Key Technologies of Wireless Heterogeneous Network Security

Wu Meng, Ji Lina, Wang Kun
(Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract:
Convergence and collaboration of heterogeneous networks in the next generation public mobile networks will be a subject of universal significance. Convergence of heterogeneous networks, as an effective approach to improve the coverage and capacity of public mobile network, to enable communication services, to provide Internet access and to enable mobile computing from everywhere, has drawn widespread attention for its good prospects in application. Construction of security system for wireless heterogeneous networks and development of new security models, key security techniques and approaches are critical and mandatory in heterogeneous networks development. Key technology of wireless heterogeneous networks security covers security routing protocol, access authentication, intrusion detection system, cooperative communication between nodes, etc.

Heterogeneous network convergence, which means different types of networks are converged to provide diversified services in a common network platform, is a novel concept and a goal we have pursued for a long time. One main feature of 4G networks is their ability to provide interoperability between multiple wireless access technologies. The Wireless Local Area Network (WLAN)–3G convergence and the Ad hoc cellular convergence are important forms of wireless heterogeneous network convergence. The network convergence technologies can greatly improve the performance of cellular networks, and make it possible for the networks to introduce new services while supporting traditional services. They have become a hotspot in the next generation wireless mobile networks supporting heterogeneous interconnection and cooperation. In recent years, heterogeneous network convergence has attracted more and more attention of the industry and has been extensively studied[1–6].

Like in other communication networks and computer networks, information security is an important issue that must be addressed in the development of wireless heterogeneous networks. The heterogeneous networks integrate the advantages of all involved networks, and their shortcomings as well. With respective to security, the converged networks have to face a series of new security problems, such as intra–network security, seamless connectivity of existing security protocols and security requirements that arise from new service providing, in addition to respective security problems of all original networks. Therefore, in the development of wireless heterogeneous networks, an important task is to work out highly–flexible, invulnerable security models, and develop key security technologies and approaches.

Although considerable efforts have been made in the research of the security of traditional Global System for Mobile communications (GSM) networks, WLANs and Ad hoc networks, and the research results have been applied in practice, the research on the security of heterogeneous networks has just started. This paper will discuss security technologies of wireless heterogeneous networks in the next generation public mobile network environment, including routing protocol, access authentication, intrusion detection, encryption/decryption and cooperative communications between nodes, for the purpose of improving the security of wireless heterogeneous networks.

1 Security Solution for Ad Hoc Network

Due to the inherent features of Ad hoc networks, such as open media, dynamic topology, distributed cooperation and limited energy, any user, either legal network user or malicious intrusion node, can access to their radio channels. Hence, Ad hoc networks are vulnerable to various attacks, and they face severer security problem than other wireless networks. So far, there are many descriptions of the security of Ad hoc networks[7–11].

The attacks against Ad hoc networks can be classified into two categories: active and passive. Accordingly, there are two main kinds of defense strategies: proactive and reactive. The first kind is

This work is supported by the Jiangsu Natural Science Foundation under Grant No. BK2007236, and Jiangsu Six–Categories Top Talent Fund under Grand No. SJ207001.

used to protect the network from attacks, and the technologies involved include authentication, encryption algorithm and key distribution. The second one aims to detect the malicious nodes or intruders to remove them or prevent them from entering the network. The technologies in this kind include intrusion detection (architecture monitoring, data collection, and proper response to attacks). Documents [12] and [13] discuss group key distribution technologies in Ad hoc networks without Certification Authority (CA). Document [12] also studies the effectiveness of key establishment. However, the key distribution schemes discussed in the two Documents are only applicable to small Ad hoc networks where any two nodes can directly communicate with each other. Another key distribution scheme is called threshold cryptosystem, where the distributed certification function of the CA is cooperatively completed by multiple nodes in the network. This scheme enhances the network's robustness because its key management system will not be destroyed due to capture of one or a few intrusion nodes. Document [14] proposes a decentralized key distribution mechanism. This mechanism assumes each mobile node has a reliable node group nearby. Two nodes exchange their public keys by combining related information of respective node groups, thus the reliability of obtained keys being greatly enhanced. But in this mechanism, key distribution may still fail, especially in large Ad hoc networks.

