RESEARCH PAPER

Study on Security Technologies for Wireless Network Integration

Feng Min

(Department of Communication Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract:

The network integration provides users with a new network with long connection time and a high data rate when needed, but it also brings the defects of all the networks that integrate together into the integrated network. This will cause all kinds of existing and some new security problems in the operation of the integrated network. A complete protection based on recovery is proposed in the paper. It uses the public-key algorithm to authorize and private-key algorithm to encrypt the communicating data. This solution can provide the system with reliable security, and avoid Denial of Service (DoS) of the user. This solution has been proposed lately, and we should further identify the correct action of all the layers and figure out how to react when a legal node is framed by multiple malicious nodes.

With the development of mobile communications technologies, the networks are developing into next generation mobile Internet, which connects wireless networks such as the cellular network, Ad Hoc network, Wireless Local Area Network (WLAN) with the Internet to provide services such as "always on-line", a possibly high data rate and dynamic network access. Besides the benefits, it also brings security problems such as confidentiality, access control and entity authentication of roaming subscribers.

At current stage, the study of wireless network integration mainly focuses on integration of any two networks. The main study directions are the integration of the cellular networks and WLAN, as well as that of the cellular and Ad Hoc networks.

Capable of offering high data rates, WLAN is adopted to converge with cellular networks. It is regarded as the high-speed data transmission network at hotspot areas in a cellular network to provide high-speed data services to subscribers. It usually works as the terminal sub-network of cellular networks or an independent network, therefore, only authentication and handover among networks are to be considered. The integration of cellular networks and WLAN mainly refers to the integration between the General Packet Radio Service (GPRS) network and WLAN, as well as between the Universal Mobile Telecommunications System (UMTS) and WLAN. The emphasized point of the integration solutions is routing and handover, and gateway is setup at the network edge to ensure network security.

There are different solutions to integration of the Ad Hoc and cellular networks. For instance, in an Integrated Cellular and Ad Hoc Relaying (iCAR) system, the Ad Hoc network is regarded as a complement to the cellular network to solve the problem of network congestion of hotspots and enhance the spectrum utilization of the system. As for the detailed iCAR system structure, please refer to the documents [1-4]. Having the similar idea to the iCAR system, a Unified Cellular and Ad-Hoc Network (UCAN) uses a proxy machine to receive data in the areas with strong signals when the data rate is decreased, and fulfills high-speed data connection by using IEEE 802.11 protocol[5] that provides high-speed connection to send data to the user. The two systems above provide services to Ad Hoc nodes by the semi-fixed node of centralized control network, with the main purpose to make full use of the resources of centralized networks.

The Cellular Aided Mobile Ad Hoc Network (CAMA) uses the "out-of-band signal" of the cellular network. It uses centralized management mechanism of the cellular network to increase the management and control of the Ad Hoc network and further improve its performance. Details are referred to the document [6]. It is one of the few networks that fully utilize the characteristics of the Ad Hoc network. However, with the introduction of the cellular network for its management, its upper-network is still similar to centralized control networks, except the Ad Hoc network at the bottom level. As for a Multi-hop Cellular Network (MCN), the multi-hop routing access of the Ad Hoc network is introduced into the cellular network through multi-hop routing between nodes. In this way, every node in the network plays a role in data transfer, which reduces the number of base stations and enlarges the coverage of the cellular network[7]. Mobile Assisted Channel Allocation (MACA) has a dynamic channel allocation mechanism. It also

introduces the Ad Hoc transfer technology into the cellular network with fixed base stations. There are detailed descriptions about this integration solution in the document [8]. The main characteristic of the two solutions above is to improve network performance only by appending multi-hop mechanism into network nodes, without adding any management or transfer equipment. However, this characteristic brings the problems of authentication and accounting.

1 Security Problems of Network Integration

Different networks have their own security weaknesses. An integrated network not only carries the security weaknesses of its sub-networks, but also has security weaknesses at the joint parts of different networks.

