Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks

Hassen Redwan and Ki-Hyung Kim
Department of Information and Communication Engineering
Ajou University
Suwon 442-749, South Korea
E-mail: hassenred1@yahoo.com

ABSTRACT

Nowadays, security is considered as one of the most critical parameter for the acceptance of any wireless networking technology. Nevertheless, security in wireless mesh network (WMN) is still in its infancy as little attention has been rendered to this topic by the research community. So far the security issue in wireless mesh networking has rarely been addressed. As entire security of the network is as strong as the weakest component, integration of security mechanisms of heterogeneous wireless networks in the open wireless network environment has paramount significance. In this paper, we analyze the security-related characteristics, the fundamental security requirements and possible security attacks of wireless mesh network. We also propose a heterogeneous wireless network integration model along with the description of security reference points at the boundaries of the heterogeneous wireless networks. Finally, a possible application scenario based on our proposed model is described.

Index Terms— **wireless network security, wireless mesh network, security attacks, wireless network integration**

I. INTRODUCTION

Wireless mesh networking has appeared as a new and promising wireless networking environment for next generation wireless networks. It facilitates quick and easy extension of local area networks into a large-scale wide area networks. Typical wireless mesh networks (WMNs) consist of mesh routers and mesh clients [3]. Mesh routers, which are static and power-enabled, form a wireless backbone of the WMNs and interwork with the wired networks to provide multi-hop wireless Internet connectivity to the mesh clients. Mesh clients access the network through mesh routers. They can also directly mesh with each other. Unlike mesh routers, the mesh clients can be battery-operated mobile nodes. The typical architecture of WMN is shown in Figure 1.

Wireless mesh networking has emerged as one of the most promising concept for self-organizing and auto-configurable wireless networking to provide adaptive and flexible wireless connectivity to mobile users. This concept can be used for different wireless access technologies such as wireless local area network (WLAN), wireless personal area network (WPAN), and wireless metropolitan area network (WMAN) technologies. The work in [1] stated that WMNs are anticipated to resolve the limitations and to significantly improve the performance of ad hoc networks, WLANs, WPANs, and wireless metropolitan area networks. The development of this technology has to deal with the challenging security, architecture and protocol design issues. The state-of-the-art work is still insufficient for deploying sizable wireless mesh networks because important aspects such as network radio range, network capacity, scalability, manageability, and security still remain open problems [14].

For any wireless networking technology, security is considered one of the most critical factors to gain greater acceptance. In WMNs, as one component of the wireless technologies, security is one of the crucial components that needs due attention. Nevertheless, how to design and implement security schemes for intrusion detection is still a challenging task which needs further investigation. Most of the research in WMNs has been focused around various protocols for multi-hop routing leaving the area of security mostly unexplored [1], [3]. Besides to this, the emergence of new applications of WMNs necessitates the need for strong privacy protection and security mechanisms of WMNs.

The organization of the rest of the paper is as follows. First, we describe statement of the problem in section II; in section III, we look at the characteristics of WMN and its security requirements; and in section IV, we discuss security attacks in WMN; we then describe integration of WMN with other wireless networks, in section V; finally, conclusion is made in section VI.

II. STATEMENT OF THE PROBLEM

There are a great number of potential application scenarios for wireless mesh networks ranging from home and community networks to high speed MANs. As described in [1] WMNs are undergoing rapid commercialization in many application scenarios such as broadband home networking, community networking, building automation, high-speed metropolitan area networks, intelligent transport system networks and enterprise networking.

Clearly, security in a WMN is extremely important for effective utilization of these application areas. One main advantage of WMNs is that it enables us to integrate various existing networks through the gateways. However, this benefit also brings related vulnerability to security attacks. This leads to the need for greater attention to be given to the security issues of WMNs. Therefore, this work will try to survey the various potential security attacks of WMNs.

In addition to this, one of the major issues in WMNs is the security integration of heterogeneous networks such as

978-0-7695-3540-1/08 $25.00 © 2008 IEEE
DOI 10.1109/FCST.2008.15

integration of WPAN, WLAN and WMAN security mechanisms. In a heterogeneous wireless mesh environment, some kind of security framework should be devised to customize the security schemes based on the type of network. The work in [3] leaves the integration aspect as one of the open problems to be investigated in the WMNs.

