *Acta Physica Sinica*, vol. 56, no. 4, pp. 1881–1887, Apr. 2007.
- [19] Y. W. Wu and X. Q. Zhou, "Token-bus Network Fidelity of Quantum Teleportation by Three-photon Entangled State," *Acta Physica Sinica*, vol. 39, no. 11, pp. 2093–2096, Nov. 2010.
- [20] X. Q. Zhou, Y. W. Wu, and H. Zhao, "Quantum teleportation internetworking and routing strategy," *Acta Phys. Sin.*, vol. 60, no. 4, pp. 1–5, Jul. 2011.

Manuscript received: August 8, 2013

Biographies

Xi Chen (jidanjtlw@163.com) received his BSc degree in physics from Luoyang College, China, in 2010. He received his MSc degree in condensed matter physics from Jishou University, China, in 2013. His research interests include quantum error correction.

Pei Zhang (290047141@qq.com) graduated from the Faculty of Physics, Taiyuan University, China, in 2011. He is a postgraduate at Jishou University, China. His main research interest is quantum teleportation.

Xiaoqing Zhou (zhouxq_jd@163.com) is a professor at the College of Physics Science and Information Engineering, Jishou University, China. He previously studied at Hunan Education College, Tsinghua University, and Central South University. Dr. Zhou graduated from the Faculty of Physics, Jishou University, in 1981. He is a postgraduate tutor, and his main research interest is quantum information.

ZTE Launches the World's Largest Capacity Data Center Switches

24 September 2013, Shenzhen—ZTE today announced the release of the BigMatrix 9900 series of data center switches, the world's largest-capacity data center switches.

The BigMatrix 9900 product family comprises data switches with the largest capacity in the world. The switches are designed large cloud computing and big data scenarios and allow for higher-density deployment in data centers. Each single slot can support up to 144 10G ports, 36 40G ports, or 12 100G ports. The Big Matrix 9900 series comprises four switch models—9916, 9912, 9908, and 9904—each of which supports a maximum switching capacity of 84.48 Tbps.

In big data systems, BigMatrix 9900 allows non-structured and non-relevant data to be extracted from existing databases. BigMatrix 9900 also has a modular system design and can be used to build a super-resilient non-blocking bi-directional forwarding platform with a switching capacity of 1.4 Pbps (1440 Tbps) in Fat-Tree mode. (ZTE Corporation)

Optimal Rate for Constant-Fidelity Entanglement in Quantum Communication Networks

Youxun Cai, Xutao Yu, and Yang Cao

(State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, China)

Abstract

In this paper, we propose an entanglement scheme for long-distance, constant-fidelity communication in quantum networks. We discuss the optimal rate of entanglement that allows for constant fidelity in both elementary and multihop links. We also discuss time complexity and propose the mathematical order of the rate capacity for an entanglement scheme. We propose a recursive entanglement scheme, a simultaneous entanglement scheme, and an adjacent entanglement scheme mathematically analyze these schemes. The rate capacity of the recursive and simultaneous entanglement schemes is $\Omega(1/e^n)$, but the adjacent entanglement scheme performs better, providing a rate of $\Omega(1/n)$.

Keywords

rate capacity; constant fidelity; entanglement scheme; ad hoc quantum networks

1 Introduction

Quantum processing and communication networks combine the disciplines of quantum mechanics and classical information science. However, quantum networks are more secure and efficient than classical networks [1]–[3]. Quantum communication networks are based on quantum teleportation, which is essential for transmitting quantum states and establishing quantum channels between nodes at a distance [2]. Quantum teleportation exploits one of the most intriguing properties of quantum mechanics: entanglement. In quantum entanglement, Einstein, Podolsky, Rosen (EPR) pairs are generated and then distributed via fibers or optical free-space links. This allows different nodes to transport a quantum state by transmitting classical bits rather than quantum bits [2].

At present, photons are primarily used as the carrier in quantum entanglement generation. They are used over distances of some hundreds of kilometers (e.g. 250 km on fiber links and 144 km on free space) [3]. However, the success of entanglement decreases exponentially with distance because of absorption loss and detector noise in the transmission channel.

A solution to entanglement delay is to insert quantum repeaters between different nodes [5], [6]. Quantum repeaters can store quantum states and use protocols to perform quantum operations. A repeater protocol defines a sequence of three operations: entanglement generation on elementary links, entanglement swapping, and entanglement purification [7]. The proto-

col should be well designed to maximize success at each link.

Entangled photons are used to express quantum states as EPR pairs. With the development of quantum networks, quantum optics has attracted more research interests recently. Fidelity is one of the most important topics in this field and is defined as the probability that a decoded message has the same amount of information after coding and transmission as it did before coding and transmission. High fidelity is essential in long-distance communication to make messages reliable. In long-distance entanglement generation, fidelity can be affected by memory decay, local measurement errors, entanglement swapping, or entanglement purification failure [7]. The upper bound of the entanglement generation rate between nodes connected by quantum repeaters is determined by these factors.

The quantum entanglement rate of each elementary link can be calculated and measured for specific quantum ad hoc networks. In a multihop network, optimized quantum repeater protocols increase the rate of quantum entanglement to reach the upper bound.

There are two main approaches to optimizing quantum repeater protocols: developing a new quantum repeater structure (using quantum mechanics), and adapting classical network concepts to the quantum network. In [8], the former approach is taken. A Duan, Lukin, Cirac, Zoller (DLCZ) protocol generates and connects entangled pairs of atomic ensembles over short distances. The protocol couples a single photon with collective atomic excitation modes. In [9], Qubus (hybrid) repeaters are described. These repeaters perform operations on both

local qubits and continuous-variable states (qubus). In [6], EPR generation rate in ad hoc quantum networks is investigated. Several heuristic algorithms are also introduced to ensure constant, maximum fidelity. These algorithms include Entanglement Swapping Scheme Search, and Shortest Path Entanglement Flow. Novel quantum broadcasting schemes, such as ring, angular, and regional broadcasting, are defined in a quantum repeater architecture and are extensions of classical broadcasting concepts [6]. Nevertheless, only recursive entanglement is applied in the quantum repeater protocols, and the entanglement rate when the number of nodes tends to infinity has not yet been determined.

In this paper, we focus on the rate capacity of entanglement that ensures constant fidelity when the number of nodes in a multihop link tends towards infinity. We use concepts from classical ad hoc networks to optimize the rate in a quantum repeater with a typical structure [7]. We propose three entanglement schemes for quantum repeater protocols. These schemes are recursive entanglement, simultaneous entanglement, and adjacent entanglement. Through mathematical analysis, we show that recursive entanglement and simultaneous entanglement provide a rate on the order of $1/e^n$. However, adjacent entanglement provides a rate on the order of $1/n$, which indicates better performance.

In section 2, we provide background on the entanglement rate capacity for an elementary link. In section 3, we describe the entanglement rate capacity model of EPR pairs for a multihop link. In section 4, we propose three entanglement schemes that ensure constant fidelity to establish multi-hop links are defined, the mathematical derivation of the rate capacity for each scheme is presented, and their performances are analyzed.

2 Entanglement Rate Capacity Model for an Elementary link

For elementary link, the average time τ_{ij} to generate an EPR pair is given as the sum of the detection time $1/fP_g$ and communication time d_{ij}/c :

$$\tau_{ij}(f, d, P_g) = (1/fP_g) + (d_{ij}/c) \quad (1)$$

where d_{ij} is the Euclidian distance between two consecutive nodes i and j ; f is the operating frequency in the quantum repeater; P_g is the probability of realizing an EPR pair; and c is the speed of light. For the quantum repeater in [7], P_g is

$$P_g(F) = 0.5 \left[1 - (2F - 1)^{\frac{2\eta}{1-\eta}} \right] \quad (2)$$

where F is the fidelity of the EPR pair between nodes, and η is the loss parameter, given by $e^{-\xi d}$, where d is the distance and ξ is the rate of loss. The operating frequency depends on the quantum memory space M and link distance d [7]:

$$M = 4 \lceil df/c \rceil \quad (3)$$

Therefore, the maximum operating frequency is [7]

$$f_{\max} = Mc/4d \quad (4)$$

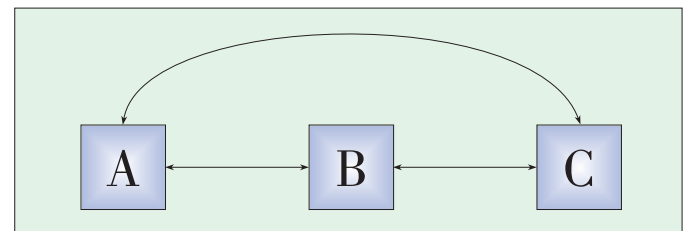
Communication time is much shorter than detection time, i. e. $(d/c) \ll (1/(fP_g))$. Therefore, the average EPR generation time is approximately equal to the detection time. A elementary link's capacity for generating EPR pairs can be defined as the reciprocal of the maximum average time to generate an EPR pair, and is given by

$$R(F) \equiv f_{\max} P_g(F) \quad (5)$$

3 Entanglement Rate Capacity Model for a Multihop Link

In practice, it is very difficult to transmit entangled photons over long distances because of channel loss and detector noise. It is reasonable to assume that entangled photons generated by a locate node can only be delivered to the consecutive node in a multihop link. A relay scheme is therefore used to ensure that any nodes over a long distance can share EPR pairs. Suppose Alice, Bob and Candy are three consecutive nodes in multihop link. Alice can transmit entangled photons directly to Bob but not to Candy. First, photons are entangled so that Alice can share the them with Bob through elementary link (A, B). At the same time, Bob shares entangled photos with Candy through elementary link (B,C). As a result, Bob has a photon from the EPR pair with Alice. He also has a photon from the EPR pair with Candy. Second, we perform entanglement connection on the two photons that Bob has. This involves consecutively swapping and purifying the entanglements. Third, we inform Alice and Candy about the classic information produced by the quantum operation. Alice and Candy use this information to operate the other entangled photons left in the quantum memory. Hence, by consuming two EPR pairs, we obtain an EPR pair between Alice and Candy, both of whom are unable to directly transmit photons. Using this relay scheme, more nodes can be added in multihop scenario, and fidelity can be constant for a remote node if entanglement swapping and purification are balanced.