1.1 Various Network Security Weaknesses

Security measures of the cellular networks such as authentication and authorization have been proved effective, but the data in transmission are unencrypted. Moreover, even CDMA network, which is better than GSM in security guarantee, cannot further provide better security guarantee besides the common security measures such as spread spectrum and scrambling code. Such security measures can only prevent information leakage at low degree such as eavesdropping, but is incapable of preventing security dangers such as channel monitoring and flow testing.

Similar to the cellular network, the WLAN requires authentication for all the nodes that want to access it, otherwise, data from unauthenticated nodes will be prevented from transmission in it. However, data transmitted through the WLAN are also unencrypted as those in the cellular network, and any nodes are capable of receiving information sent by other nodes.

With open architecture, the Internet is vulnerable to malicious attacks. The release of such protocols as Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) provides somewhat security guarantee for the unsafe Internet. IPSec works in two ways as described in the document [9]. IPSec can provide better security by utilizing the tunnel technique. However, the inherent defects of IPSec limit its further application in other networks.

The Ad Hoc network is a distributed system. Either legal network subscribers or malicious invading nodes can access its wireless channels, and all its nodes are not only terminals but also responsible for data transmission without designated security equipment in charge of authentication. Therefore, the security solution for wireless network integration should start at the Ad Hoc network with worst security. Moreover, the solution to inter-network security should especially consider the Ad Hoc network that lacks special security equipment.

1.2 Security Defects of Ad Hoc Network

The special architecture of the Ad Hoc network decides its failure to provide good security guarantee, and makes it vulnerable to either active or passive attacks. Unique properties of the Mobile Ad Hoc Network (MANET), such as open architecture, shared wireless resources, strict resources limitation, and highly dynamic network topology, bring series of new problems to the design of its security solution. Therefore, available security solutions to the wire networks cannot be applied to MANET directly.

There are 4 main security problems. First, wireless links make the Ad Hoc network vulnerable to link-layer attacks, including passive eavesdropping, active pretending, information replay, and information damage. Second, the nodes roaming in the hostile environment (such as at the battlefield) lack of physical protection, which makes the network vulnerable to attacks from inside nodes that have leaked secrets (besides outside nodes). Third, the distributed network architecture often changes the topology and members of the Ad Hoc network. Trust relationship among nodes changes from time to time. Comparing with mobile IP, the Ad Hoc network lacks help from trustful third-party authentication, and accordingly has a central security problem of establishing trust relationship among nodes. Fourth, an Ad Hoc network generally has thousands of nodes, requiring scalable security mechanism.

Another security defect of the Ad Hoc network is also considered here. Because of the open architecture of the Ad Hoc network, all terminals supporting Ad Hoc can access the network, or become part of the network. Therefore, legal subscribers of other networks may become malicious nodes in the Ad Hoc network. For instance, they reject forwarding data due to energy saving concerns, duplicate data before forwarding for certain special purposes, or carry out malicious action aiming to a certain number or cluster. Accordingly, it is necessary to independently consider solutions to inter-network and intra-network security based on the integration of multiple wireless networks.

1.3 Security Problems Brought by Network Integration

An integrated network has both advantages and weaknesses of its member networks. The security defects discussed earlier will more or less affect the security of the integrated network. Besides, an integrated network will definitely face series of new security issues when providing diversified services, such as the safe information exchange between networks.

The Ad Hoc network has no special security authentication centers. It needs further discussion on whether using a substitution to replace the reliable third party in the solution based on certification encryption and authentication, or setting up a special security center for the Ad Hoc network. Besides, the transmission of keys and certificates is difficult for an integrated network. These keys and certificates include the keys and certificates service providers assign to their customers, keys for inter-network authentication, and temporary certificates distributed to the legal customers of a network when they access other networks.

2 Security Solutions to Wireless Network Integration

There are differences in the security solutions to different integrated wireless networks.

The security solutions to networks with centralized control like the cellular network and WLAN are rather simple. Since the security performance of such networks has improved in

practical applications, only authorization and authentication between networks need to be considered. Meanwhile, such networks have special equipment for access and routing as the hardware support for the deployment of the security solution. Therefore, only the authentication for access by the authentication center is necessary, and the security solution to routing is fullfilled on routers. The security solutions of such networks can be easily identified and fulfilled because of their architectures.