The routing security is another important issue in Ad hoc networks. Among the existing secure routing schemes, if we want to take proactive defense strategies, the digital signature can be used to authenticate the invariable part of a message, and the Hash link can be used to encrypt the hop information. In this way, the intermediate malicious nodes are prevented from adding false routing information[15]. Another way is to bind IP address with Media Access Control (MAC) address, allowing authentication to be done in the link layer, thus improving the security[16]. If reactive defense strategies are adopted, the intrusion detection method can be used, where each node has its own Intrusion Detection System (IDS) to monitor its ambience. Besides, the neighboring nodes can exchange their intrusion information. No doubt, a successful IDS is very complex, and depends on the degree of trust between neighboring nodes. The watchdog scheme can protect the packet data from being dropped, modified or added with false routing information during its forwarding[17]. But how to improve the security of such routing protocols as Ad hoc On–Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) is still under active research[18–19]. Above all, the poor security of Ad hoc network arises from its non–centric architecture, which can be improved with a distributed security mechanism. However, such problems as increasing network overhead, prolonged decision time and inaccurate judgment still perplex Ad hoc networks.

2 Security Solution for Heterogeneous Network

2.1 Security Architecture

The current security research focuses on two types of convergence networks: GSM/General Packet Radio Service (GPRS)–WLAN and 3G (especially Universal Mobile Telecommunications System (UMTS))–WLAN. Document [20] discusses the GSM/GPRS–WLAN convergence architecture supporting mobile subscribers, where WLAN is regarded as the access network of 3G network and is directly connected to the elements of 3G network (e.g. cellular core). Both WLAN and 3G networks are centralized, enabling their common resources to be easily shared during billing, signaling and transmission, and facilitating security management. But this solution does not take into account dual–mode terminals (GSM/GPRS and WLAN). Document [21] presents a 3G–WLAN integrated architecture to provide an Internet roaming solution for enterprises. In this architecture, the security management is achieved by installing servers and gateways in proper places. Another solution is Virtual Private Network (VPN) program, which can be used to provide the enterprises with secure connection to 3G networks, public WLANs and private WLANs. Among 3rd Generation Partnership Project (3GPP)'s specifications, 3GPP TS23.234 describes the internetworking architecture between 3G and WLAN, where internetworking elements such as Packet Data Gateway (PDG) and WLAN Access Gateway (WAG) are added[22]; 3GPP TS33.234 further specifies the security requirements for 3G–WLAN internetworking, which security mechanisms are based on existing UMTS Authentication and Key Agreement (AKA) mode[23].

As to the security of Ad hoc cellular convergence network, Document [24] proposes an architecture which adopts the out–of–band signaling and the central management mechanism of cellular network to improve the quality of network control and management, thus improving the routing and security performance of Ad hoc network. But this architecture is only for Ad hoc network, taking no account of the security of cellular network and inter–network security.

Generally, in constructing a comprehensive security architecture for wireless heterogeneous network, three basic principles should be followed: First, the architecture should guarantee security at each layer as the wireless heterogeneous network's protocol structure complies with the Open Systems Interconnection (OSI) system; second, the architecture should be based on the MAC layer security solutions of all wireless access sub–networks in order to achieve seamless connectivity between security protocols; third, the architecture should adapt itself to the services, technologies and development trend of wireless heterogeneous networks, allowing seamless transition from existing security solutions.

Therefore, the security management system that integrates centralized control and distributed agent can be used. In such a system, security agents will be configured, which conduct centralized control over the distributed networks in terms of access authentication, key distribution and update, routing security guarantee and intrusion detection.

2.2 Secure Routing Protocol

Routing security plays a leading role in

the security of heterogeneous networks. In heterogeneous networks, routing protocols have to discover both mobile nodes and base stations. Most of the existing routing protocols only pay attention to route selection and selection strategies, and only a few of them cover security issue.