In the case of three nodes (**Fig. 1**), we assume that entanglement occurs in the two elementary links at the same time. The average time for this process to occur has a lower bound of $\max \left\{ \frac{1}{f_{AB}P_{g,AB}(F)}, \frac{1}{f_{BC}P_{g,BC}(F)} \right\}$. The probability of entanglement



▲ Figure 1. Entanglement for three nodes.

Optimal Rate for Constant-Fidelity Entanglement in Quantum Communication Networks

Youxun Cai, Xutao Yu, and Yang Cao

connection is determined by the physical structure of the quantum repeater and is denoted P_c . The minimum average time τ_{AC} to obtain an EPR pair between Alice and Candy can be expressed as:

$$\tau_{AC} = \max \left\{ \frac{1}{f_{AB} P_{g, AB}(F)}, \frac{1}{f_{BC} P_{g, BC}(F)} \right\} \frac{1}{P_c} \quad (6)$$

Moreover, the maximum average rate $R(A, C)$ can be expressed as

$$R(A, C) = 1/\tau_{AC} \\ = \min\{R(A, B), R(B, C)\} P_c \quad (7)$$

For n consecutive hops, entanglement connection can be done on the k th repeater, and

$$R(0, N) = \min\{R(0, k), R(k, N)\} P_c \quad (8)$$

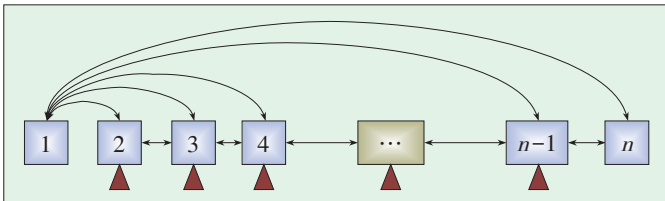
4 Three Entanglement Schemes for Establishing Multihop Links

To create an EPR pair between the source node and destination node, intermediate nodes are essential because they generate EPR pairs and follow swapping steps to transmit an entanglement. Take, for example, a finite multihop link with n nodes. If we know the exact entanglement rate between each pair of consecutive nodes, we can choose the appropriate sequence scheme for entanglement on a node. In this way, the rate of entanglement can be optimized. In this paper, we are mainly concerned with the upper bound on the rate capacity with high probability (w.h.p); i.e. with probability tending to 1 as n approaches infinity. In the following, we use a probabilistic variation to denote the mathematical order. As n approaches infinity, $f(n) = \Omega(g(n))$ w.h.p. as n approaches infinity. If there is a constant K , then $\lim_{n \rightarrow \infty} P(f(n) \geq Kg(n)) = 1$.

4.1 Recursive Entanglement Scheme

Recursive entanglement is an immediate scheme in which only one intermediate node is chosen for entanglement connection at every turn. This process is repeated recursively so that an EPR can be established between the source node and destination node in a multihop scenario. The start node can be selected arbitrarily, and entanglement connection should be done at recursively before or after the node.

If the source node is chosen as the start node, the process for an $n-1$ hop path in the ad hoc quantum network is as in **Fig. 2**. The arrows in Fig. 2 indicate EPR pairs between nodes,



▲ **Figure 2.** Recursive entanglement when the source node is the start node.

and the triangles below the nodes indicate entanglement connections. The recursive scheme involves $n-1$ steps:

- 1) Each node generates entanglements and shares an EPR pair with the adjacent nodes (Fig. 1). Node 1 shares an EPR pair with node 2, and node 2 shares an EPR pair with node 3. Node $n-1$ shares an EPR pair with node n .
- 2) Entanglement connection is done in node 2, and then node 2 sends the classical information to node 3 so that node 1 can share an EPR pair with node 3.
- 3) Entanglement connection is done in node 3, and then node 3 sends the classical information to node 4 so that node 1 can share an EPR pair with node 4.
- ...
- $n-1$) Entanglement connection is done in node $n-1$, and then node $n-1$ sends the classical information to node n so that node 1 can share an EPR pair with node n .

The time taken to send classical information is negligible. Therefore, by applying (8) recursively, we can conclude that

$$R(1, n) = \min\{\min\{\min\{R(1, 2), R(2, 3)\} P_c, R(3, 4)\} P_c, R(4, 5)\} P_c \dots \\ = \min\{R(1, 2) P_c^{n-2}, R(2, 3)\} P_c^{n-3}, R(3, 4) P_c^{n-4}, \dots, R(n-1, n)\} P_c \quad (9)$$

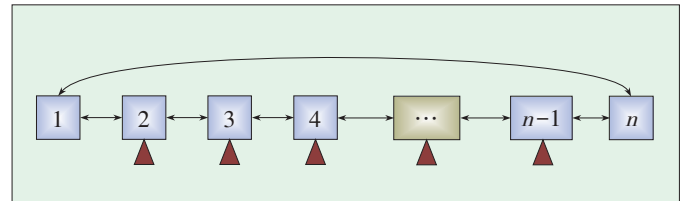
It is not necessary to choose node 1 as the starting node for the whole process if we know the exact entanglement generation rate of each elementary link. Then, we can use heuristic algorithms to determine which node to use as the start node and how to recursively do execute the process. In this way, the maximum value of $R(1, n)$ can be obtained. However, here we mainly focus on the mathematical order of $R(1, n)$. Considering there are always $n-1$ steps, we let $R(k\text{th})$ be the rate of the elementary link between the k th node and the next node at which entanglement is done. Then, we conclude that

$$R(1, n) = \min\{R(1\text{st}) P_c, R(2\text{nd}) P_c^2, R(3\text{rd}) P_c^3, \dots, R((n-1)\text{th}) P_c^{n-2}\} \\ = r/a^{n-2} \quad (10) \\ = \Omega(1/e^n) \text{ w.h.p. as } n \text{ approaches infinity}$$

where r is a constant, and $a = 1/P_c$. The recursive entanglement scheme only provides a rate on the order of $1/e^n$.

4.2 Simultaneous Entanglement Scheme

Simultaneous entanglement was first described in [5]. A quantum routing mechanism was proposed to construct the quantum communication network. Here, we describe the mathematical order of the simultaneous entanglement swapping scheme (**Fig. 3**). This scheme allows entanglement connection in parallel (rather than recursively) at the intermediate nodes.



▲ **Figure 3.** Simultaneous entanglement.

All the classical information is collected and applied to a specially designed quantum logical circuit in the destination node. Then, the source and destination are entangled. This scheme involves three steps:

- 1) Each node generates entanglements and shares an EPR pair with the adjacent nodes (Fig. 2). Node 1 shares an EPR pair with node 2, and node 2 shares an EPR pair with node 3. Node $n-1$ shares an EPR pair with node n .
- 2) Entanglement connection is done in parallel at all the intermediate nodes.
- 3) All the intermediate nodes send the classical information to node n . This information is received and processed at node n with a special quantum logical circuit. Node n then shares an EPR pair with node 1.

The time needed to send classical information is negligible, and all the $n-2$ entanglement connections should occur successfully at the same time. By applying (8) simultaneously, we conclude that

$$\begin{aligned} R(1, n) &= \min\{R(1, 2), R(2, 3), R(3, 4), \dots, R(n-1, n)\} P_c^{n-2} \\ &= r/a^{n-2} \\ &= \Omega(1/e^n) \text{ w.h.p. as } n \text{ approaches infinity} \end{aligned} \quad (11)$$

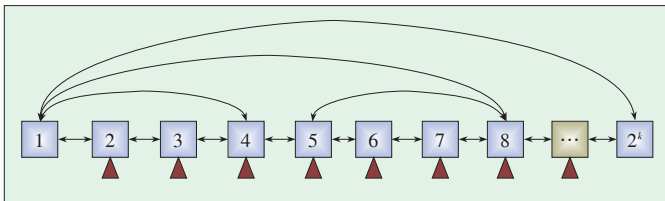
The simultaneous entanglement scheme only provides a rate on the order of $1/e^n$.

4.3 Adjacent Entanglement Scheme

In both the recursive and simultaneous entanglement schemes, the whole entanglement progress is a sequential chain of successful entanglement connections of each intermediate node. Therefore for an $n-1$ hop link the total probability is always presented as a constant multiplied by an $n-2$ power of P_c . To decrease the mathematical order of the entanglement rate, we propose using the adjacent entanglement scheme. The main idea of adjacent entanglement is to divide the multihop link into sets that contain adjacent nodes. This ensures that entanglement connection is done independent to that of other sets. After nodes in each set have performed entanglement connection, cluster sets are formed by small sets and continue with entanglement connection independently. Because entanglement connection occurs independent of other sets, the total probability is multiplied by P_c only once at every turn, and the order decreases. We describe a concise scenario in which there are only 2^k nodes in a multihop link (Fig. 4).

The adjacent entanglement scheme involves $2(\log_2 2^{k-1})$ steps:

- 1) Each node generates entanglements and shares an EPR pair



▲ Figure 4. Adjacent entanglement scheme for an a node link.

with adjacent nodes (Fig. 4) Node 1 shares an EPR pair with node 2, and node 2 shares an EPR pair with node 3. Node $n-1$ shares an EPR pair with node n .

- 2) The link is divided into 2^{k-2} sets. Set 1 contains nodes 1 to 4, set 2 contains nodes 5 to 8 etc. Set i contains nodes $4i-3$ to $4i$, where i is an integer. Set 2^{k-2} contains nodes 2^k-3 to 2^k .
- 3) Entanglement connection is done at nodes 2, 3, 6, 7, ..., $4i-2$, $4i-1$ at the same time. These connections are independent. By the end of step 3, node 1 is entangled with node 4, node 5 is entangled with node 8 etc. Node $4i-3$ is entangled with node $4i$ etc.
- 4) Entanglement connection is done at nodes 4 and 5 so that node 1 is entangled with node 8 etc. Entanglement connection is done at nodes $8i-4$ and $8i-3$ etc.
- 5) Entanglement connection is done at nodes 8 and 9 so that node 1 is entangled with node 16 etc. Entanglement connection is done at nodes $16i-8$ and $16i-7$ etc.
- 6) Entanglement connection is done at nodes 16 and 17 so that node 1 is entangled with node 32 etc. Entanglement connection is done at node $32i-16$ and $32i-15$ etc.