The characteristics of Ad Hoc, such as open peer–to–peer network architecture, shared wireless resources, strict resource limitation and highly dynamic topology, decide that after simplifying, the security solutions to the Ad Hoc network can also be applied to other networks with centralized control.

2.1 Classification of Network Integration Solutions

Recently, MANET has received extensive attention due to its self–organization and self–maintenance. When the Ad Hoc network is integrated with the cellular network, it becomes an effective complement to the cellular network. Using the characteristics of the Ad Hoc network, different integration methods can fulfill different functions. For instance, iCAR, UCAN, MCN and CAMA systems are designed to implement different functions.

When networks with big differences are integrated, routing, handover, authentication, and accounting of the integrated network must be implemented on the basis of original routing, handover, authentication and accounting processes of the sub–networks. Comparing with routing and handover, authentication is the prerequisite of normal communications and the base for implementation of all other functions. While authentication is only part of the security issue, a security solution must ensure the security of data exchange during communications.

The solutions to network integration can be classified into 3 types without considering cost. First, the cellular network is treated as the backbone network and the Ad Hoc network as a complementary edge network. This solution makes full use of the frequency resources of the cellular network through the Ad Hoc network. Second, out–of–band signals of the cellular network are used to manage the Ad Hoc network, the local backbone network. On one hand, the strengths of the Ad Hoc network are put into full play and on the other hand, the centralized control of the cellular network help the Ad Hoc network to be more stable. Third, multi–hop routing protocols are introduced into the cellular network to reduce the number of base stations and improve coverage.

2.2 Security Emphases of Network Integration Solutions

Security emphases shall be identified first. As for the first type of network integration, the security emphases are how to let legal customers of the cellular network access Ad Hoc network safely, and how to ensure the security of their communications in the Ad Hoc network. For the second type, the security emphases are how to fulfill security in the Ad Hoc network, and how to transport control messages safely when the cellular network manages the Ad Hoc network. Moreover, the third type requires stricter authentication on each user's identity.

The security emphases can be classified as the safe transmission of signaling and messages, and reliable authentication on users' identity. The solution to the security emphases, plus appropriate system configuration, can basically ensure the information security of users. Since the security problem of signaling and messages is mainly caused by the open architecture of the Ad Hoc network, the working focus should be put on security guarantee of the Ad Hoc network. The public–key protocol using asymmetric encryption technology is one of the defensive security solutions presented by Tseng et al. Combining this protocol algorithm with the method for enforcing correct implementation and multi–protection in the reference document [10] and the method of applying IPSec to provide security guarantee in [11–13], a solution applicable for integrated networks to guarantee the security of signaling and messages is provided here.

2.3 Security Strategy

2.3.1 Brief Introduction of Security Strategy

The security strategy proposed in this paper is as following:

(1) Security guarantee of the entire network is to ensure the security of all layers of the network protocol stack. The security is fulfilled by analyzing security weaknesses of every layer of the protocol stack and enforcing corresponding security measures. Meantime, connection of the layers may also be used to protect the entire protocol stack.

(2) Due to the unpredictability of the attacking ways of unknown attackers, a solution based on such uncertainty is unreliable. Therefore, a better solution to prevent attacks is to study the weaknesses of the protocol itself and enhance reliable implementation of nodes to the protocol specifications.

(3) It is necessary to encrypt data for security. Reliable encryption algorithms are needed for encypting data during transmission to ensure the security of users' data. Currently public–key authentication and private–key encryption are extensively used in security solutions to various networks. Therefore, the public–keys can be used for authentication, and used to be the seed of the private–keys. This helps not only provide reliable security performance, but also offer efficient data encryption during a communication process with a great amount of data and high real time requirement, which meets security requirements from users without bringing too much computing burden for mobile terminals. However, for long–time data connection, how to update the private key for encryption and define the updating period is worth further discussion.

