Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2009, Article ID 532434, 3 pages
doi:10.1155/2009/532434

Editorial

Wireless Network Security

Yang Xiao,[1] Hui Chen,[2] Shuhui Yang,[3] Yi-Bing Lin,[4] and Ding-Zhu Du[5]

[1] *Department of Computer Science, University of Alabama, P.O. Box 870290, Tuscaloosa, AL 35487-0290, USA*
[2] *Department of Mathematics and Computer Science, Virginia State University, Petersburg, VA 23806, USA*
[3] *Department of Math, Computer Science and Statistics, Purdue University, Calumet, 2200 169th Street, Hammond, IN 46323, USA*
[4] *Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu 300, Taiwan*
[5] *Department of Computer Science, University of Texas at Dallas, Richardson, TX 75083, USA*

Correspondence should be addressed to Yang Xiao, yangxiao@ieee.org

Received 13 December 2009; Accepted 13 December 2009

Wireless networking has been enjoying fast development, evidenced by wide deployments of many wireless networks of various sizes, such as wireless personal area networks (WPANs), local area networks (WLANs), metropolitan area networks (WMANs), and wide area networks (WWANs). These wireless networks can be of different formations, such as cellular networks, ad hoc networks, and mesh networks, and can also be domain specific networks, such as vehicular communication networks and sensor networks. However, wireless networks are lack of physical security because the underlying communications are carried out by electromagnetic radiations in open space. Wireless networks pose a unique challenge in computer and network security community. The effort to improve wireless network security is linked with many technical challenges including compatibility with legacy wireless networks, complexity in implementation, and practical values in the real market. The need to address wireless network security and to provide timely solid technical contributions establishes the motivation behind this special issue.

This special issue received many submissions. Unfortunately, due to the limited space and volume, we can only choose twelve papers in this special issue, as a result of the peer-review process.

Wireless vehicular networks and sensor networks are two domain-specific networks that can have many important applications. This special issue includes a few papers investigating topics of locating and tracking malicious insiders and key management for sensor networks.

In vehicular communication networks that are hardened by public cryptographic systems, security modules including secret keys can be exposed to wrong hands due to weakness of physical security than those that can be enforced. With the security modules and secret keys, various security attacks can be launched via authenticated messages. Christine Laurendeau and Michel Barbeau designed a hyperbolic position bounding algorithm to localize the originator of an attack signal within a vehicular communication network. Their algorithm makes use of received signal strength reports for locating the source of attack signals without the knowledge of the power level of the station that is transmitting packets. Find the details of their work in the paper entitled "Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks."

Key management is always a challenging issue in wireless sensor networks due to resource limitation imposed by sensor nodes. Xiang et al. surveyed key establishment and distribution protocols in their paper entitled "In situ key establishment in large-scale sensor networks," where key establishment protocols are categorized as deterministic key predistribution, probabilistic key predistribution, and in situ key establishment protocols. Different from predistribution protocols, in situ protocol only requires a common shared key among all nodes to prevent node injection attack. Keys for securing pairwise communication among nodes are achieved by key establishment process after deployment. The paper provides an in-depth discussion and comparison of previously proposed three in situ key establishment protocols, namely, iPAK, SBK, and LKE. In addition, the study leads to an improvement where random keys can be easily computed from a secure pseudorandom function. This new approach requires no computation overhead at regular worker sensor nodes, and therefore has a high potential to conserve the network resource.

In the paper entitled "A flexible and efficient key distribution scheme for renewable wireless sensor networks," A-N. Shen et al. proposed a key distribute scheme for three-tier hierarchical wireless sensors networks that consist of base stations, cluster heads, and sensor nodes. By making use of secret keys generated by a bivariate symmetric polynomial function and well-designed message exchanges, the key distribution protocol can allow new sensor nodes to be added, deter node captures, and cope with the situations when base stations are either online or offline.

Routing protocols are integral components of multihop networks. Attacks on routing protocols can render such networks nonfunctional. Many wireless sensor networks can be viewed as multihop ad hoc networks. The following three papers discuss security issues of routing protocols.

Establishing trusts among sensor nodes can be an effective approach to counter attacks. In the paper entitled "Cautious rating for trust-enabled routing in wireless sensor networks," I. Maarouf et al. studied trust-aware routing for wireless sensor networks. Trust awareness of sensor nodes are commonly obtained by implementing a reputation system, where the measures of trustworthiness of sensor nodes are provided by a rating system. In the paper, the authors proposed and studied a new rating approach for reputation systems for wireless sensor networks called "*Cautious RAting for Trust Enabled Routing (CRATER)*."

In multihop wireless networks, designers of routing protocols concern not only network performance (such as bandwidth and latency) but also malicious attacks on routing protocols. Nevertheless, how to choose a path between two nodes in a network relies on both performance and security considerations. In their paper entitled "On multipath routing in multihop wireless networks: security, performance, and their tradeoff," L. Chen and J. Leneutre formulate the multipath routing problem as optimization problems with objectives as minimal security risks, maximal packet delivery ratio, or maximal packet delivery ratio under a given security risks. Polynomial time solutions to the optimization problems are proposed and studied.