...
 $2(\log_2 2^k - 1)$. Entanglement connection is done at node 2^{k-1} and $2^{k-1}+1$ so that node 1 is entangled with node 2^k .

The time needed to send classical information is negligible, and each set is independent. Each time entanglement connection is done, P_c is only multiplied once because of this independence. Therefore, for a link with 2^k hops, the total probability is a constant multiplied by a $2(\log_2 2^k - 1)$ power of P_c .

In a simple 8-node scenario,

$$R(1, 8) = \min\{\min[R(1, 2), R(2, 3), R(3, 4)] P_c^2, R(4, 5), \min[R(5, 6), R(6, 7), R(7, 8)] P_c^2\} P_c^2 \quad (12)$$

Therefore for an 8-hop link, the total probability is a constant multiplied by a $2(\log_2 8 - 1)$ power of successful connection probability P_c . For $n \rightarrow \infty$, the integer $k = \lceil \log_2 n \rceil$ makes $n \leq 2^k$, and

$$\begin{aligned} R(1, n) &\leq R(1, 2^k) \\ R(1, 2^k) &= \Omega\left(\frac{r}{a^{2(\log_2 2^k - 1)}}\right) \\ &= \Omega(1/a^k) \\ &\leq \Omega(1/n) \end{aligned} \quad (13)$$

Therefore, the adjacent entanglement scheme can only provide a rate on the order of $1/n$.

5 Conclusion

In this paper, we have discussed the optimal rate of entanglement that can be achieved while still maintaining constant fidelity in a quantum communication network. Our discussion focused on a network in which the number of nodes in a multihop link approaches infinity. We proposed a recursive entan-

Optimal Rate for Constant-Fidelity Entanglement in Quantum Communication Networks

Youxun Cai, Xutao Yu, and Yang Cao

glement scheme, a simultaneous entanglement scheme, and an adjacent entanglement scheme. These ensure constant fidelity when establishing multihop links. However, mathematical analysis shows that the recursive and simultaneous entanglement schemes only provide a rate on the order of $1/e^n$ whereas the adjacent entanglement scheme performs better, providing a rate on the order of $1/n$.

References

- [1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum Entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, 2009.
- [2] Malaney and A. Robert, "Location-dependent communications using quantum entanglement," *Phys. Rev. A*, vol. 81, no. 4, pp. 042319, 2010.
- [3] K. Inoue, "Quantum key distribution technologies," *IEEE Journal of Quantum Electronics*, vol. 12, no. 4, pp. 888–896, July–Aug 2006.
- [4] D. Stucki, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.*, vol. 11, 2009.
- [5] S. T. Cheng, C. Y. Wang, and M. H. Tao, "Quantum communication for wireless wide-area networks," *IEEE JASC*, vol. 23, no. 7, pp. 1424–1432, July 2005.
- [6] T. Bacinoglu, B. Gulbahar, and O. B. Akan, "Constant fidelity entanglement flow in quantum communication networks," in *Proc. IEEE GLOBECOM*, San Francisco, USA, 2010.
- [7] B. He, Y.-H. Ren, and J. A. Bergou, "Creation of high-quality long-distance entanglement with flexible resources," *Phys. Rev. A*, vol. 79, no. 5, pp. 052323, 2009.
- [8] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature (London)*, pp. 413–413, 2001.
- [9] L. Jiang et al., "Quantum repeater with encoding," *Phys. Rev. A*, vol. 79, no. 3, pp. 032325, 2009.

Manuscript received: July 25, 2013

Biographies

Youxun Cai (220110558@seu.edu.cn) is a postgraduate student at the State Key Laboratory of Millimeter Waves, Southeast University. His current research focus is quantum information theory and quantum wireless networks.

Xutao Yu (yuxutao@seu.edu.cn) is an associate professor at the State Key Laboratory of Millimeter Waves, Southeast University. Her research interests include wireless network protocols and quantum communication network protocols.

Yang Cao (220110559@seu.edu.cn) is a postgraduate student at the State Key Laboratory of Millimeter Waves, Southeast University. His research interests include wireless communication and quantum computation.

Powering Next-Generation Broadband Networks: ZTE's World-First Flexible, Configurable Router

16 September 2013, Shenzhen—ZTE today unveiled the world's first flexible, reconfigurable terabit router that allows customers to build the highest-performance broadband networks.

The terabit router supports the deployment of multiple line cards with processing capabilities of 10 Gbps to 1 Tbps. It also supports the deployment of modules that can scale throughput from 200 Gbps to 18 Tbps. For easy installation in a range of environments, the router interfaces are flexible and the component design is loose-coupled. This allows customers to customize networks to their needs and promotes adaptability, consistency, and continuity.

The superior performance of the terabit router is due to two proprietary ZTE technologies: cloud routing and intelligent system resource scheduling. Cloud routing involves building a system control plane that is based on distributed modular technology. This ensures efficient network resource use, scalability, and support for simultaneous deployment of multiple transmission protocols. Intelligent system resource scheduling allows for physical and logical system resource sharing and flexible scheduling. This ensures that resources are automatically allocated according to system load and that power consumption is driven down to 0.8 W/Gbps.

"Globally, it is becoming more important to deliver excellent value to customers and help them achieve sustainable development," said Xu Ming, general manager of ZTE's Bearer Network Product Division. "The flexible, reconfigurable terabit router offers industry-leading routing and can increase efficiency and extend equipment lifespan. The router is highly flexible, configurable, and scalable and can support a wide range of services as the network evolves."

For increased stability and scalability, the router uses ZTE's self-developed chipset. Better system integration helps improve energy consumption. With an open, programmable framework that includes SDN, the router makes the network architecture more modularized and provides network virtualization functions. This means that service developers can be integrated with network developers to build next-generation networks that are highly competitive.

Broadband bearer networks are regarded as key strategic assets in many countries. In August, China's State Council outlined the Broadband China plan, mapping out development objectives in the future. ZTE's flexible, reconfigurable terabit router helps align operators with the requirements of the Broadband China plan.

(ZTE Corporation)

IVI/MAP-T/MAP-E: Unified IPv4/IPv6 Stateless Translation and Encapsulation Technologies

Congxiao Bao and Xing Li

(Network Science and Cyberspace Research Center, Tsinghua University,
Beijing 100084, China)



Abstract

Stateless translation and stateless double translation/encapsulation technologies (IVI/MAP-T/MAP-E) define the address mapping and protocol translation/encapsulation algorithms between IPv4 and IPv6. IVI/MAP-T/MAP-E technologies maintain end-to-end address transparency between IPv4 and IPv6 and support communication initiated by IPv4-only or IPv6-only end systems. Therefore, they are the very critical techniques for the IPv4/IPv6 coexistence and transition.



Keywords

stateless translation; address mapping; protocol translation

1 Introduction

It is well-known that the 2^{32} addresses in the IPv4 address space have been exhausted. Two methods can be used to solve this problem: IPv4 address translation (NAT44) and IPv6. NAT44 translation technology is used between public and private IPv4 addresses. It is a mature technology; however, it destroys end-to-end address transparency and only supports private IPv4 initiated communication. NAT44 has been widely used on the user end for many years. However, when it is used in the core network, bulk states must be maintained on NAT44 translators. In addition, there are only about 16 million 10.0.0.0/8 private addresses available for each site on the IPv4 Internet. It has already shown that the use of NAT44 and 10.0.0.0/8 causes problems in terms of network interconnection, manageability, and security. To solve IPv4 address problems for the longer term, IPv6 must be developed.

¹ This denotation combines the Roman numbers IV (four) and VI (six) so that IVI means the interconnection of IPv4 and IPv6.

The problem of IPv4 address exhaustion was first raised about a decade ago, and the IPv6 protocol, which provides an address space of 2^{128} , was proposed. Initially, the Internet Engineering Task Force (IETF) recommended dual-stack technology for transitioning from IPv4 to IPv6. Several carriers all over the world have trialed IPv6 in different scales, and some Internet Content Providers have also offered IPv6 services [1]. However, by 2012, traffic in global IPv6 networks was lower than 1% of that in IPv4 networks. This indicates that dual-stack technology does not directly benefit operations, and even worse, does downgrade the user's experience. This is why dual-stack technologies have not really promoted the transition to IPv6 over the past decade.

The value of a network fundamentally relies in the number of people who use it. Currently, the number of people using new IPv6 networks is much less than the number of people using IPv4 networks. If people using IPv6 networks cannot connect to IPv4 networks, then IPv6 has no value at all. Hence, the most critical problem with transition is the interconnection between new IPv6 networks and old IPv4 networks. Interconnection can only be implemented through translation technology. However, because the IPv4 and IPv6 protocols were not compatible, interconnection is technically very difficult. With the construction of more IPv6-only networks and more research being done on IPv6, in 2010 the IETF has made breakthroughs in IPv4 and IPv6 interconnection technologies, especially in stateless translation technology (IVI¹). The IETF has released a series of RFC standards and working group drafts for new IPv4/IPv6 transition solutions in the recent years.

2 Stateless IPv4/IPv6 Translation Technology

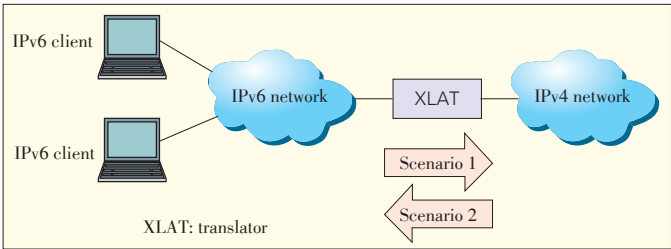
The Internet has a connectionless architecture, and routers do not need to maintain session states. Because the IVI translator is actually a router, stateless IVI translation has great value to the carriers for its highly scalability, manageability, and security. It also supports communication initiated from both the IPv4 and IPv6 sides.