2.3.2 Multi–protection System

For the security of integrated networks, it is very important to fulfill authentication between networks and to ensure the security of the Ad Hoc network. As for various networks with centralized management, authentication between any two networks is quite similar, which is easy to be applied to inter–authentication among multiple networks. Moreover, it is simple to deploy the authentication center and security measures like authentication for the centralized–management network with special routing equipment because a unique core network is responsible for providing services to customers. For instance, the authentication for access and service request can be deployed on routing and switching equipment, that is to say, there is special equipment

to take charge of the system security. The security solution of the Ad Hoc network can't follow such a concept due to its distributed network architecture.

The concept of multi–protection is to improve security performance of the Ad Hoc network through compelling network users to strictly follow protocol specifications. It can also be applied to other networks for security concerns.

Further division of original functions of all the layers helps fulfill multi–protection, that is to say, each function module of every layer has multiple sub–modules that ensure the implementation of multi–protection. For instance, the network–layer security is to ensure that the nodes forwarding messages completely follow indications of the router list, preventing malicious actions such as local duplication and tampering with the next address of a data packet. The link–layer security is to ensure one–hop connection between two communicating nodes.

Using encryption to ensure the security of each module needs long time for authentication and authorization, but shorter time is preferred by users. Therefore, this paper thinks that improving the capability of each module to distinguish between right and wrong operations (that is, to make clear if the operations follow the protocol specifications) can prevent malicious nodes from invading the Ad Hoc network, that is, reduce the damage done by malicious attacks. In this way, when one particular node doesn't follow protocol specifications, other nodes can suspect its identity, make its authentication compulsory, and report their suspects to the trustful center. The trustful center will decrease one grade from the total reliable grades of this node. When the remaining grades reach a certain value, this node will be banned as the forwarding candidate node. It won't get the network service when the grade becomes zero. The near–by nodes can get to know whether its neighbor nodes correctly implement protocol specifications through monitoring data packets in the network. It is worth noting that the trustful center needs to distinguish the suspect reports from multiple nodes to avoid a malicious node's framing a legal one. Besides, self–organization of Ad Hoc should be fully utilized to build the network, which requires any nodes could access the network at any time. This requires the network trust every node fully.

Another model presented here is to treat every mobile node first entering the network as the reliable node with a low reliability grade. Therefore, it has low priority in choosing routes. These nodes are only regarded as end nodes except in some special cases. Correct implementation of protocols will increase the reliability grade of such a node, and once or limited times of erroneous operations will greatly decrease its reliability grade. This method fulfills tolerance on malicious nodes and decreases damage to network by malicious nodes as much as possible.

As for inter–network authentication, different network operators can sign a roaming agreement in advance to ensure their legal subscribers roaming and obtaining services on all the networks. Before accessing to another network and requesting for network services, a subscriber of a network applies to the authentication center of the visiting network by presenting the certification distributed by the authentication center of its home network. Its home and visiting authentication centers exchange authentication to make sure the legal identity of this subscriber. When he wants a service, he is required to sign with his private key to avoid Denial of Service (DoS). The detailed process can be found in the public–key–based protocol part of the document [14].

2.3.3 Data Encryption Technology

Data encryption is just a method used for security protocols. Available public–key algorithms can provide good security, therefore, public–key encryption algorithms are used in this paper to improve reliability of authentication and avoid DoS. However, the use of the public–key encryption algorithms will definitely increase computational complexity of mobile terminals, which is a great challenge to their limited computing capability. In this consideration, this paper suggests using parameters of the public–key algorithms to bring the private–key or private–key–generating–seed at the time of authentication or beginning of communications. This not only ensures information security, but also improves the efficiency of encryption.

3 Key Technologies for Security

3.1 Solutions to Security

Several solutions to security of integrated networks are proposed. For instance, Ala–Laurila et al[15] have presented a structure supporting mobile customers through integration of GSM/GRPS and WLAN. However, the structure doesn't consider bi–interface (GSM/GPRS and WLAN) terminals. WLAN, as the access network, directly connects to the main components of the 3G network (such as the cellular operation center). Two networks share the same resources such as billing system, signaling and transmission system. Luo et al[16] provide enterprises with the Internet roaming solution by integrating 3G system and WLAN. This solution requires placing a large number of servers and gateways at appropriate places. The Virtual Private Network (VPN) provides enterprises with safe connections to 3G system, public and private WLAN.