In the United Cellular Access Network (UCAN)[25], the security problem mainly lies in the authentication of legality of intermediate nodes in the data forwarding routing. When a routing request message is sent from the destination node to the base station, a single keyed message authentication code is piggybacked. The MAC authenticates the relay path so that the base station can precisely keep track of the number of data flows that are relayed by each proxy or relay node. Meanwhile, each user has a secret key given by the base station. The UCAN tries to prevent a private host from deleting legitimate hosts or enable the forwarding function of unauthorized hosts. It effectively prevents selfish nodes. But when collision occurs, its defense capability will decrease. Document [26] suggests a new routing algorithm against malicious attacks. Aiming to protect the routing mechanism and routing data, the authors of the Document develop a trust model for convergence network, and propose a security performance analysis mechanism. The core idea of this routing algorithm is to select a path (to the base station) with the largest throughput for each host. Each host periodically detects the throughputs of neighbor nodes and selects the node with the largest throughput for data forwarding. The goal of the algorithm is to identify the attack types of malicious nodes and to provide effective detection to avoid them.

The research on secure routing protocols should include at least two parts: routing between base station and mobile terminal and routing between any two mobile terminals (e.g. Ad hoc network routing). As existing routing protocols for heterogeneous networks are mainly extensions of those routing protocols used in Ad hoc networks, the study of their security should extend to the security of the protocols for Ad hoc networks. Moreover, research results in Ad hoc secure routing can be referred. The SPRITE[27], a simple, cheat–proof, credit–based system, is obviously a good start for such a research. The SPRITE itself needs a Credit Clearance Service (CCS), which is independent of Ad hoc network, for maintaining credit balance between nodes and stimulating intermediate nodes to forward data. The CCS, on the other hand, has to obtain complete routing information between any two nodes. This can be easily achieved in heterogeneous networks as there are fixed infrastructures, such as base stations.

In addition, the security of routing protocols for heterogeneous networks should be based on authentication supported by service providers. This requires the security system and encryption technologies of fixed infrastructures to be enhanced so that the nodes can access to heterogeneous networks and be authenticated.

2.3 Access Authentication

Most of existing authentication systems, for example, Kerberos and X.509, are for centralized networks because they require centralized authentication bodies such as certificate issuing center or CA. Ad hoc networks are characterized as distributed, mobile and without any fixed infrastructure, and their topologies keep changing dynamically. As a result, only the distributed authentication mode is applicable. For heterogeneous networks, the introduction of cellular base stations solves the inherent problem of Ad hoc network, i.e. no fixed infrastructure. Meanwhile, they can make full use of the advantages of Ad hoc network; and they can develop their access authentication systems based on the characteristics of centralized network and distributed network. Document [28] discusses the secure authentication in case WLAN nodes access 3G network. It proposes a 3G–WLAN trust model to strictly maintain the trust relation between all participants in the 3G–WLAN integrated network; hence the access authentication procedure is strengthened, and fraudulent access authentication requests are prevented from entering 3G network.

In Ad hoc cellular converged networks, access authentication varies with the convergence modes. There are three modes for convergence of Ad hoc network and cellular network. In the first mode, the converged system is based on cellular technologies, but aided by Ad hoc network, and its access authentication focuses on how to let legal Ad hoc network users to securely access to the cellular network. In the second mode, the system is based on Ad hoc network and aided by cellular technologies, and the purpose of its access authentication is to achieve internal security within Ad hoc network and to securely transmit control information when the cellular network manages Ad hoc network. In fact, such a system can directly adopt the same access authentication procedure as the cellular network, as in the case of Cellular Aided Mobile Ad hoc network (CAMA). The third mode is a hybrid mode, which requires strict measures to authenticate each user's ID. The authentication of user ID in heterogeneous networks includes two parts: authentication between Ad hoc network and the centralized network and authentication between any two centralized networks.