2.1 Applications of IVI Translation Technology

The IPv6 address space is much bigger than the IPv4 address space. Therefore, stateless IVI translators are theoretically unfeasible without constraints. IETF RFC 6144 defines eight scenarios of IVI translation. IPv4 networks are on one side of the translator and IPv6 networks are on the other. One of the differences between these scenarios is which side the ISP's network and the Internet are located. Another difference is the side on which communication is initiated. **Fig. 1** shows the scenarios of stateless IVI translation technology [2]. In scenario one, IPv6 clients in the ISP's network access the server in IPv4 Internet. In scenario two, IPv4 clients in the IPv4 Internet access the server in IPv6 network.

IVI/MAP-T/MAP-E: Unified IPv4/IPv6 Stateless Translation and Encapsulation Technologies

Congxiao Bao and Xing Li



▲ Figure 1. Application of stateless IVI translation technology.

In both scenarios, IPv6-only networks are constructed, and IPv6 hosts can access the IPv4 Internet through the XLAT translator. The stateless IVI translation technology can be used in both scenarios, but the stateful NAT64 translation technology can only be used in scenario one. IVI translation technologies include address mapping and protocol translation mechanisms.

2.2 Address Mapping and Domain Name Translation

Because there is a large difference between IPv4 and IPv6 address space, stateless mapping can be used to convert IPv4 into IPv6 addresses, which are called IPv4-converted IPv6 addresses. Mapping from IPv6 to IPv4 is difficult. Mapping tables can be maintained dynamically for stateful address mapping, or a sub IPv6 address space can be selected for stateless mapping to IPv4 addresses. Mapped IPv6 addresses are called IPv4-translatable IPv6 addresses. The address-mapping algorithms are defined in IETF RFC 6052. Fig. 2 shows the IPv4-embedded IPv6 address format [3].

An IPv4-embedded IPv6 address comprises a variable-length IPv6 network prefix, the embedded IPv4 address, and a variable-length suffix. Bits 64 to 71 of the address are reserved for compatibility with the u-bit in the IPv6 address architecture and must be set to zero. The suffix, with all the bits set to zero in basic address mapping, is reserved for coding of the transport layer ports to map one IPv4 address onto several IPv6 addresses. In this way, scarce public IPv4 addresses can be statelessly multiplexed and can be used by many IPv6 hosts. In addition, RFC 6052 requires IPv4-converted IPv6 addresses and IPv4-translatable IPv6 addresses to have the same prefix so that the best route can be automatically chosen.

When an IPv6-only client accesses the IPv4 Internet, a DNS64 with above mapping rule must be implemented , which is defined in RFC 6147 [4]. DNS64 is the domain name server (DNS) connected to both the IPv4 and IPv6 networks, and it can translate A records into AAAA records dynamically. The IPv6-only client queries the AAAA record of the domain name through DNS64. If the AAAA record exists, DNS64 returns the AAAA record to the IPv6-only client. If the AAAA record does not exist, DNS64 generates the AAAA record (based on the mapping al-

gorithms defined in RFC 6052), and returns the AAAA record to the IPv6-only client. Stateless translators support communication initiated from the IPv4 Internet side. In this case, DNS46 should be statically configured. When a client in the IPv4 internet accesses an IPv6 server, DNS46 returns an A record based on the AAAA record of the IPv6 server [5].

2.3 Protocol Translation

The second issue for interconnection between two different protocol stacks is protocol translation. Fortunately, the IPv4 and IPv6 protocols are translatable. RFC 6145 defines the protocol translation algorithms, including [6]

- version number mapping
- mapping from IPv4 type of service (TOS) to IPv6 traffic class
- mapping from IPv4 total length to IPv6 payload length
- mapping from IPv4 time to live to IPv6 hop limit
- mapping from IPv4 transport layer protocol to IPv6 next header
- mapping from IPv4 address to IPv6 address.

The most difficult part of the protocol translation is fragmentation. IPv4 supports router fragmentation (DF = 0) and end-system fragmentation (DF = 1), but IPv6 only supports end-system fragmentation (implies DF = 1). An IPv6 header should be added so that fragmented IPv4 packets can be reassembled in the end systems. In addition, IPv4 and IPv6 networks support different maximum transmission units (MTUs). Because an IPv4 header is 20 bytes and an IPv6 header is 40 bytes, packets size will be increased/decreased during the translation. There are also many differences between Internet Control Message Protocol version 4 (ICMPv4) and ICMPv6, which needs to be handled in a different way.

An IPv6 router does not generally use translatable addresses. This means that if the translator fails to find the relevant IPv4 address when the router returns an ICMPv6 packet, the source address of the translated ICMP packet cannot be traced. IETF RFC 6791 defines the method for handling this problem [7].

RFC 6145 also defines the protocol translation algorithms used by stateful NAT64 translators. Beside RFC6145, RFC 6146 defines state maintenance technologies in these stateful translators, including the generation, maintenance, and destruction algorithms of dynamic mapping tables from IPv6 to

PL	0-----32---40---48---56---64---	72---80---88---96---104---112---120
32	Prefixv4 (32)	uSuffixzero
40	Prefixv4 (24)	u(8)Suffixzero
48	Prefixv4 (16)	uv4 (16)Suffixzero
56	Prefix(8)	uv4 (24)Suffixzero
64	Prefix	uv4 (32)Suffixzero

▲ Figure 2. IPv4-embedded IPv6 address format.

IPv4 addresses and ports [8].

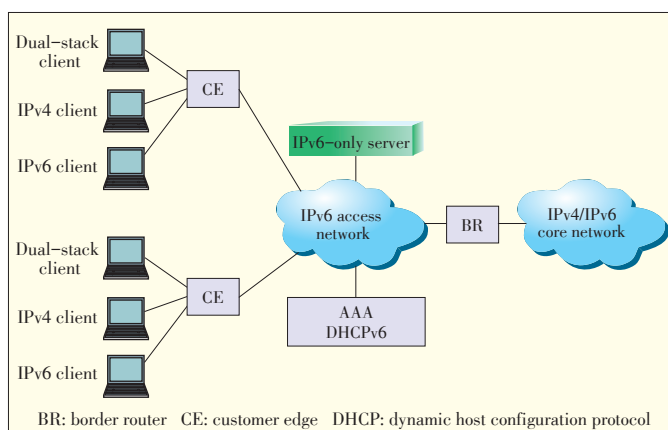
3 Stateless Double Translation/Encapsulation Technologies (MAP Series)

IVI translation technologies allow the interconnection between IPv4 and IPv6. However, three problems still need to be addressed. First, IPv4 addresses are being exhausted. In stateless IVI translation, public IPv4 addresses must be multiplexed so that IPv4 address resources can be used efficiently. Second, some applications (e.g. Skype) do not support IPv6, and some other applications (e.g. FTP) have embedded addresses. Third, customer edge is often assigned a 64-bit prefix rather than a single IPv6 address. MAP-Translation (MAP-T) and MAP-Encapsulation (MAP-E) are the stateless double translation and encapsulation technologies to solve above problems. MAP-T and MAP-E were proposed by IEFT in [9] and [10]. DHCPv6 options [11] and deployment considerations [12] have also been detailed by IEFT.

3.1 Application of Double Translation Mode

Fig. 3 shows an application of stateless double IVI translation (MAP-T).

The BR in Fig. 3 is the core translator. To IPv6, the BR is a router. To IPv4, the BR is an IVI translator using IPv4 address multiplexing. The second translation is done on the customer edge (CE). To IPv6, the CE is a router. To IPv4, the CE is an IVI translator and maps the ports at the transport layer according to the algorithms shown in subsection 2.3. The IPv6 access network deploys the AAA and DHCPv6 server for authentication and IPv6 prefix allocation. The IPv6-only server, which uses translatable addresses, can be deployed in the IPv6 access network. Through CE or BR translation, this server can provide services to IPv4-only clients. The user devices may be IPv4-only, dual-stack, or IPv6-only clients and are connected to the IPv6 access network through the CEs. If the user device is an IPv4-only client, it can access resources on the IPv6-only server through CE translation; it can access resources in the



▲ **Figure 3.** Application of stateless double IVI translation.

IPv4 internet through CE and BR with double translation; and it can visit other clients. If the user device is a dual-stack client, it can directly access Intranet and IPv6 internet resources; it can access resources in the IPv4 internet through CE and BR with double translation; and it can visit other clients. If the user device is an IPv6-only client, it can access iIntranet and IPv6 Internet resources; it can access resources in the IPv4 Internet through BR translation; and it can visit other clients.

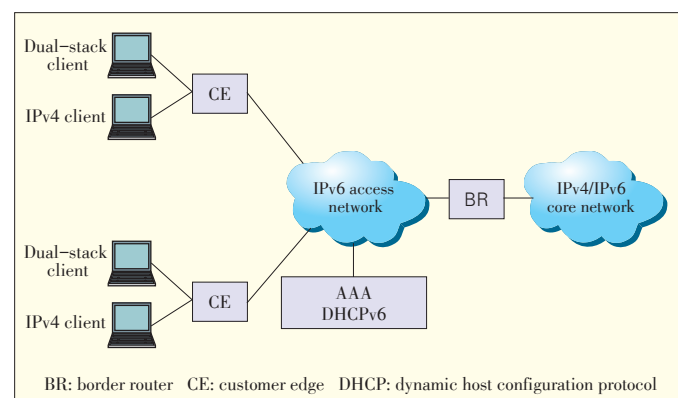
3.2 Application of Encapsulation Mode

Fig. 4 shows an application of MAP-E.