3.2 Encryption Technologies

Encryption technologies are divided into the private–key encryption technologies and the public– key encryption technologies. The characteristic of private–key encryption is that the same key or the keys identical in essence are used to encrypt and decrypt data. It involves the transmission and storage of the key, and is accordingly hard to be applied to networks with open architecture. On the other hand, public–key encryption requires complex computation, but can offer good security performance because it doesn't involve transmission of the key. Moreover, public–key encryption supports digital signature. Therefore, public–key algorithms can provide security guarantee for authorization and accounting in modern communications.

Presently, all the encryption methods used for the cellular networks belong to the traditional encryption methods, that is, the private–key encryption technology. No matter the sender or the receiver uses the same key for data encryption, user authentication, verification of data integrity and digital signature

during the information exchange process.

3.3 Key Distribution Mechanism

The public–key encryption technology, and IPSec and IKE working principles are used to encrypt data and distribute keys in this paper. The public–key encryption technology used in the process of access and authentication definitely helps improve the security performance. However, the safe distribution of keys needs further discussion. Networks with centralized control have their authentication center, to which a user needs to apply before access the network. The authentication center will issue a private–key to the user, and the key is only known by the center and the user. The center will also broadcast the corresponding public–key to other users of the network. However, if adding one authentication center trustable for all nodes, the distributed Ad Hoc network will fail to make full use of self–organization that is the main purpose of the Ad Hoc network. Therefore, how to introduce public–key encryption into the Ad Hoc network is the focus of future study.

The time for encryption and decryption during data transmission should be reduced in order to support real–time services and lessen the burden of mobile terminals. In this concern, the private– key encryption technology works well. Transmission for private–key is another issue to be considered. For networks with centralized control, private–key can be transmitted at the time of authentication or after public–key encryption to guarantee the security of the private key. The main difficulty lies in the distribution and transmission of the private key in the Ad Hoc network.

This paper suggests using the public–key encryption technology (that is, authentication based on certificates) to fulfill routing security. When prior distribution of a sharing key is unnecessary for network access, certificate–based authentication provides a powerful measure for communication parties to verify entities. It uses certificates to generate digital signature, and supports complex service models. When the public–key–based authentication protocol is used, the verifier must certify the public–key certificate of a communicating entity, besides, computation directly related to the protocol[17]. If certificate–based authentication is used for the Ad Hoc network, the verifier needs to not only make sure if a single certificate is correct (such as certification of certificate signature and legal use time) and will withdraw, but also certify all the certificates on this certificate link. As for authentication for routing, the document [19] can be referred to.

When applying IPSec, the channel model is used to ensure information security for multi–hopping. Since the transmission model is convenient, one–hopping neighbors can be stored in every Ad Hoc node, therefore, information transmission among one–hopping neighbors can utilize the transmission model at low expense.

4 Conclusion

A security framework for next generation networks with integration of different networks is proposed in this paper. This is a recovery–based multi–protection solution using public–key encryption algorithms for authentication and the private key encryption algorithms for data encryption. This solution can provide reliable security of the system and avoid DoS. However, the recovery–based security system is still at the primary stage of research, and it is necessary to identify the correct actions at different layers and figure out the actions taken when a legal node is framed by multiple malicious nodes.