Mobile Ad Hoc Networks (MANETs) are often subject to node capture attack. Once a node is captured by an adversary, all the security material stored in the node falls in the hands of the adversary. The captured node after reprogram or a newly deployed node operated by the adversary can make use of the stored security material to gain access to the networks and hence launch attacks on the network. Thus, it is beneficial to reduce the probability that nodes are detected and located, in particular, in hostile environments. X. Lu et al. proposed a routing protocol for wireless ad hoc networks where the antennas of nodes can act as both omnidirectional and directional antennas in the paper entitled "Minimizing detection probability routing in ad hoc networks using directional antennas." The routing protocol aims at reducing detection probability while finding a secure routing path in ad hoc networks where nodes employ directional antennas to transmit data to decrease the probability of being detected by adversaries.

Captured nodes pose security threats to many wireless networks. Capturing node is an important and yet very typical attack that is commonly launched to attack wireless ad hoc networks and sensor networks. Therefore, it should not come as a surprise that this issue includes another paper investigating this attack. M. Conti et al. in their paper entitled "Mobility and cooperation to thwart node capture attacks in MANETs" demonstrated that node mobility, together with local node cooperation, can be leveraged to design secure routing protocols that deters node capture attacks, among many other benefits.

This special issue also includes discussions on another type of an important attack, called "*coordinated attacks*," launched via Botnets. Advancements of wired and wireless networks have also enabled attackers to control applications running on many networked computers to coordinately attack while letting users to access remote computing resources much easily. Software applications in many hosts can form self-propagating, self-organizing, and autonomous overlay networks that are controlled by attackers to launch coordinated attacks. Those networks are often called Botnets. In their paper entitled "Botnet: classification, attacks, detection, tracing, and preventive measures," J. Liu et al. provide a survey on this subject. The paper discusses many fundamental issues regarding Botnets and sheds light on possible future research directions.

Ever-evolving mobile wireless networking technology leads to coexistence of many different wireless networks. Seamless and fast handover among different networks such as Wireless LANs (e.g., IEEE 802.11), WiMax (e.g., IEEE 802.16), and personal communication systems (e.g., GSM) becomes an important topic under investigation. The handover mechanisms need to not only maintain the security of the networks involved but also sustain the quality of the service (QoS) requirements of network applications. The following two papers study internetwork handover mechanisms.

In the paper entitled "Pre-authentication schemes for UMTS-WLAN interworking," A. Al Shidhani and V. Leung proposed and studied two secure pre-authentication protocols for the interworking Universal Mobile Telecommunication System (UMTS) and IEEE 802.11 Wireless Local Area Networks (WLANs). The authors also verified the proposed protocols by the Automated Validation of Internet Security Protocols and Applications (AVISPAs) security analyzer.

Growing interesting in multimedia access via mobile devices has led the IEEE 802.21 workgroup to standardize the Media Independent Handover (MIH) mechanisms that enable the optimization of handovers in heterogeneous networks for multimedia access. Based on the analysis on IPSec/IKEv2 and DTLS security solutions for secure MIH message transport, J.-J. Won et al. show that handover latency can be too large to be acceptable. They thus proposed and studied a secure MIH message transport solution that reduces authentication time. Find the detail of their work in the paper entitled "Secure media independent handover message transport in heterogeneous networks."

S. Song et al. study a related but different problem in mobile wireless networks in the paper entitled "A secure and lightweight approach for routing optimization in mobile IPv6." Mobile IPv6 (MIPv6) provides mobile terminals uninterrupted access to networks while on the move via a mechanism called Router Optimization (RO). They found three weaknesses in RO that attribute to a session hijack attack where an adversary can join an ongoing sessions at a chosen location. They proposed an authentication mechanism that hardens RO. Via performance evaluation, they show that the improved protocol achieves strong security and at the same time requires minimal computational overhead.

Cooperative radio is an important wireless communications technology that can improve capacity of wireless channels. It has been a topic that attracts growing interests. This special issue nonetheless has included the paper entitled "Distributed cooperative transmission with unreliable and untrustworthy relay channels."

Cooperative radio is subject to malicious attacks and performance degradation caused by selfish behaviors. Z. Han and Y. (Lindsay) Sun demonstrated the security vulnerabilities of the traditional cooperative transmission schemes and proposed a trust-assisted cooperative scheme that can detect attacks and has self-healing capability.

In summary, this special issue reflects growing interests in wireless network security, without which the usability of wireless networks is questionable. We believe that this special issue is a good snapshot of current research and development of wireless network security and is an important reference for researchers, practitioners, and students.

In the end, we would like to extend our appreciation to every author who has submitted their work. We are very regretful that we could not include every decent paper in this special due to the page limitation. Without unselfish reviewers' countless efforts, it would be impossible for us to select these papers from the great number of submissions and to ensure the quality of the special issue. We are thus deeply indebt to our reviewers. Last, but not the least, we thank our editor Hend Abdullah and many other editorial staff members with the journal. Without their coordination and skillful management, we would not be able to finish our task as guest editors.

Yang Xiao
Hui Chen
Shuhui Yang
Yi-bing Lin
Ding-zhu Du