The BR in Fig. 4 is the core encapsulator/decapsulator. To IPv6, the BR and CE are both routers. To IPv4, the BR is an IPv4 over IPv6 encapsulator/decapsulator with IPv4 address multiplexing; and the CE is an IPv4 over IPv6 encapsulator/decapsulator for mapping the ports at the transport layer. The IPv6 access network deploys the AAA and DHCPv6 server for authentication and IPv6 prefix allocation. User devices are connected to the IPv6 access network through the CEs. A user device that is an IPv4-only client can access the IPv4 internet through CE encapsulation and BR decapsulation, and visit other clients. A user device that is an IPv4/IPv6 dual-stack client can access intranet and IPv6 internet resources; it can access resources in the IPv4 Internet (through CE encapsulation and BR decapsulation); and it can visit other clients. However, MAP-E does not support the deployment of IPv6-only servers in IPv6 access networks nor does it allow IPv6-only clients to connect to the IPv4 internet.

3.3 Port Mapping

The stateless mapping algorithm of addresses and ports is one of the key algorithms in MAP Series. It uses 16-bit ports of transmission control protocol (TCP) and user datagram protocol (UDP) to expand IPv4 addresses. For non-multiplexed IPv4 addresses, 65,536 concurrent TCP/UDP ports are available for each client. If the multiplexing ratio is 16, then 4096 concurrent TCP/UDP ports are available for each client. If the multiplexing ratio is 128, then 512 concurrent TCP/UDP ports are available for each client. Experimental data shows that 200



▲ **Figure 4.** MAP-E application scenario.

IVI/MAP-T/MAP-E: Unified IPv4/IPv6 Stateless Translation and Encapsulation Technologies

Congxiao Bao and Xing Li

to 500 concurrent TCP/UDP ports are enough for a normal connection for each common client. Therefore, the stateless mapping algorithm of addresses and ports can be used for efficiently multiplexing public IPv4 address resources. When the stateless mapping algorithm of addresses and ports is used, a port-set ID (PSID) should be defined for each client. The mapping relationships between PSIDs and available ports are determined by the extended modulus algorithm, defined as

- Given a PSID, the number of ports P at the transport layer available for the end system is $P = R \times M \times j + M \times K + i$, where R is the multiplexing ratio, M is the number of continuous ports, and i and j are integer variables.
- Given P , the PSID of the system is $PSID = \text{floor}(P/M) \% R$, where floor means that the number is rounded down to the nearest integer, and $\%$ is the modulus operator.

The extended modulus algorithm allows the transport-layer ports that are used by the clients with different PSIDs to be distributed evenly in the port space or in blocks. The algorithm also adjusts the number of continuous ports in each block and supports address clustering similar to classless interdomain routing. The PSID length can be defined for clustering available ports.

If the multiplexing ratio, number of continuous ports, and port clustering length are given, the extended modulus algorithm can be used to calculate the total number of TCP/UDP ports available for a specific client through the PSID. The PSID can also be calculated from the ports given vice versa. In this way, management overhead can be significantly reduced, and security and traceability can be significantly improved by stateless multiplexing of public IPv4 addresses. Because the ICMP and ICMPv6 packets only have ID number and no source and destination port number, the extended modulus algorithm should be used for the ID number.

3.4 Address Format

Fig. 5 shows the MAP address format, which is an extension of RFC 6052. The main additions to RFC 6052 are:

- The MAP address format includes a 64-bit prefix that contains an IPv6 prefix, EA-bits, and subnet-id. EA-bits comprise an IPv4 subnet ID and a PSID and are used for identifying different clients. Subnet-id identifies an IPv6 subnet

used by a client, and the subnet prefix no shorter than /64.

- The suffix in MAP is not zero, PSID is embedded in the suffix.
- Different prefixes are used for converted and translatable addresses in MAP to assign prefixes to clients.

The EA-bits give each CE a unique prefix. Different prefixes can also be assigned to CEs without using EA-bits. The advantages of using EA-bits are address clustering and good extensibility. However, if the EA-bits are not used, the IPv6 prefixes are independent from the IPv4 addresses. Both methods have advantages and can be selected as required.

3.5 Unified Mechanism for Double Translation and Encapsulation Modes

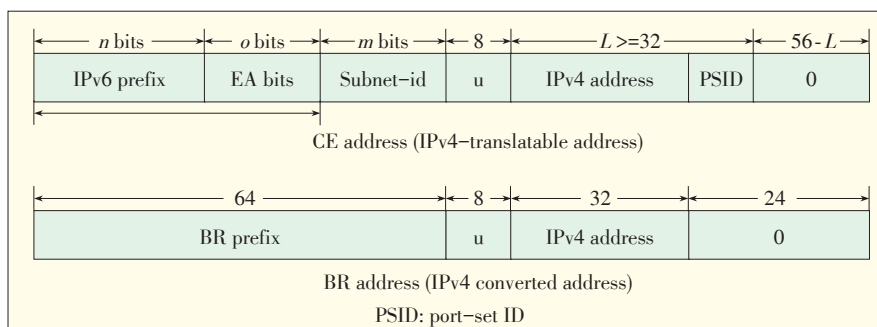
Stateless double translation supports both IPv4-only applications, such as Skype and applications with embedded IP addresses, such as FTP without application-layer gateways between IPv4 and IPv6. In addition, double translation does not require DNS64 or DNS46. From another perspective, stateless double translation can be presented as an IPv4 over IPv6 encapsulation technology with header compression. MAP-T and MAP-E technologies use the same extended modulus algorithm and address format (BR prefix is reduced to a single address in encapsulation mode) and are therefore very similar. The only difference is in the packet processing method. With MAP-T, data packets are translated as defined in RFC 6145. With MAP-E, data packets are encapsulated as defined in RFC 2473 [13].

The advantage of MAP-T is seamless evolution to single translation, which can promote transition to IPv6-only networks but keep interconnection with the IPv4 Internet. In addition, with MAP-T, the IPv6 packets in an IPv6 access network do not have an encapsulated data structure and can use all the management and control functions at the network and transport layers on IPv6 routers. MAP-E, however, can only manage and control packets after decapsulation. The advantage of MAP-E is that all the information in the IPv4 packets can be kept, and the checksum at the transport layer does not need to be modified. The encapsulation modes defined in RFC 2473 and the TCP and UDP protocols at the transport layer are all defined by the next header in the IPv6 header structure, so the decision

to use translation or encapsulation mode will be made only for packets transmitted from IPv4 to IPv6. For packets transmitted from IPv6 to IPv4, the translation or encapsulation mode is automatically selected according to the value of the IPv6 next header. Therefore, MAP-T and MAP-E mode can be configured flexibly [14].

3.6 Unified Stateless/Client State/Stateful

Stateless means that the mapping relationships between IPv4 and IPv6 addresses and



▲ Figure 5. MAP address format.

ports are entirely determined by algorithms, and mapping tables are not maintained on devices. Stateful means that the mapping relationships between IPv4 and IPv6 addresses and ports are generated dynamically according to the five-tuples of sessions, and the mapping tables are maintained on devices. Client's state means that the mapping relationships between IPv4 and IPv6 addresses and ports are defined according to different clients (called semi-stateful), and only client-orientated mapping tables are maintained on devices. MAP-T can be used together with MAP-E, NAT64, and Dual-Stack Lite [15]. Therefore, the MAP-T/MAP-E CE can work with NAT64 translator and Dual-Stack Lite AFTR without any modifications. Because stateless and stateful are two extremes, the MAP-T/MAP-E CE can support client state scenario without any modifications.

4 Transition Roadmap

Although IPv4 addresses have been exhausted, IPv6 are still seldom used. To ensure the healthy and sustainable development of the Internet, a transition roadmap should be formulated. We should rethink policies that favor dual stack over translation proposed by IETF a decade ago, because former policies have failed to promote the transition from IPv4 to IPv6 over the past decade. Also, in China, no more public IPv4 addresses are available for dual stack, and implementing dual stack by using private addresses through NAT44 does not encourage IPv6 transition.

Because IVI and MAP technologies are becoming increasingly sophisticated, we suggest building IPv6-only networks and formulating policies that favor translation and double translation/encapsulation over dual stack. The specific technical solutions are:

- IPv6 should be used for communication with peer IPv6 networks.
- Stateless IVI translation technology should be used for communication with IPv4 networks on the peer side.
- Stateless double translation technology should be used if the application programs do not support IPv6 or have embedded IPv4 addresses.
- Encapsulation technology should be used if all the information in IPv4 packets need to be kept or the encrypted packets at the transport layer needs to be processed.

In the middle and later stages of transition, double translation will seamlessly evolve into single translation, and then evolve into the stage that translators will eventually be removed. This is when the transition ends and the IPv6-only era begins.

5 Conclusion

The recommended roadmap can be used for transitioning China's networks to IPv6 and interconnection with the IPv4 in-

ternet, with highly usage of existing IPv4 public address. In this way, China can take the initiative in IPv4/IPv6 transition. This technical solution conforms to China's government roadmap and schedule for next-generation Internet. It has already been specified that, from 2011 to 2015, the government will guide the transition to IPv6 networks and allow the coexistence of IPv4 and IPv6 networks. However, IPv6-only networks must be constructed and interconnected with IPv4 networks. At present, five IETF RFC standards have been released for IVI technology, and four IETF working group drafts have been formulated for MAP technologies. IVI technology has been supported by equipment manufacturers such as Cisco, ZTE, and Huawei and has been running properly in CNGI-CERNET2 for more than two years. MAP technologies have been released by Cisco and other equipment manufacturers and have attracted the attention of international carriers such as Telecom Italia, Soft-Bank, Deutsche Telekom, and Charter Communications. The industry chain is slowly being shaped. IVI and MAP technologies are the only stateless translation and double translation technologies for IPv4/IPv6 interconnection and will develop in leaps and bounds over the next few years.