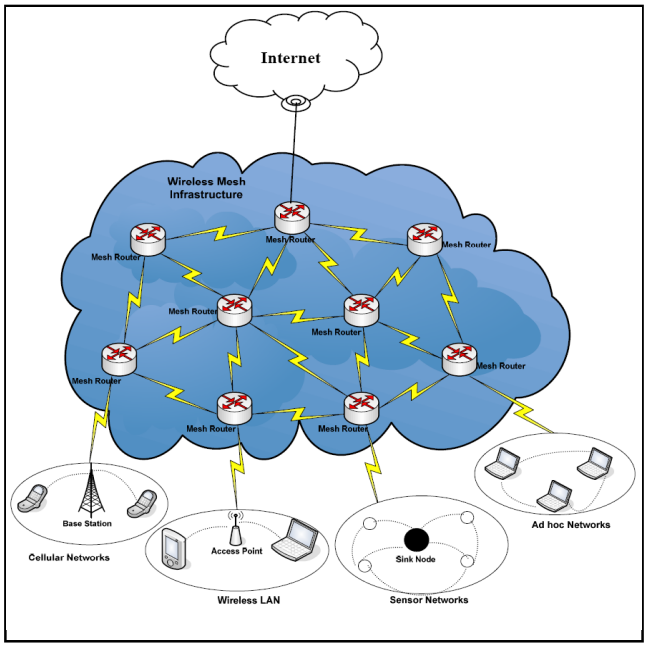

Figure 1: Infrastructure of Wireless Mesh Network

Similarly, the work in [4] indicate open research issue concerning security solutions adapted for the differing security requirements of more challenging usage scenarios.

Accordingly, dealing with the security requirements and the security integration of mesh network with other wireless networks is essential to come up with better functionality of WMNs.

III. CHARACTERISTICS OF WMN AND ITS SECURITY REQUIREMENTS

In this section, we discuss the characteristics as well as the major security requirements of wireless mesh networks.

A. Characteristics of Wireless Mesh Networks

Many authors give various definitions to WMN. The work in [2] defines WMN as a wireless co-operative communication infrastructure between a massive amount of individual wireless transceivers. The coverage area of the WMN radio nodes working as a single network is sometimes called a mesh cloud [15]. So as to create a radio network, the radio nodes should work in harmony with each other. Thus access to the mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network.

Wireless mesh architecture is constructed from peer radio devices that do not have to be cabled to a wired port. With careful design, such architecture may provide high bandwidth, efficiency, and economic advantage over the coverage area.

One of the measures for performance of a network is the reliability issue. The topology of WMN is tremendously very reliable and offer redundancy as each node is connected to several other nodes. In WMNs, the multi-hopping communication makes the routing aspect a very important and necessary functionality of the network.

When the number of devices in WMN become more, then the more bandwidth will be available. These days, wireless infrastructures are becoming cheaper than the traditional networks. Due to this reason as stated in [2], many wireless community network groups are already creating wireless mesh networks.

B. Security Requirements

To ensure the security of WMNs, the following major security objectives of any application have paramount importance.

- **Confidentiality**

It means that certain information is only accessible to those who have been authorized to access it. In other words, it ensures that certain information is never disclosed to unauthorized entities. In order to maintain the confidentiality of some classified information, we need to keep them secret from all entities that do not have the privilege to access them. It is also one of the design goals for many cryptosystems which made practical by using the techniques of cryptography.

Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Exposing such information to enemies could lead to devastating consequences. In some cases, routing information must also remain confidential as the information might be valuable for enemies to identify and locate their targets in a battlefield.

- **Integrity**

Integrity guarantees that a message being transferred is never corrupted. Integrity can be compromised mainly in the following two ways [8]:

Malicious altering - such as an attacker altering an account number in a bank transaction

Accidental altering - such as a transmission error

A message could be removed, replayed or revised by an adversary with malicious attack goals on the network, which is regarded as malicious altering. On the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication such as radio propagation impairment or hardware errors such as hard disk failure, then it is categorized as accidental altering

- **Availability**

Availability ensures the survivability of network services despite denial of service (DoS) attacks. This security requirement is challenged mainly during the DoS attacks, in which all the nodes in the network can be the attack target and

thus some selfish nodes make some of the network services unavailable. A DoS attack could be launched at any layer of the network [23]. For instance, on the physical and media access control layers, an adversary could employ jamming signal to interfere with communication on physical channels. On the network layer, an adversary could interrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target of an adversary is the key management service, which is an essential service for any security framework.

- **Authenticity**

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to ensure their identities using some techniques of authentication. Without the use of an authentication mechanism, the adversary could impersonate a benign entity and thus gain access to confidential resources.