For complex heterogeneous networks, the traditional access authentication is just the first defense. To cope with those malicious nodes that have already wormed themselves into the network, more drastic measures have to be taken. One good solution is to establish an authentication mechanism based on reputations of base stations and nodes. Completely depending on cooperation of widely–distributed nodes to maintain normal communication, the access network at the end of the cellular system has to refuse the access of malicious nodes on one hand, and evaluate reputation of each node on the other to ensure that the access of legal nodes will not be refused due to frame–up of malicious nodes. With the reputation–based authentication mechanism, the availability of network resources can be maximized.

In heterogeneous networks, both base stations and mobile nodes can act as reputation evaluation centers, thus a base station–centered evaluation system aided by mobile nodes is established. Document [29] proposes another access authentication method, where a node is pre–authenticated when accessing to

the network, and then the base stations and other mobile nodes in the network trace its behaviors. Once any misbehavior is found, its credential will be re–evaluated, and re–authentication will be required.

2.4 Intrusion Detection

Heterogeneous networks quite differ from wired networks, so the IDSs developed for wired networks cannot be directly applied in wireless heterogeneous networks. Firstly, traditional IDSs largely depend on monitoring and analyzing real–time services of the entire network, but in heterogeneous networks, the mobile environment can only provide the local data related to direct wireless communication, so their IDSs have to use the incomplete information to implement intrusion detection. Secondly, the mobile networks have relatively low–rate links and limited bandwidths and their nodes must be powered by batteries. These features impose high requirements on communication. Consequently, mobile networks cannot use those communication protocols defined for wired IDSs. Thirdly, the quickly changing topology of mobile network fuzzes the boundary between normal operations and abnormal operations. The node that sends error information may be a captured node or a node which has not been timely synchronized due to quick move. As a result, for a common IDS it is hard to tell real intrusion from temporary system fault. A good approach is to develop a scalable multi–layer integrated intrusion detection system based on the characteristics of heterogeneous networks.

Currently, two IDSs are highly praised: the distributed IDS based on mobile agent technology[30] and the distributed IDS for Ad hoc network[31]. The core of the former is mobile agent modules, which are limited in number and effectively distributed into different nodes according to their functions to implement different intrusion detection tasks. The detection result will be finally implemented by an execution module. As the number of mobile agents considerably decreases, the network cost using this IDS is much lower than when other IDSs are used.

The distributed IDS for Ad hoc network requires all nodes in the network to participate in intrusion detection and response. Each node is configured with an IDS agent that adopts anomaly detection technology. When one node reports an anomaly, the neighboring DIS agents will cooperate with each other to initiate global intrusion detection and response. Based on this IDS, Document [32] suggests a cluster–based multi–layer cooperative IDS. Any node in a cluster (including cluster head, deputy cluster head and gateway nodes) independently runs its own IDS, monitors local activities and participates in local intrusion detection. If a node (deputy cluster head or gateway node) detects an anomaly or a suspect but cannot be sure whether it is attacked, it makes a request to the cluster head, asking for global cooperative detection. Upon receiving such a request, the cluster head checks the states of all nodes' IDSs and then determines if any of them is suffering from attack. This IDS can be introduced into heterogeneous networks because the base station with centralized management function can act as the cluster head to coordinate the detection of other nodes.

In terms of the security of Ad hoc cellular converged network, the CAMA architecture suggests a solution for intrusion detection. When detecting an intrusion node, a CAMA agent will broadcast the information within the entire network through the base station. The main purpose of intrusion detection in the CAMA is to solve the routing security problem resulted from the false position information which is intentionally provided by a node. When a node finds that the next–hop node in the routing table received from the base station does not exist, it reports a routing error to the base station. The CAMA agent then finds out the malicious node and expels it from the network.