References

- [1] *Basic Transition Mechanisms for IPv6 Hosts and Routers*, RFC 4213, 2005.
- [2] *Framework for IPv4/IPv6 Translation*, RFC 6144, 2011.
- [3] *IPv6 Addressing of IPv4/IPv6 Translators*, RFC 6052, 2010.
- [4] *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*, RFC 6147, 2011.
- [5] *The CERNET IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition*, RFC 6219, 2011.
- [6] *IP/ICMP Translation Algorithm*, RFC 6145, 2011.
- [7] *Stateless Source Address Mapping for ICMPv6 Packets*, RFC 6791, 2012.
- [8] *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*, RFC 6146, 2011.
- [9] X. Li, C. Bao, W. Dec, et al., "Mapping of address and port using translation (MAP-T)," IETF, draft-ietf-software-map-t-00, 2012.
- [10] O. Troan, W. Dec, X. Li, et al., "Mapping of address and port with encapsulation (MAP)," IETF, draft-ietf-software-map-02, 2012.
- [11] T. Mrugalski, O. Troan, C. Bao, et al., "DHCPv6 options for mapping of address and port," IETF, draft-ietf-software-map-dhcp-01, 2012.
- [12] Q. Sun, M. Chen, G. Chen, et al., "Mapping of address and port (MAP) — deployment considerations," IETF, draft-ietf-software-map-deployment-00, 2012.
- [13] *Generic Packet Tunneling in IPv6 Specification*, RFC 2473, 1998.
- [14] X. Li, C. Bao, G. Han, et al., "MAP interoperability testing results," IETF, draft-xli-software-map-testing-00, 2012.
- [15] *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*, RFC 6333, 2011.

Manuscript received: April 1, 2013

Biographies

Congxiao Bao is an associate researcher with Network Science and Cyberspace Research Center, Tsinghua University. His research interests include computer networks and multimedia communication systems. He is the leading author of five IETF RFC documents on stateless IPv4/IPv6 translation technology.

Xing Li is a professor with Network Science and Cyberspace Research Center, Tsinghua University. His research interests include signal and information processing, computer networks, and multimedia communication systems. He is the leading author of eight IETF RFC documents.

A Parallel Platform for Web Text Mining

Ping Lu¹, Zhenjiang Dong¹, Shengmei Luo¹, Lixia Liu¹,
Shanshan Guan², Shengyu Liu², and Qingcai Chen²

(1. ZTE Corporation, Nanjing 210000, China;

2. Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen 518055, China)

Abstract

With user-generated content, anyone can be a content creator. This phenomenon has infinitely increased the amount of information circulated online, and it is becoming harder to efficiently obtain required information. In this paper, we describe how natural language processing and text mining can be parallelized using Hadoop and Message Passing Interface. We propose a parallel web text mining platform that processes massive amounts of data quickly and efficiently. Our web knowledge service platform is designed to collect information about the IT and telecommunications industries from the web and process this information using natural language processing and data-mining techniques.

Keywords

natural language processing; text mining; massive data; parallel; web knowledge service

1 Introduction

With the rapid development of Web 2.0 and social networks, more and more information is being created. New technologies allow anyone to create all kinds of user-generated content (UGC), and this has spawned millions of new search results. As a result, seeking information has become more difficult and troublesome. Increasingly, people have less time to acquire information, and knowledge services have become more important.

Natural language processing and text mining have matured; however, they still need to be made more efficient for mass text engineering. Cloud computing has been very successful for large internet companies, who have used large numbers of cheap PCs to construct computer clusters that provide distributed storage and simple, efficient distributed processing of massive amounts of information. Cloud computing platforms have uncomplicated programming and high fault tolerance,

and they can be conveniently expanded. They use the open-source Hadoop file system and Message Passing Interface (MPI) to parallelize many common text-mining techniques. This allows for fast, more efficient information processing.

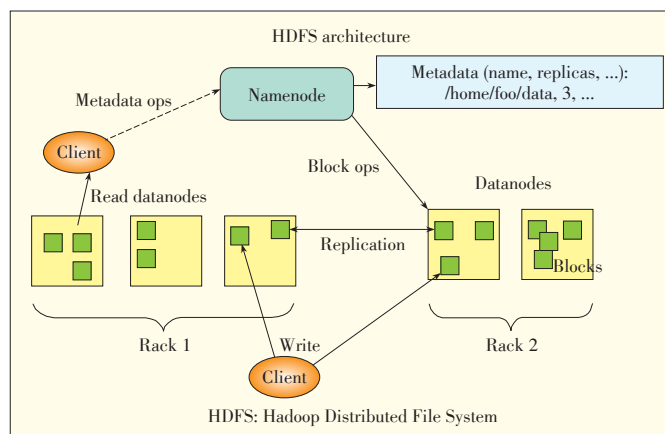
1.1 Hadoop Platform

Apache Hadoop is an open-source software framework that allows large data sets to be processed in a distributed way across clusters of computers with simple programming models. Hadoop is designed to scale from a single server to thousands of machines, each of which is capable of local computation and storage. Rather than rely on hardware to provide high availability, the Hadoop library is designed to detect and handle failures at the application layer. Hadoop can deliver a highly available service on a cluster of computers, each of which may be prone to failure. The Hadoop kernel is Hadoop Distributed File System (HDFS) (Fig. 1).

1.2 Message Passing Interface

MPI is a library specification for message-passing and has been proposed as a standard by a committee of vendors, implementers, and users. The MPI standard defines the syntax and semantics of a core of library routines that is very useful to a wide range of users writing portable message-passing programs in Fortran 77 or C. MPI is a language-independent communication protocol used to program parallel computers. Both point-to-point and collective communication are supported. In [1], MPI is defined as “a message-passing application programmer interface together with protocol and semantic specifications for how its features must behave in any implementation.” MPI is designed for high performance, scalability, and portability, and it remains the dominant model for high-performance computing today [2].

The MPI interface provides a virtual topology, synchronization, and communication functionality in a set of processes that



▲ Figure 1. The structure of Hadoop Distributed File System.

have been mapped to nodes, servers, and computer instances. These processes are mapped in a language-independent way and have language-specific syntaxes (bindings) and a few language-specific features.

2 Design of a Parallel Text-Mining Platform

A platform based on HDFS and MPI comprises several parallel modules, including web crawler, Chinese word segmentation, text categorization, text clustering, topic detection and tracking (TDT), automatic summarization, semantic computing, and sentiment analysis (**Fig. 2**). Experiments show that all the modules operating together are much more effective than a single node operating by itself.

2.1 Web Crawler

A web crawler is a program for parsing web pages. It downloads internet pages for the search engine (SE) and is an important part of the SE. A traditional crawler starts with initial URLs and parses other pages through the links on the pages given by the initial URLs. While parsing, the crawler extracts URLs from the current page until reaching some end conditions. The crawler always processes a large number of web pages. A crawler run on a single computer cannot properly parse and update pages for the SE. However, a distributed crawler draws on the computing ability of multiple computers and can improve parsing speed and system throughput.

In our system, the crawler sends and receives message in different computers by MPI. We use HDFS to store the files, and we eliminate repeated URLs by using BerkeleyDB. The crawler has three processes: start-up, data download and handing out URLs, and writing data to HDFS.

2.2 Chinese Word Segmentation

ELUS is a natural language processing (NLP) application that comprises Chinese word segmentation, part-of-speech tagging, and named entity recognition.

Word segmentation technology is based on the n -gram model. In statistical language models such as n -gram, natural language is a random process, and each natural-language sentence comprises minimum structure units (words). An n -gram

model is also called an $n-1$ Markov model. They use an absolute discount smoothing algorithm. The whole process involves searching words in a rapid-indexing dictionary, combining two algorithms, and making the word segmentation.

Part-of-speech tagging uses a conditional random fields (CRF) model. For a given observed value sequence, the model uses index calculation to calculate the conditional probability of the whole label sequence. CRF is a type of undirected graph model or Markov Random Field model.

In a series of input random variables X , the conditional probability of the outputs random variable is Y . The inverse ratio versus the potential function of each clique is $P(Y|X)$. This model can solve label bias.

Named entity recognition combines the maximum entropy (ME) model (a probability model) with Chinese named entity rules. This combination achieves better results.

2.3 Text Classification

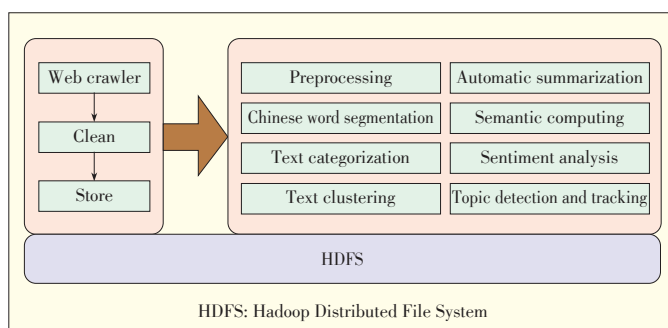
Text classification is based on text content and is used to classify a certain text into one or more predefined classes. Text classification involves five stages: preprocessing, feature selection, text representation, classifier design, and assessment of results [3]. For this platform, we use 10 feature selection methods, including document feature (DF), information gain (IG), expected cross entropy (ECE), mutual information (MI), and chi-square (CHI). We also implement six classifiers, including support vector machine (SVM), k -nearest neighbor (k -NN), and Bayes'.

Text classification is a supervised learning process in which classifier models are learned according to the training data set. Then, the generated classifier model is used to predict the category of the input document. However, for mass data, stand-alone training and prediction is very inefficient, and a parallel model needs to be used. The program inputs and outputs in HDFS. At the same time, multiprocessing operation is achieved with MPI. One process trains data, and the rest of the process divides the files on HDFS into smaller files and makes predictions.

2.4 Text Clustering

Text clustering involves dividing the entire text set into clusters so that documents in the same cluster are as similar as possible and different from documents in other clusters. A typical division-based clustering algorithm is k -means [4]. This algorithm is efficient and fast and is often preferred for clustering large data sets. The k -means algorithm also has good parallelism. In this paper, we develop the k -means algorithm by using MPI to incorporate it into HDFS and interprocess communication.

The agglomerative hierarchical clustering (AHC) algorithm reflects the hierarchical relationships between documents. AHC is better than a division-based clustering algorithm in terms of retrieving relevant documents, detecting topics, and



▲ **Figure 2.** Architecture for a platform based on HDFS and MPI.