- **Non-repudiation**

Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. It is useful for detection and isolation of a node with some abnormal behavior. For instance, when node-A receives an incorrect message from node-B, non-repudiation allows node-A to accuse node-B using this message and to convince other nodes that node-B is compromised.

- **Authorization**

Authorization is a process in which an entity is issued a credential by the trusted certificate authority. It is generally used to assign different access rights to different level of users.

For example, we may need to make sure that network management function is only accessible by the network administrator. In this case, there should be an authorization process before the network administrator accesses the network management functions.

- **Anonymity**

Anonymity means that all the information that can be used to identify the owner or the current user entity should be kept private and not distributed to other communicating parties. This security requirement is closely related to the preservation of privacy. Hence, we should try to protect the privacy of a user entity from arbitrary disclosure to any other entities.

IV. SECURITY ATTACKS OF WMN

In this section, the main threats that violate the security criteria, which are generally known as security attacks, are analyzed.

Major Attack Types of WMN

There are various kinds of attacks in wireless mesh network. The main types of attack are briefly described as follows.

- *Denial of Service attack*

The DoS attack is encountered either by accidental failure in the system or a malicious action. The conventional way to create a DoS attack is to flood any centralized resource so that it no longer operates correctly or stop working. A distributed DoS (DDoS) attack is an even more severe threat to WMNs. DDoS attack is launched by a group of compromised nodes who are part of the same network and who collude together to bring the network down or seriously affect its operation. One instance of DoS attack is SYN flooding.

- *Impersonation attack:*

This attack creates a serious security risk in WMNs. If proper authentication of parties is not supported, compromised nodes may be able to join the network, send false routing information, and masquerade as some other trusted nodes. A compromised node may get access to the network management system of the network; and it may start changing the configuration of the system as a legitimate user who has special privileges.

Security mechanism of impersonation attacks could be to apply strong authentication methods in contexts where a party has to be able to trust the origin of data it has received or stored.

- *Routing attack*

Routing attacks in WMNs could be:

Routing table overflow attack - an attacker attempts to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to a resource exhaustion or DoS attack.

Wormhole attack - an attacker receives packets at one location in the network and tunnels them selectively to another location in the network. Then, the packets are resent into the network, and the tunnel between two colluding attackers is referred to as a wormhole.

Blackhole/sinkhole attack - a malicious node uses the routing protocol to advertize itself as having the shortest path to the node. In this situation, the malicious node advertize itself to a node that it wants to intercept the packet.

Byzantine attack - an invalid operation of the network initiated by malicious nodes where the presence of compromised nodes and the compromised routing are not detected. This attack will eventually resulted in sever consequences to the network as the network operation may seem to operate normal to the other nodes.

Location disclosure attack - this attack reveals something about the structure of the network or the locations of nodes such as which other nodes are adjacent to the target, or the physical location of a node.

Thus the routing mechanisms of WMN must be secured. The usual mechanism, to ensure integrity of data, is using hash functions and message digest [2].

V. INTEGRATION OF WMNs WITH OTHER WIRELESS NETWORKS

In this section, security issues of each wireless networks and the proposed network integration model is briefly described.

A. Constraints

There are four main constraints in wireless mesh network [2] or in any wireless system which has mobile clients. These are CPU, battery, mobility and bandwidth constraints

B. Wireless Ad Hoc Networks

In wireless ad hoc network, each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to wired networks and WLAN.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. Wireless ad hoc networks can be further classified by their application [13] as mobile ad hoc networks (MANETs), wireless mesh networks and wireless sensor networks.

C. Security in MANET

MANET is a collection of wireless mobile nodes, communicating among themselves over possibly multi-hop paths, without the help of any infrastructure such as base stations or access points. For secure nodes communication, management of key plays important role. The role of key management is to ensure that only valid members have access to a valid group key at any time. As described in [16] MANETs are more vulnerable to malicious attacks than the traditional wired networks. This is because of the facts such as the low degree of physical security of mobile nodes, an open medium features, a dynamic topology, a limited power supply, and the absence of a central management point.

Security is critical for such networks when nodes are deployed in hostile environments, and security concerns remain a serious impediment to widespread adoption of these wireless networks. Besides to this, node mobility causes many security issues in MANETs, such as dynamic membership, key management, and configuration [5]. Nodes in MANETs are powered by battery. Hence, energy efficiency should be considered when designing security schemes.

D. Security in Wireless Sensor Networks

A wireless sensor network is a multi-hop routed and infrastructure-less network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [17][19]. Sensor data that are acquired by sensor nodes are transferred in a multi-hop routing to the sink node. The sink node is usually connected to other networks.