As for detection methods used in IDSs, the Artificial Immune System (AIS) combines two methods, i.e. anomaly detection and misuse detection, to find out the heterogeneity. For instance, S. Forrest and J. O. Kephart design an AIS for data detection, while Kephart uses the AIS to detect the virus. Therefore, the AIS theory, as well as the gene selection technique, can be used to design an intrusion detection model.

2.5 Cooperative Communication between Nodes

In heterogeneous networks, some problems need urgent solutions. For example, how to ensure the privacy of contents during their transmission through relay nodes of Ad hoc network, how to guarantee the security of Ad hoc network, the least secure network in heterogeneous networks, and protect it from attacks by malicious nodes and selfish nodes. To solve these problems, it is required to design an incentive strategy which can not only prevent attacks from malicious nodes and stimulate selfish nodes to participate in cooperation, but also ensure the privacy of contents during their transmission.

The existing incentive schemes can be roughly classified into two types: reputation (or detection) based and market (or charging) based.

In the reputation based system, the node observes the behaviors of other nodes and takes actions accordingly: reward the cooperative behaviors or punish the non–cooperative ones. The node can use a "watchdog" to find out whether another node forwards packets, thus avoiding misbehaving nodes in routing selection. Meanwhile, the source node can use the pathrater[33] to select the most reliable route for packet transmission. The "Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks" (CONFIDANT)[34] system is a reputation system used to resist the

denial of service attack. If a node does not forward its neighbor's packets, it will be regarded as non–cooperative, and its reputation will be broadcast in the network. The CORE[35] scheme introduces three types of reputation: subjective reputation, indirect reputation and functional reputation. The weight of the three types of reputation is used to determine whether a node is cooperative or not as well as to avoid the attacks of malicious nodes. The Secure and Objective Reputation–based Incentive (SORI)[36] scheme aims to avoid the behavior of refusal of forwarding. It uses a mechanism similar to watchdog to monitor the behaviors and maintains the packet forwarding ratio of the node, i.e. the ratio of the number of forwarded packets to the number of received packets.

Another type of incentive cooperative schemes is market based. In this type, each node gets paid from its forwarding operations, and in return, it must pay for transmission of its own data. One virtual currency, called Nuglets[37], is used as the unit of per hop charge to simulate the cooperation in transmission. In the scheme presented in Document [38], the node can get rewards from the sender each time after it forwards the data. This scheme requires a forgery–proof device to be installed at each node, as in the SIP[39] protocol, so as to ensure the charges to accurately added or deducted. The SPRITE scheme does not need any forgery–proof hardware. Instead, it uses a security protocol to manage the charges. The common feature of the two abovementioned incentive schemes is a fixed price paid to all nodes in the network for forwarding the same packet. In contrast, the iPASS[40] scheme runs Vickery auction in the router to decide bandwidth assignment and price.

Security is the most critical problem in incentive schemes. To ensure security in cooperation between nodes, not only should selfish and malicious nodes be coped with, but also attacks of other kinds have to be prevented. The refusal of forwarding is just a type of misbehavior. There are many other routing–related attacks which should be given more attention to, such as black hole attack, gray hole attack and worm hole attack. Therefore, the incentive schemes need extra devices or mechanisms to resist these attacks, leading to a more complex system and more centralized services. For example, in the SIP scheme, a key establishment device is required, and each node needs a security module; in the SORI scheme, Hash link–based authentication is needed for broadcast reputation evaluation; in the SPRITE scheme, the RSA signature of each data packet has to be verified and stored; the Stub Ad hoc network adopts encryption technology in public key; and in the CASHnet, a public key based facility rather than direct key conversion is required due to open environment. The introduction of digital signature prevents the packets from being secretly modified and allows the original packet and forwarding nodes to be uniquely identified, so invalid packets (e.g. unpaid) will not be forwarded. In this way, rewards are safely allocated.