A Parallel Platform for Web Text Mining

Ping Lu, Zhenjiang Dong, Shengmei Luo, Lixia Liu, Shanshan Guan, Shengyu Liu, and Qingcai Chen

tracking [6]. However, it is complex, and there are too many clusters in the results. We propose a secondary hierarchical clustering algorithm called DAHC. The affinity propagation (AP) algorithm can be used to filter the “noise” outlier data and can detect clusters with an arbitrary shape [7], [8]. However, when the text vector dimension is too high, data sparseness becomes a serious problem. In this case, the number of clusters is often greater than the number of predefined categories. The average scale of clusters is also too small, and each cluster is more pure. Therefore, we propose an APAHC algorithm that combines AP algorithm and AHC algorithm.

2.5 Topic Detection and Tracking

A TDT event is a certain thing that occurs in a specific location at a certain time. The TDT research task comprises story segmentation, new event detection, story link detection, topic detection, and topic tracking [9].

Often-used TDT methods include methods based on the incremental TF-IDF model [10], improved vector space model [11], clustering [12], or named entity [13]. The popularity of an event depends on related news stories, blogs, bulletin boards, and other commentary. The TDT module focuses on recalling and organizing hot events. It also implements MPI parallelization at a document level. Large documents that are stored in Hadoop are divided into several parts, each of which is clustered independently to generate topics. This clustering is performed by a clustering algorithm designed specifically for TDT. Descriptive words are produced for each topic, and topics generated by all of the parts are clustered using single-pass clustering on the parallelization platform.

2.6 Automatic Summarization

In automatic summarization, the most important information in the original text is extracted and output in the form of concise, fluent language. Most existing automatic summarization methods analyze the structure of an article and use word syntax and statistics to determine the subject. Some automatic summarization methods have been successful, but accuracy can be improved. Semantic analysis is very important in determining the main idea of an article, but most existing automatic summarization methods lack this. We propose combining semantic analysis, structural analysis, statistical methods, and natural language processing to develop an automatic summarization system that meets practical requirements. In a parallelized system, Hadoop is used to split the document collection, and MPI is used to parallelize the program.

2.7 Semantic Computing

The purpose of semantic computing is to explain the natural language statement and the meaning of each part of it. There are many difficulties with semantic calculation. There are many ambiguities, such as synonymy and polysemy, in natural language. A sentence may mean different things in different

contexts. Theories and methods of semantic computing are not mature.

In semantic computing, semantic similarity is commonly calculated using word distance. There are two kinds of word similarity calculation: one based on ontology or taxonomy and another based on statistics derived from a large corpus.

In our system, the computation of semantic similarity is based on HowNet. First, we determine word similarity by making an inquiring through HowNet. If two words are both in HowNet, the semantic similarity can be directly obtained. If one of the words is not in HowNet, the semantic similarity can be obtained from the distance between the two words in the synonym tree. If both words are not in HowNet, fuzzy string matching is used to calculate the semantic similarity.

2.8 Sentiment Analysis

Sentiment analysis is used to determine how to recognize, classify, label, and extract opinion text and its sentiment. Recognizing sentiment words and judging the semantic polarity of the sentiment words are fundamental to sentiment analysis. Each sentiment word may contain one or more polarities, such as positive, negative, and neutral polarity. We roughly classified text sentiment by using sentiment-dictionary methods and machine-learning methods.

The sentiment-dictionary method involves directly classifying the text according to a sentiment dictionary that we compiled ourselves. We use this method in conjunction with other related heuristic language rules. The machine-learning method involves extracting features and using them to train a classifier. The obtained model is then used to classify the sentiment of the text.

We use both methods to classify the documents on Hadoop. After making many necessary modifications for the LIBSVM, the interface can run in parallel using an MPI library.

3 Performance Testing

In our experiment, we used an HP Elite 7100 Microtower PC with an Intel(R) Core(TM) i5 2.80 GHz processor and 4 GB RAM. The software environment included SUSE Enterprise 11, MPICH2-1.4, and Hadoop-0.20.2-cdh3u0.

We take advantage of recall and precision in our evaluations; however, to only use one of these would be one-sided. The F-measure is one an index that includes both recall and precision. It is defined as

$$F_measure = (2PR)/(P+R) \quad (1)$$

Examining the speedup ratio is important when evaluating parallelization. We scanned the running time of the programs, which were running on between one to six nodes.

3.1 Chinese Word Segmentation

We use the public evaluation corporuses of Peking University

(PKU), Microsoft Research Asia (MSRA), City University of Hong Kong (CITYU), and Academia Sinica, Taiwan (AS). In this public evaluation corpora, F values range from 97.7% to 99.1%.

We used 6930 documents (about 92 MB) to evaluate the speedup ratio (**Table 1**).

▼ **Table 1.** The speedup ratio from our examination of Chinese word segmentation

Node	1	2	3	4	5	6
Time (s)	1222	750	649	474	504	507

3.2 Text Categorization

In our examination of the English corpus, called Reutor, we used SVM and ECE with micro-F of 0.91985 and macro-F of 0.86547.

When examining speedup ratio, we used a 1.7 MB standard corpus. The running results of the examination are shown in **Table 2**.

▼ **Table 2.** Speedup ratios from our examination of text categorization

Node	1	2	3	4	5	6
Time (s)	44.93	41.15	38.9	38.47	37.78	37.13

3.3 Text Clustering

We examined the labeled standard corpus with a purity of 0.84509, and the F-value was 0.69492. **Table 3** shows the speedup ratios.

▼ **Table 3.** Speedup ratios from our examination of text clustering

Node	1	2	3	4	5	6
Time (s)	9034	5884	4006	3546	3741	3769

3.4 Topic Detection and Tracking

We used two test corpora, one of which was an event corpus of news topics and the other of which only included blog webpages. In the former corpus, the precision was 95.04% and the F-value was 90.17%. In the latter corpus, the precision was 92.18%.

Table 4 shows the speedup ratios.

▼ **Table 4.** Speedup ratios from our examination of topic detection and tracking

Node	1	2	3	4	5	6
Time (s)	9760	3871	1843	985	419	567

3.5 Automatic Summarization

The test corpus comprised 100 news articles that were offered by the project group. The precision was 64.44%, and the recall was 66.38%. The F-measure was 65.4%.

In our examination of speedup ratio, we used a 42 MB stan-

dard corpus. The results are shown in **Table 5**.

▼ **Table 5.** Speedup ratios from our examination of automatic summarization

Node	1	2	3	4	5	6
Time (s)	193	158	148	144	136	136

3.6 Semantic Computing

We used an NTCIR 2009 test corpus that comprised 409 similar statement pairs, and the precision was 68.05%. However, parallelization failed in this examination.

3.7 Sentiment Analysis

Table 6 shows the results of the sentiment analysis when NTCIR-7 MOAT multilanguage analysis was performed.

▼ **Table 6.** Results of sentiment analysis when NTCIR-7 MOAT multilanguage analysis is used

Method	Precision	Recall	F1
Sentiment-dictionary	0.7162	0.5958	0.6505
Machine-learning (category 2)	0.7634	0.4922	0.5985
Machine-learning (category 1)	0.8498	0.2394	0.3736

Finally, the results of the whole performance test are shown in **Table 7**.

▼ **Table 7.** Results of the whole performance test

Item Tested	F-value	Speedup
Chinese word segmentation	0.977	2.58
Text categorization	0.919	1.19
Text clustering	0.695	2.55
Automatic summarization	0.654	1/42
Semantic computing	0.680	—
Sentiment analysis	0.651	2.24
Topic detection and tracking	0.902	2.25

4 Application System Design

We build a web knowledge service system according to the demands of users from the IT and telecommunications fields. This knowledge service system is based on the parallel web text mining platform.

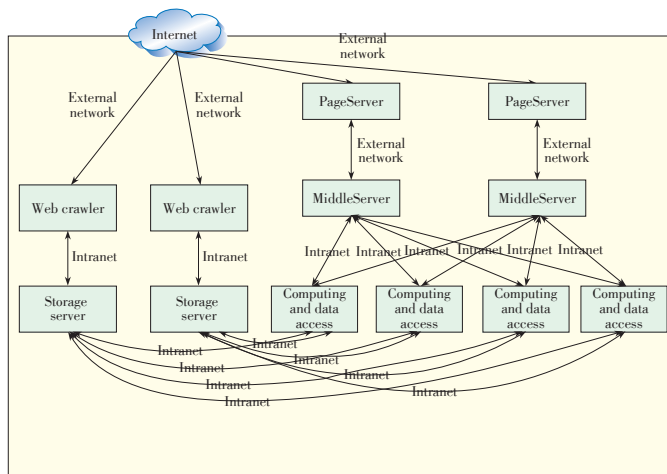
4.1 Physical Architecture of Proposed Platform

In **Fig. 3**, PageServer provides the page display function, and all web pages a user visits are provided by this server. PageServer is used to show and recommend information resources of the IT and telecommunications industries. It allows the user to manually submit information resources.

MidServer provides the interface to access the database. Pages on PageServer access the database through MidServer.

A Parallel Platform for Web Text Mining

Ping Lu, Zhenjiang Dong, Shengmei Luo, Lixia Liu, Shanshan Guan, Shengyu Liu, and Qingcai Chen



▲ Figure 3. Physical architecture of proposed platform.

The server provides the interface to access the database.

Computing and data access is used to calculate and access data, analyze the collected data, and mine data.

The storage server is used for database management and Hadoop-based parallel storage. The web crawler supports parallel data acquisition as well as parallel data reading and writing. The web crawler also supports incremental crawling, for which the running environment must remain unchanged.

4.2 System Functions

The web knowledge service system comprises the following modules: information, blog, journals, conference, and university.

