Security Challenges in Multihop Wireless Mesh Networks–A Survey

Divya[*] and Sanjeev Kumar[**]

Computer Science & Engineering
Punjab Engineering College,
Chandigarh. India
{divya,sanjeevsofat}@pec.edu.in

Abstract. Security is a paramount concern in Wireless Mesh Networks (WMN) and also one of the core components in making WMNs successful and an enabler into different markets. A core challenge in securing the WMN is the large number of communication links over the air; as each mesh device may be mobile and deployed outdoors, each mesh link presents an exposure and vulnerability into the mesh network. These vulnerabilities are partially due to the structure of WMNs and cannot be removed easily. Security procedures present in 802.11s only take care of the potential security attacks in network association and secure link establishment. Ensuring that the routing protocol is secure is also not specified in the standard. In this paper we analyze the security problems in WMN and present few promising open research challenges which need immediate attention.

Keywords: Vulnerabilities, Attack prevention, IEEE 802.11s, Key Management, Secure routing.

1 Introduction

Original mesh architectures emerged from mobile ad hoc networks (MANETs) for military networks. The IETF MANET Work Group has been developing various MANET protocols for almost a decade [1]. MANETs were envisioned to be military and tactical networks where peer nodes could gain mutual trust between them. Mesh networks are different from MANETs in that there is more infrastructure communication rather than direct, peer-to-peer communication with mesh networks becoming a popular deployment in public spaces. IEEE 802.11s inherits security framework from 802.11i with certain extensions. Thus, whatever security problems exist in 802.11i will also occur in 802.11s. Moreover, due to the multihop mesh network architecture, security becomes a more challenging issue. It is thus evident that especially in the metropolitan space, existing IEEE networks' security standards 802.1X and 802.11i-2007 [2] based security mechanisms lack the specificity for securing the WMN. Even though

[*] Lecturer and Associate Coordinator, Cyber Security Research Centre.

[**] Professor and Coordinator, Cyber Security Research Centre.

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 92–101, 2010.

many vendors are using strong 128-bit encryption to relay client and infrastructure traffic over the air, as previous wireless LAN attacks have shown, a hacker may not necessarily need to crack the key to get user information or damage the network.

2 Potential Attacks on WMN Protocols

As mentioned earlier, WMNs face a range of security challenges that emerge due its multi-hop nature. To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Several routing protocols for WMNs have been proposed. A majority of these protocols assume a trustworthy collaboration among participating devices that are expected to abide by a "code-of-conduct". But there lie several security threats [3], some arising from shortcomings in the protocols, and others from the lack of conventional identification and authentication mechanisms. We classify the attacks into two categories namely external attacks and internal attacks. The attacks that are designed to exploit the vulnerabilities of WMN are called external attacks. In such attacks the attacker is in the close proximity but not a trusted node. In contrast, in internal attacks the attackers are actually willing to participate in the mesh network.

2.1 External Attacks

By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker can successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. External attacks are usually prevented with conventional security mechanisms such as member authentication.

2.2 Internal Attacks

These are more severe kind of threats which come from compromised nodes advertising incorrect routing information to other nodes. Detection of such incorrect information is difficult as merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys. External attacks are usually used as stepping stones leading to internal attacks. To defend against the first kind of threats, nodes can protect routing information in the same way as they protect data traffic. However, this defense is ineffective against attacks from compromised servers. Detection of compromised nodes through routing information is also very difficult in a WMN because of its dynamic topology changes.

Attacks on routing layer can be classified into two categories, attacks on routing protocols & attacks on packet forwarding/delivery. Attacks on routing prevent a victim from finding the path from source to destination even if routes exist and attack on packet forwarding disrupt packet delivery even if the path is known.

Attacks on routing can create various undesirable affects. On the other hand, certain properties of WMNs can be exploited to achieve secure routing which are discussed in the end of the paper. Routing protocols for WMNs must also be able to handle outdated routing information to accommodate the dynamically changing topology.

False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes without involving these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies in WMNs.

3 Secure Routing Protocols

The mechanisms discussed in this section prevent internal attacks by preventing misbehaving nodes from attacking the routing information. To address the security attacks on routing mechanism, several secure routing protocols have been proposed: such as SAODV, Ariadne, SEAD, CSER, SRP, SAAR, BSAR, and SBRP [4]. The default routing protocol in 802.11s TGs is Hybrid Wireless Mesh Protocol (HWMP) [5], which provides the ability for a mesh node to learn routes to another mesh node using a broadcast route discovery mechanism. Broadcast-based route discovery mechanisms are traditionally susceptible to DoS attacks as they use exhaustive rebroadcasting methods.