The incentive schemes without extra devices are vulnerable. In the CONFIDANT scheme, a malicious node can send error information to affect the behaviors of non–malicious nodes because no mechanism is available for verifying the reliability of behaviors in received information. As a result, the nodes are vulnerable to Sybil attack. Besides, there is not a salvation mechanism for misbehaving nodes. The charging system in the iPASS scheme is not integrated with secure trade. Recent research is mainly based on the gambling theory and includes the market element because all network functions rely on the contributions of all participants. The nodes have to forward each other's packets to ensure multi–hop communication. In this case, the important thing is not to design cooperative mechanisms, but to balance packet forwarding.

Some incentive schemes take into account security issue without extra devices. For example, the CORE scheme uses its own security mechanism to resist attacks. The negative evaluation of reputation will not be broadcast between nodes, so one node will not maliciously lower the reputation of another node. The reputation system of CORE allows the nodes in Mobile Ad hoc Network (MANET) to gradually isolate those selfish nodes. When the reputation of a node reduces to a value lower than the pre–set threshold, its services will be interrupted.

3 Conclusions

Heterogeneous network convergence is of great significance in the future network development. Now its theories are gradually worked out and its application is continuously extended. With the convergence technology, the wireless and wired networks can be unified in the Next Generation Network (NGN) platform. Being an important evolution to future wireless mobile network, wireless heterogeneous networks have good prospects in both application and market, and they can bring huge economic and social benefits.

On the other hand, the information security is an important issue that must be addressed in the development of wireless heterogeneous networks. With the extension of network application and the diversity of access modes, the attacks multiply. The security plays a crucial role in each key aspect of heterogeneous networks, including routing, authentication, billing, cooperation between nodes and intrusion detection, which are all vulnerable. Currently, the research on the security of wireless heterogeneous networks just starts. Although achievements have been obtained in some aspects of security, there are still many security problems to be solved because of the extreme complicacy of heterogeneous networks.

Therefore, regarding the information security of wireless heterogeneous networks, it is quite important to conduct a comprehensive and systematical research on the key technologies and management system for convergence and interconnection of different networks, and study the individual and common security problems of all involved networks. By extensively studying and applying security mechanisms and protocols, a new active defense system should be developed to achieve the ultimate goal of information security: reliable, controllable and available.

References

[1] INOUE M, MAHMUD K, MURAKAMI H, et al. Novel out–of band signaling for seamless internetworking