Sensor networks are being deployed for a wide variety of applications [12], including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. In order to provide security, security challenges such as key establishment, secrecy, privacy, robustness to DoS attack, and secure routing needs critical consideration.

Techniques such as public key algorithms may not be applicable to sensor nodes due to the limited resources that are unable to handle complex processing. The severe constraints and demanding deployment environments of wireless sensor networks make computer security for these systems more challenging than for conventional networks [20].

E. Security in Cellular Networks

A cellular network is a single-hop and infrastructure based network using base stations and provides radio coverage over a wide area. The security mechanisms of cellular network consists of functions like user privacy based on identities, mutual authentication based on challenge-response handshake authentication protocol, session key agreement during a mutual authentication process and secure communication with a session key that enables confidential communication and message integrity [10].

In cellular networks, all the security aspects can be successfully handled by the base station. Centralizing all security operations at one point would delay attack detection and treatment, and therefore give the adversary an undeniable advantage [18].

F. Security in Wireless LAN

A WLAN is a single-hop and infrastructure-based wireless local area network that uses access points (AP) to connect wireless users to a local wired network. Several wireless APs can link together to form a larger network that allows roaming services.

Roaming is a general term in wireless telecommunications that refers to the extending of connectivity service in a location that is different from the home location where the service was registered [11]. Concerning the security issue, roaming is technically supported by mobility management, authentication, authorization and accounting. The security mechanisms of WLAN are based on the authentication and confidentiality features.

G. Heterogeneous Network Integration Model

In the previous sub-sections, we discussed some of the relevant features of the heterogeneous wireless networks. The interoperation of these wireless networks with the wireless mesh network and one another is shown in the network integration model of Figure 2. Here the flow of traffic could be from the mesh network to other wireless client networks and vice-versa. Traffic can flow from mesh subscriber stations to mesh base stations, then out of the mesh network and vice-versa [21].

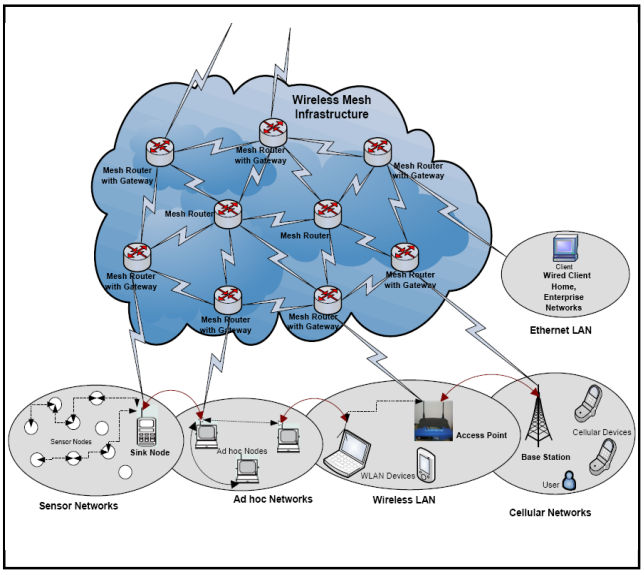

Figure 2: Heterogeneous Network Integration Model

Systems of fourth-generation (4G) mobile communication as described in [9][22] will mainly be characterized by a horizontal communication model, where such different access technologies will be combined on a common platform called the converged broadband wireless platform, or open wireless architecture (OWA).

- *Vulnerabilities of the Integration Network Model*

Security is much more difficult to maintain in the wireless networks than in the wired network. Possible vulnerabilities in the integration of wireless networks are the following.

a) Lack of Secure Boundaries between Wireless Networks

Figure 2 shows the security integration aspect of wireless sensor networks, Ad hoc Networks, Wireless LAN and Cellular Networks with that of WMN. As shown in the figure each of the heterogeneous wireless networks has formed connection with the mesh backbone through the Mesh gateway interface. When these networks communicate with the Mesh cloud, they pass through the gateway routers of the mesh backbone. The security issue at the boundary between the heterogeneous wireless networks and the mesh infrastructure should be dealt intensively. In line with this, when passing through the mesh cloud, each of these heterogeneous networks need the mesh infrastructure to fulfill their own individual security requirements.

Accordingly a security module that integrates the security technologies of each of these various and different networks should be incorporated in the gateway routers of the Mesh backbone which in turn will ascertain the security interoperability. This module then should provide security according to the applications and users requirements of each one of these heterogeneous networks.