The information module located hot information in technical fields such as cloud computing, new media and the internet. It displays this information in different categories, and we give this information a value. The blog module locates hot information in technical fields such as cloud computing, new media and the internet. It displays this information in different categories. As well as displaying the blog articles, it can also show rankings and bloggers. The journals module collects articles from mainstream journals from home and abroad. It is updated regularly to obtain the most recent scientific and technological developments in specific fields. The conference module is designed to collect and organize information of well-known, top-level conferences. The content includes the name, place, and time of the conference; paper submission deadline; and other details (the entire contents of the original page). The conference module collects information from various conferences with unstructured information; it formats and stores this information in the database; and it displays this information in the foreground. The module imports the conference name and builds the program automatically. In this way, the user can easily locate the relevant conference information. The university module extracts and displays information from researchers in every field. It extracts the name, gender, job title, work units, research direction, personal web pages, office telephone,

email, and other details. The system can provide global searches as well as subfield searches to users. Fig. 4 shows the index



▲ Figure 4. Index page of the information service system.

page of the information service system.

5 Conclusion

To solve the problem of slow, inefficient text mining of big data, we have proposed a parallel web text mining platform and built a web knowledge services system for the IT and telecommunications industries. These serve as references for the development of subsequent products.

References

- [1] W. Gropp, E. Lusk, N. Doss, and A. Skjellum, "A high-performance, portable implementation of the MPI message passing interface standard", in *Parallel Computing*, vol.22, no. 6, pp. 789–828, Sep. 1996.
- [2] S. Sur, M. Koop, and Dhabaleswar K. Panda, "High-performance and scalable MPI over InfiniBand with reduced memory usage: an in-depth performance analysis," in *Proc. 2006 ACM/IEEE Conf. on Supercomputing*, Tampa, FL, Nov. 2006, p. 13.
- [3] Kjersti Aas and Line Eikvil. (1999). *Text Categorization: A Survey*, Norwegian Computing Center. [Online]. Available: http://www.oocities.org/rr_andres/docs/aas99text.pdf
- [4] J. McQueen, "Some methods for classification and analysis of multivariate observations," in *Proc. 5th Berkeley Symp on Mathematical Statistics and Probability*, Berkeley, CA, 1967, pp. 281–297.
- [5] J. P. Marques and Y. F. Wu, *Pattern recognition: Concepts, methods and applications*, Beijing: Tsinghua University Press, 2002, pp. 51–74.
- [6] P. Willett, "Recent trends in hierarchic document clustering: A critical review," *Info. Processing and Management*, vol. 24, no. 5, pp. 577–597, 1988.
- [7] B. J. Bezdek, *Pattern recognition with fuzzy objective function algorithms*. New York: Plenum Press, 1981.
- [8] M. Ankerst, M. M. Breunig, and H.P. Kriegel, "OPTICS: Ordering points to identify the clustering structure," in *Proc. ACM SIGMOD Int. Conf. on Management of Data*, Madison, WI, Jun 2002, pp. 49–60.
- [9] He Ruifang, "Topic detection and tracking research," TS Group Meeting, 2005.
- [10] T. Brants, F. Chen, and A. Farahat, "A system for new event detection," in *Proc. of ACM SIGIR Conf. on Research and Development in Info. Retrieval*, To-

A Parallel Platform for Web Text Mining

Ping Lu, Zhenjiang Dong, Shengmei Luo, Lixia Liu, Shanshan Guan, Shengyu Liu, and Qingcai Chen

ronto, Canada, Jul. 2003, pp. 330–337.

- [11] Giridhar Kumaran and J. Allan, "Text classification and named entities for new event detection," In *Proc. ACM SIGIR Conf. on Research and Development in Info. Retrieval*, Sheffield, UK, Jul. 2004, pp. 297–304.
- [12] J. Allan, "Introduction to topic detection and tracking," In *Topic Detection and Tracking: Vent-based Information Organization*, Norwell, MA: Kluwer, 2002,

pp. 1–16.

- [13] Qi He, Kuiyu Chang, and Ee-Peng Lim, "Analyzing feature trajectories for event detection", in *Proc. ACM SIGIR Conf. on Research and Development in Info. Retrieval*, Amsterdam, Netherlands, Jul. 2007, pp. 207–214.

Manuscript received: December 19, 2012

Biographies

Ping Lu is the president of Communication Services R&D Institute for Cloud Computing and IT Operation, ZTE Corporation. He received his MS degree from Southeast University in 1996. His research interests include cloud computing, internet of things, home networking, multimedia networking, and mobile networking.

Zhenjiang Dong is the vice president of the Communication Services R&D Institute for Cloud Computing and IT Operation, ZTE Corporation. He received his MS degree from Harbin Institute of Technology in 1996. His research interests include cloud computing, multimedia networking, and mobile networking.

Shengmei Luo graduated from Harbin Institute of Technology in 1996 and has been involved in telecommunication network and service development for many years. He is currently the chief architect at ZTE Corporation and a professor at Nanjing University of Post and Telecommunications. He has been awarded a prize for scientific and technological progress and is the holder of many patents. He has published a number of academic papers in core communication journals. He is the member of the China Cloud Computing Committee and has rich experience in ICT domains.

Lixia Liu is a senior engineer in the pre-research department at ZTE. She received her MS degree from Ocean University of China in 2008. Her research interests include natural language processing, text mining, data mining, machine learning, mathematical statistics, and cloud computing.

Shanshan Guan is a graduate student in the Department of Computer Science and Technology, Harbin Institute of Technology (Shenzhen Graduate School). He received his BS degree in 2011 from Harbin Institute of Technology at Weihai. His research interests include text mining and machine learning.

Shengyu Liu is a PhD student in the Department of Computer Science and Technology, Harbin Institute of Technology (Shenzhen Graduate School). He received his MS degree in 2011 from Harbin Institute of Technology. His research interests include text mining, natural language processing, information extraction, and machine learning.

Qingcai Chen is a professor and PhD supervisor in the Department of Computer Science and Technology, Harbin Institute of Technology (Shenzhen Graduate School). He received his PhD degree in 2003 from Harbin Institute of Technology. His research interests include machine learning, pattern recognition, natural language processing, information retrieval and speech processing. He has published about 50 papers in renowned academic journals and conferences proceedings. He is the member of the IEEE Systems, Man and Cybernetics Society and a reviewer for IEEE Transactions on Systems, Man and Cybernetics.

ZTE USA Announces Its First Corporate Partnership and Consumer Marketing Push in Conjunction with the Houston Rockets

5 October 2013, Houston—The Houston Rockets and ZTE USA, the fastest-growing smartphone provider in the United States, announced that ZTE will be the official smartphone of the Houston Rockets for the 2013–14 NBA season. This is the first partnership of its kind for ZTE globally and the first big consumer marketing push in the United States since the company entered the country 15 years ago.

ZTE will have the opportunity to engage directly with the fans of the Rockets around the world. ZTE will have a presence at key Rockets events, in TV broadcasts of Rockets games, in Rockets digital media, and through customized activation during Rockets games.

Both the Rockets and ZTE brands are debuting new, more powerful lineups this year. ZTE is launching two new smartphones—ZTE Grand S and ZTE nubia 5—at the same time the Rockets have a highly anticipated new roster featuring James Harden, Dwight Howard, Jeremy Lin, and Chandler Parsons. Both brands are expanding globally, with ZTE providing its technology to more than 500 carriers and operators in more than 160 countries and the Rockets reaching more than 325 million people worldwide through more than 30 different networks.

ZTE and the Rockets announced this partnership in a special press event just before the first preseason game on Saturday, October 5. Under the terms of the agreement, ZTE will have corporate sponsor status, including the use of Rockets marketing rights, TV-visible signage, and the right to announce ZTE's sponsorship of the preseason opener and new devices. Looking forward, ZTE will treat fans to giveaways and promotions at branded kiosks during home games at Toyota Center and through in-game activation. ZTE will also be the presenting sponsor of the Rockets upcoming Blacktop Battle and will participate in the Season of Giving community program.

(ZTE Corporation)

ZTE Communications Call for Papers

Special Issue on Software Defined Networks (SDN)

Software Defined Networks (SDN) are considered as a promising technology as for a new generation of networking. It has become of great interest to academic research, network equipment manufacture as well as network carriers and service providers including mobile, data-centre and enterprise networks. The network architecture provides centralized, programmable control-plane and data-plane abstraction, where control and data planes are separated. It also provides the ability to control and manage virtualized resources and networks without requiring new hardware technologies.

SDN is a major shift in networking technology and has attracted major attention from academia, industries and standard organizations. Many works have been carried out on SDN recently. Therefore, it is a good time for excellent papers to be published in a special issue of the journal.

This special issue seeks original articles describing development, relevant trends, challenges, and the best practices in the field of SDN. Position papers, technology overviews, and case studies are also welcome.

Appropriate topics include, but are not limited to

- SDN control plane and management
- Open API for SDN and network programming
- SDN switching technology and OpenFlow
- SDN monitoring and testing
- Network virtualisations
- SDN standardization activities
- Security and QoS support
- SDN applications
- Future network architecture

ZTE Communications (<http://www.zte.com.cn/magazine/English>) is a quarterly peer-reviewed technical journal ISSN (1673-5188) and CODEN (ZCTOAK). The journal focuses on hot topics and cutting edge technologies in the telecom industry. The journal has been listed in Inspec, the Ulrich's Periodicals Directory, Index of Copernicus (IC) and Cambridge Scientific Abstracts (CSA). It is distributed worldwide to telecom operators, science and technology research institutes, and colleges and universities in more than 140 countries.

Submission Guideline:

Submission should be made electronically by email in WORD format to Ms. Zhu Li:

Email: zhu.li1@zte.com.cn;

Editorial Office, 12F Kaixuan Building, 329 Jinzhai Rd, HeFei 230061, PR. China.

Manuscript Submission Due: 25 January, 2014

Acceptance Notification: 1st March, 2014

Final Manuscript Due: 1st April, 2014

Publication date: 25 June, 2014

Guest Editors	Prof. Zhili Sun, CCSR, University of Surrey, z.sun@surrey.ac.uk
	Prof. Kun Yang, CSEE, University of Essex, kunyang@essex.ac.uk
	Prof. Jiandong Li, ISN, Xidian University, jdli@mail.xidian.edu.cn