between heterogeneous networks [J]. IEEE Wireless Communications, 2004, 11(2): 56–63.
[2] LIN Y D, HSU Y C. Multihop cellular: a new architecture for wireless communication [C]// Proceedings of the Conference on Computer Communications (Infocom'00): Vol. 3, Mar 26–30, 2000, Tel Aviv, Israel. Piscataway, NJ, USA: IEEE, 2000: 1273–1282.
[3] AGGELOU G N. An integrated platform for ad hoc GSM cellular communications [M]// Ilyas m. Handbook of Ad Hoc Wireless Networks. Boca Raton, FL, USA : CRC Press, 2002.
[4] ZHAO DONGMEI, TODO T D. Real–time traffic support in relayed wireless access networks using IEEE 802.11 [J]. IEEE Wireless Communications, 2004, 11(2): 32–39.
[5] WEI Hungyu, GITLIN R D. Two–hop–relay architecture for next–generation WWAN/WLAN integration [J]. IEEE Wireless Communications, 2004, 11(2): 24–30.
[6] McNAIR J, FANG Zhu. Vertical handoffs in fourth–generation multinetwork environments [J]. IEEE Wireless Communications, 2004, 11(3): 8–15.
[7] KARPIJOKIV. Security in ad hoc network [EB/OL]. http//www.tcm.hut.fi/Opinnot/Tik–110.501/2000/papers.
[8] LUO Haiyun, ZERFOS P, KONG Jiejun. Self–securing ad hoc wireless networks [C]// Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02), Jul 1–4, 2002, Taormina, Italy. Piscataway, NJ, USA: IEEE 2002: 567–574.
[9] PAPADIMITRATOS P, HAAS Z J. Secure routing for mobile ad hoc networks [C]// Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02), Jan 27–31, 2002, San Antonio, TX, USA. 2002: 27–31.
[10] DENG Hongmei, LI Wei, AGRAWAL D P. Routing security in wireless ad hoc networks [J]. IEEE Communication Magazine, 2002, 40(10): 70–75.
[11] AURA T, MAKI S. Towards a survivable security architecture for ad hoc networks [EB/OL]. http://research.microsoft.com/users/tuomaura/Publications/aura–mak–protocols 01.pdf.
[12] ASOKAN N, GINZBOORG P. Key agreement in ad–hoc network [J]. Computer Communications, 2000, 23(17): 1627–1637.
[13] HIETALAHTI M. Key establishment in ad–hoc network [EB/OL]. http://www.camars. kaist.ac.kr/hyoon/courses/cs710_2002_fall/2002cas/security/papers.
[14] HUBAUX J P, BUTTYAN L, CAPKUN S. The quest for security in mobile ad hoc network [C]// Proceedings of 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing in MOBIHOC' 01, Oct 4–5, 2001, Long Beach, CA, USA. New York, NY, USA: ACM, 2001: 146–155.
[15] ZAPATA M G, ASOKAN N. Securing ad hoc routing protocols [C]// Proceedings of ACM Workshop on Wireless Security (WiSe'02), Sep 28, 2002, Atlanta, GA, USA. New York, NY, USA: ACM, 2002: 1–10.
[16] BINKLEY J, TROST W. Authenticated ad hoc routing at link layer for mobile systems [J]. Wireless Networks, 2001, 7(2): 139–145.
[17] MARTI S, GIULI T, LAI K, at al. Mitigating routing misbehavior in mobile wireless networks [C]// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM' 00), Aug 6–11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 255–265.
[18] BUCHEGGER S, Le BOUDEC J V. Performance analysis of the confident protocol (cooperation of nodes: Fairness in dynamic ad–hoc networks) [C]// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM' 00), Aug 6–11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 226–236.
[19] WANG Weichao, YI Lu, BHARGAVA B K. On vulnerability and protection of ad hoc on–demand distance vector protocol [C]// Proceedings of International Conference on Telecommunication (ICT'03): Vol. 1, Feb 23–Mar 1, 2003, Paris, France. Piscataway, NJ, USA: IEEE, 2003: 375–382.
[20] Ala–LAURILA J, MIKKONEN J, RINNEMAA J. Wireless LAN access network architecture for mobile operators [J]. IEEE Communications Magazine, 2001, 39(11): 82–89.
[21] 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.
[22] 3GPP TS 23.234 V6.1.0. 3GPP System to WLAN Interworking; System Description [S].
[23] 3GPP TS 33.234 V1.0.1. 3G Security: Wireless Local Area Network (WLAN) Interworking Security [S].
[24] BHARGAVA 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.
[25] LUO H, RAMJEE R, SINHA P, et al. UCAN: a unified cellular and ad hoc network architecture [C]// Proceedings of 9th Annual International Conference on Mobile Computing and Networking (MOBICOM' 03), Sep 14–19, 2003, San Diego, CA, USA. New York, NY, USA: ACM, 2003: 353–367.