In addition to the above wireless network-to-router gateway security issue, the vulnerabilities such as possible security attacks at the boundaries between the wireless heterogeneous networks also necessitates a separate study. This happens when we use the hybrid wireless mesh network since the mesh clients can perform mesh functions with other mesh clients despite accessing the network. One possible attack is DoS attack made by malicious intruders to flood the network with a large volume of traffic and there by make the system inaccessible to the real users.

As stated in [17], an integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of wireless networks and the unique security mechanism used in each of these networks.

b) Intra-security threats in a wireless network

In the proposed integration model, the intra-security vulnerabilities are obvious in the WMN, sensor, ad hoc, WLAN and cellular networks. For instance, there is no such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network such as freedom to join, leave and move inside the network [7].

In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets [6]. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network. Once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically.

- *Application Scenario of the Network Integration Model*

In this sub-section we briefly describe one feasible application scenario of our proposed network integration model – the telemedicine service.

Telemedicine service

Recent technological advancements are serving a crucial human need by making medical diagnosis and treatment available to anyone at anywhere. Assume a visitor has gone to a sub-urban area and he has made a contract with the medical doctor in one of the hospitals in his region. Also the visitor is armed with medical sensor nodes in different parts of his body to monitor his health condition. The node of the doctor could be a wireless ad hoc node, a cellular network device like cell-phone, or a WLAN device like PDA inside or outside the hospital. Each of the integrated networks contains their own security mechanisms.

Having this information in mind, the proposed integrated network infrastructure could function as follows. The sink node - a node handled by the visitor to store sensors reading of his body parts - transmits the gathered readings to the physician across the optimum network of the integration model. Readings of the sensors could be sent either through the gateway router of wireless mesh network or through the ad hoc network and WLAN. Here, the visitor as a user, should first authenticate himself with the devices in the sensor network. If the reading is sent through the WMN, security

negotiation is made between the sink node of sensor network and the gateway router of WMN. If the WMN provide the user's security requirement, then the reading is routed to the destination across the WMN. Until the reading reaches the destination, security requirement negotiation is conducted at the boundaries between two networks of the integration model. In line with this, the doctor periodically monitors symptoms from the readings. If any kind of abnormalities come across, the doctor, say using his preferred device, sends an urgent message along with the medical prescription and multimedia instruction to the visitor. In the end, the messages from the doctor are displayed at the user device such as the sink node. The security reference points that can be used in this application scenario are described below.

- *Security Reference Points of the Network Integration Model*

As shown in Figure 3, the security reference points of the network integration model are:

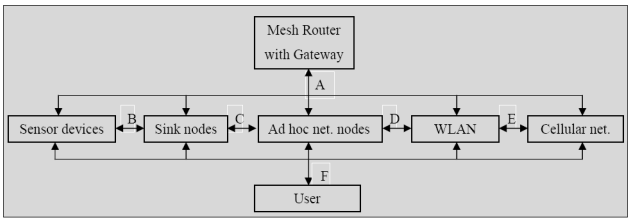

Figure 3: Security reference points of the network integration

Between the Mesh Gateway and heterogeneous client networks - the reference points between Mesh Gateway on one hand and the sensor networks, ad hoc networks, WLAN and cellular networks on the other hand (i.e. reference point A)

Between sensor devices and sink nodes (i.e. reference point B)

Between sensor network and ad hoc network (i.e. ref. point C)

Between ad hoc network and WLAN (i.e. reference point D)

Between WLAN and Cellular Network (i.e. reference point E)

Between user and various networks (i.e. reference point F)

- *Trust Relationship on the Network Integration Model*

Trust and security should go hand in hand. The level of trust has an impact on the level of security. Heterogeneous wireless networks involve various types of security domains and security implementation mechanisms. A trust relationship which considers the heterogeneousness of these networks security procedures is essential. In order to establish trust in the network integration, a distributed trust relationship that considers the individual security mechanisms of heterogeneous networks is recommended. This can be accomplished by specifying the levels of security requirements (see section III-B) and security mechanisms (such as encryption, digital signature, authentication) at the boundaries of each integrated networks. In other words, each of the integrated networks should contain their own security requirements along with the levels of trust they are willing to provide to other networks. For secure communication, negotiation of these security domains is done before any interaction takes place. For example, in the heterogeneous network integration model of Figure 2, the confidentiality requirement of wireless sensor networks may be associated with different levels of security mechanisms such as DES, AES and 3DES. Some models that use distributed trust environment are proposed in [24].