References

[1] Wu H Y, Qiao C M, De S, Tonguz O. Integrated Cellular and Ad–hoc Relay Systems: iCAR[J]. IEEE Journal on Selected Areas in Communications, 2001,19 (10): 2105–2115.
[2] Qiao C M, Wu H Y. iCAR: An Integrated Cellular and Ad–hoc Relay System[C]// Proceedings of IEEE Ninth International Conference on Computer Communication and Network. Oct 16–18, 2000, Las Vegas, NV, USA. Los Alamitos: IEEE Computer Society Press, 2000:154–161.
[3] Wu H Y, Qiao C M. Quality of Coverage: A New Concept for Wireless Networks[J]. ACM Computer Communication Review (CCR), 2002, 32(1).
[4] Wu H Y, Qiao C M. Modeling iCAR via Multi–dimensional Markov Chains[J]. Mobile Networks and Applications, 2003, 8(3): 295–306.
[5] Luo Haiyun, Ramachandran R, Prasun S, et al. UCAN: A Unified Cellular and Ad Hoc Network Architecture[C]//Proceedings of Annual International Conference on ACM Mobile Computing and Communications (MOBICOM 2003). Sep 14–19, 2003, San Diego, CA, USA. New York, NY, USA: ACM Press, 2003: 353–367.
[6] Bhara B, Wu Xiaoxin, Lu Yi, et al. Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad Hoc Network (CAMA)[J]. Mobile Networks and Applications, 2004, 9(4): 393–408.
[7] Lin Y D, Hsu Y C. Multihop Cellular: A New Architecture for Wireless Communications [C]// Proceedings of IEEE INFOCOM, Vol 3. Mar 26–30, 2000, Tel Aviv, Israel. Piscataway, NJ, USA: IEEE, 2000: 1273–1282.
[8] Wu Xiaoxin, Biswanath M, Chan S H. MACA—An Efficient Channel Allocation Scheme in Cellular Networks[C]//Proceedings of Global Telecommunications Conference (GLOBECOM ´ 00), Vol 3. Nov 27–Dec 1, San Francisco, CA, USA. Piscataway, NJ, USA: IEEE, 2000: 1385–1389.
[9] Elkeelany O, Matalgah M M, Sheikh K P, et al. Performance Analysis of IPSec Protocol: Encryption and Authentication[C]//Proceedings of IEEE International Conference on Communications (ICC 2002), Vol 2. April 28–May 2, New York, NY, USA. Piscataway, NJ, USA: IEEE, 2002: 1164–1168.
[10] Yang Hao, Luo Haiyun, Ye Fan, et al. Security in Mobile Ad Hoc Networks: Challenges and Solutions[J]. IEEE Wireless Communications, 2004,11(1): 38–47.
[11] Assaf N, Luo Jijun, Dillinger M, et al. Interworking Between IP Security and Performance Enhancing Proxies for Mobile Network[J]. IEEE Communications Magazine, 2002, 40(5): 138–144.
[12] Qu Wei, Srinivas S. IPSec–Based Secure Wireless Virtual Private Network[C]// Proceedings of Military Communications Conference (MILCOM 2002), Vol 2. Oct 7–10, Anaheim, CA, USA. Piscataway, NJ, USA: IEEE, 2002: 1107–1112.
[13] DaSilva L A, Midkiff S F, Park J S, et al. Network Mobility and Protocol Interoperability in Ad Hoc Networks[J]. IEEE Communications Magazine, 2004, 42(11): 88–96.
[14] Tseng Yunmin, Yang Chouchen, Su Jiannhaur. Authentication and Billing Protocols for the Integration of WLAN and 3G Networks[J]. Wireless Personal Communications, 2004, 29(34): 351–366.
[15] Ala–Laurila J, Mikkonen J, Rinnemaa J. Wireless LAN Access Network Architecture for Mobile Operators[J]. IEEE Communications Magazine, 2001, 39(11): 82–89.
[16] Luo H, Jiang Z, Kim B J, et al. Integrating Wireless LAN and Cellular Data for the Enterprise[J]. IEEE Internet Computing, 2003, 7(2): 25–33.
[17] Salgarelli L, Buddhikot M, Garay J, et al. Efficient Authentication and Key Distribution in Wireless IP Networks[J]. IEEE Wireless Communications, 2003, 10(6): 52–61.
[18] Grecas C F, Maniatis S I, Venieris I S. Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration[J]. Mobile Networks and Applications, 2003, 8(2): 145–150.
[19] Kong Jiejun, Zerfos P, Luo Haiyun, et al. Providing Robust and Ubiquitous Security Support for Mobile Ad–hoc Networks[C]//Proceedings of Ninth International Conference on Network Protocols. Nov 11–14, 2001, Riverside, CA, USA. Los Alamitos, CA, USA: IEEE Computer Society Press, 2001: 251–260.

Manuscript received: 2005–10–27

Biography

Feng Min is studying for her Master's degree at Department of Communication Engineering of Nanjing University of Posts and Telecommunications. Her research direction is the Ad Hoc network and its security.