[26] CARBUNAR B, IOANNIDIS L, Nita–ROTARU C. JANUS: Towards robust and malicious resilient routing in hybrid wireless networks [C]// Proceedings of the ACM Workshop on Wireless Security (WiSe' 04), Oct 1, 2004, Philadelphia, PA, USA . New York, NY, USA: ACM, 2004: 11–20.
[27] ZHONG S, CHEN J, YAN Y R. Sprite: a simple, cheat–proof, credit–based system for mobile ad–hoc networks [C]// Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03): Vol. 3, Mar 30–Apr 3, 2003, San Francisco, CA, USA. New York, NY, USA: IEEE, 2003: 1987–1997.
[28] DURRESI A, EVANS L, PARUCHURI V, et al. Secure 3G user authentication in ad hoc serving networks [C]// Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES'06), Apr 20–22, 2006, Vienna, Austria. Los Alamitos, CA, USA: IEEE Computer Society, 2006: 488–495.
[29] ABOUDAGGA N, REFAEI M T, ELTOWEISSY M, et al. Authentication protocols for ad hoc networks: taxonomy and research issues [C]// Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks (Q2SWinet '05), Oct 13, 2005, Quebec, Canada. New York, NY, USA: ACM, 2005: 96–104.
[30] KACHIRSKI O, GUHA R. Intrusion detection using mobile agents in wireless ad hoc networks [C]// Proceedings of IEEE Workshop on Knowledge Media Networking (KMN'02), Jul 10–12, 2002, Kyoto, Japan. Piscataway, NJ, USA: IEEE, 2002: 153–158.
[31] ZHANG Y, LEE W, HUANG Y A. Intrusion detection techniques for mobile wireless networks [J].Wireless Networks, 2003, 9 (5): 545–556.
[32] GEVARYAHU R, YAROS B. Misuse Detection and Prevention in Ad–hoc Networks [EB/OL]. http://www.seas.upenn.edu/~ cse400/CSE400_2004_2005/18writeup.pdf.
[33] MARTI A, GIULI T J, LAI K, et al. Mitigating routing misbehavior in mobile ad hoc networks [C]// Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MOBICOM' 00), Aug 6–11, 2000, Boston, MA, USA. New York, NY, USA: ACM, 2000: 255–265.
[34] BUCHEGGER S, Le BOUDEC J Y. Performance analysis of the CONFIDANT protocol (Cooperation of nodes–fairness in dynamic ad–hoc networks) [C]// Proceedings of Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '02), Jun 09–11, 2002, Lausanne, Switzerland. 2002: 80–91.
[35] MICHIARDI P, MOLYA R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks [C]//Proceedings of IFIP Communication and Multimedia Security Conference (CMS'2002), Sep 26–27, 2002, Portoroz, Slovenia. 2002: 107–121.
[36] HE Q, WU D, KHOSLA P. SORI: a secure and objective reputation–based incentive scheme for ad hoc networks [C]// Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'04): Vol. 2, Mar 21–25, Atlanta, GA, USA. Piscataway, NJ, USA: IEEE, 2004: 825–830.
[37] BUTTYAN L, HUBAUX L P. Nuglets: a virtual currency to stimulate cooperation in self–organized ad hoc networks [R]. Technical Report DSC/2001/001, Lausanne: Swiss Federal Institute of Technology, 2001.
[38] BUTTYAN L, HUBAUX J P. Stimulating cooperation in self–organizing mobile ad hoc networks [J].ACM/Kluwer Mobile Networks and Applications, 2003, 8 (5): 579–592.
[39] ZHANG Y C, LOU W J, FANG Y G. SIP: a secure incentive protocol against selfishness in mobile ad hoc networks [C]// Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'04): Vol. 3, Mar 21–25, 2004, Atlanta, GA, USA. Piscataway, NJ, USA: IEEE, 2004: 1679–1684.
[40] CHEN K, NAHRSTED T. iPass: an incentive compatible auction scheme to enable packet forwarding service in MANET [C]//Proceedings of 24th International Conference on Distributed Computing Systems (ICDCS'04), Mar 23–26, 2004, Tokyo, Japan. Piscataway, NJ, USA: IEEE, 2004: 534–542.

Biographies

Wu Meng

Wu Meng is a professor and doctoral advisor at the College of Telecommunications and Information Engineering of Nanjing University of Posts & Telecommunications. His research interests include wireless communications and information security. Up to now, he has published over 70 papers and his 2 invention patents have been granted nationally.

Ji Lina

Ji Lina is a graduate student at the College of Telecommunications and Information Engineering of Nanjing University of Posts & Telecommunications. Her research interests include wireless communications and information security.

Wang Kun

Wang Kun is a PhD candidate at the College of Telecommunications and Information Engineering of Nanjing University of Posts & Telecommunications. His research interests include wireless communications and information security.