VI. CONCLUSION

In summary, the major security requirements for the wireless mesh network which should be regarded as a guiding principle to come up with the solutions to the security issues in the WMN are analyzed. The security related features of heterogeneous wireless networks such as WMNs, sensor networks, ad hoc networks, WLAN and cellular networks are briefly discussed. Then we come up with a heterogeneous wireless network integration model that integrates and clarifies the security reference points at the boundaries between heterogeneous networks. Our network integration model provides workable framework for wireless security concerns and for challenges in the realization of open wireless architecture. In addition to this, various security attacks that mainly threaten the WMN are discussed.

REFERENCES

[1] Ian F. Akyildiz, Xudong Wang and Weilin Wang, "wireless mesh networks: a survey," *Computer Networks,* vol. 47, pp. 445-487, Jan. 2005.

[2] Muhammad S. Siddiqui and Choong Seon Hong, "Security Issues in Wireless Mesh Networks," *IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*, 2007

[3] W. Zhang, Z. Wang, S. K. Das, and M. Hassan, "Security Issues in Wireless Mesh Networks," In Book *Wireless Mesh Networks: Architectures and protocols*. New York: Springer, 2008

[4] Yan Zhang, Jijun Luo and Honglin Hu. Wireless Mesh Networking: Architectures, Protocols and Standards. New York: Taylor & Francis Group, 2007

[5] Mohsen Guizani, Xianojiang Du, Hsiao-Hwa Chen and Peter Mueller, "Security in Wireless Mobile Ad Hoc and Sensor networks," *IEEE Wireless communication*, vol. 14, no. 5, pp.6-7, Oct 2007

[6] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks," In Book *Ad Hoc Networks Technologies and Protocols*, Springer, 2005.

[7] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communication*, vol. 14, no. 5, pp.85-91, Oct 2007

[8] Data Integrity, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Data_integrity (Accessed on May 24, 2008)

[9] Willie W. Lu, "Open Wireless Architecture and Its Enhanced Performance," *IEEE Communications Magazine*, vol. 41, no. 6, pp. 106-07, June 2003

[10] G. M. Koien, "An Introduction to Access Security in UMTS," *IEEE Wireless Communication*, vol. 11, no. 1, pp.8-18, Feb.2004

[11] Roaming, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Roaming (Accessed on May 26, 2008)

[12] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, August 2002.

[13] Maria Striki, John S. Baras and Kyriakos Manousakis, "A Robust, Distributed TGDH-based Scheme for Secure Group Communications in MANET," *IEEE International Conference on Communications (ICC '06)*, vol. 5, pp. 2249-2255, June 2006

[14] Xudong Wang, Sunghyun Cho and Jean-Pierre Hubaux, "Wireless Mesh Networking: Theories, Protocols and Systems," *IEEE Wireless communication*, vol. 13, no. 2, pp. 8-9, April 2006

[15] Wireless mesh network, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Wireless_mesh_network (May 24, 2008)

[16] Bo Sun, Lawrence Osborne, Yang Xiao and Sghaier Guizani. "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *IEEE Wireless communication*, vol. 14, no. 5, pp. 56-63, 2007

[17] Jongmin Jeong and Zygmunt J. Hass. "An Integrated Security Framework for Open Wireless Networking Architecture," *IEEE Wireless communication*, vol. 14, no. 2, pp. 10-18, April 2007

[18] Naouel B. Salem and Jean-Pierre Hubaux, "Securing Wireless Mesh Networks," *IEEE Wireless Communication*, vol. 13, no. 2, pp. 50-55, April 2006

[19] Kay Romer and Friedemann Mattern, "Design Space of Wireless Sensor Networks," *IEEE Wireless Communication*, vol. 11, no. 6, pp. 54-61, December 2006

[20] Adrian Perrig, John Stankovic and David Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, no. 6, June 2004

[21] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), pp. 1-857, 2004.

[22] Chen Yiping and Yang Yuhang, "A New 4G Architecture Providing Multimode Terminals Always Best Connected Services," *IEEE Wireless Communication*, vol. 14, no. 2, pp. 36-41, April 2007

[23] X. Gu and R. Hunt, "Wireless LAN Attacks and Vulnerabilities" In *the Proceeding of IASTED Networks and Communication Systems*, April 2005

[24] Christian Tchepnda and Michel Riguidel, "Distributed Trust Infrastructure and Trust-Security Articulation: Application to Heterogeneous Networks," In *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA'06)*, vol. 2, pp. 33-38, April 2006