3.1 Use of Cryptographic Approaches

In [6] the use of asymmetric cryptography to secure on-demand ad hoc network routing protocols has been proposed. However, as above, when the nodes in an ad hoc network are generally unable to verify asymmetric signatures quickly enough, or when network bandwidth is insufficient, these protocols may not be suitable. In [7] *symmetric*-key approaches to implement the authentication of link-state updates have been described, but they do not discuss mechanisms for detecting the status of these links. Furthermore, these protocols assume the use of periodic routing protocols, which are not always suitable in ad hoc networks. In [8] cryptographic mechanisms similar to those used in Ariadne with TESLA have been used but this approach optimistically integrates routing data before it is authenticated adversely affecting security. A number of other researchers have also proposed the use of symmetric schemes for authenticating routing control packets. In [9, 10] a mechanism requiring shared keys between all communicating routers is proposed. This scheme may not scale to large mesh networks and may be vulnerable to single-node compromise. In [10] use of symmetric primitives to secure routing between nodes and a trusted base station has been proposed. In [11] use a network-wide symmetric key to secure routing communication is proposed which is vulnerable to a single node compromise, although the use of secure hardware to limit the damage that can be done by a compromised node is also specified.

There is yet another kind of routing protocols which use one-way hash chains. SEAD is one such routing protocol which builds on the DSDV-SQ version of the DSDV (Destination Sequenced Distance Vector) protocol. However SEAD does not cope with wormhole attacks. SEAD [12] uses hash chains to authenticate routing updates sent by a distance-vector protocol; however, this approach builds on a periodic protocol, and such protocols tend to have higher overhead than on-demand protocols and may not be suitable in highly mobile networks.

IETF's AODV and DSR are efficient in terms of network performance, but they allow attackers to easily advertise falsified route information, to redirect routes, and to launch DoS attacks. In case these protocols are applied to WMNs, an attacker may easily snoop frames over a WLAN mesh backhaul and learn about MAC addresses or various mesh nodes in the network. Although the network infrastructure of 802.11 WMNs tends to have less mobility and most of the traffic is to and from the Internet, however, some nodes such as handset devices, laptops, etc. can be an MP and may need mobility support.

In a routing protocol, nodes usually need to exchange routing messages for the purpose of finding link status, collecting neighbor information, requesting routing path, and so on. Thus, many control messages are involved. In order to meet diverse requirements by making the routing protocol be efficient for different scenarios, HWMP is being specified in 802.11s. In 802.11s, such messages are sent in various mesh action frames as information elements. Before draft 1.06 of 802.11s, one mandatory routing protocol and one optional routing protocol have been specified. The mandatory routing protocol is called hybrid wireless mesh protocol (HWMP), which is a hybrid routing protocol of on-demand routing and proactive tree-based routing. The optional routing protocol is based on link state routing and is called radio aware optimized link state routing (RA-OLSR).

The basic features of on-demand routing protocol based on radio-metric ad hoc on-demand distance vector (AODV) routing are adopted in HWMP with certain extensions 802.11s. The proactive tree-based routing is applied when a root node is configured in the mesh network. With this root, a distance vector tree can be built and maintained for other nodes, which can avoid unnecessary routing overhead for routing path discovery and recovery. It should be noted that the on-demand routing and tree-based routing can run simultaneously. Wireless Mesh Network (WMN) has emerged as a key technology and found a great deal of interest for the researchers in the recent past. Hybrid Wireless Mesh Protocol (HWMP) is the default path selection (i.e., routing) protocol fully specified in the current draft D.1.06 of 802.11s for WMN. However, security in routing or forwarding functionality is not specified in the standard. As a consequence, HWMP in its current from is vulnerable to various types of routing attacks. Since HWMP is based on the AODV [13], an open-source AODV software stack can be used to continually generate route request (RREQ) frames keeping all mesh nodes in the network busy re-broadcasting those. This may cause one or more mesh nodes to melt down, reboot, or stop servicing the network.

Further, most of the fields used in routing related information in AODV such as RRER, RREP, and RERR, are vulnerable to modification and forgery. Example of such mutable fields is: ID, Hop Count, Metric, Sequence Number, etc. Most damaging is the vulnerability of an MAC address, as an adversary can impersonate an MP by simply using its MAC address; an adversary can simply form part of mesh forwarding paths and launch any attack from there. Similar attacks are also possible against RA-OLSR, which is the optional path selection protocol in IEEE 802.11s draft standard.

SAODV [13] is a secure version of the original AODV protocol, which combines these techniques and more (e.g., digital signature for static fields in headers and hash chains to protect Hop Count). While SAODV is appropriate for ad hoc networks, it comes with some costs for WMNs. Even though hash chains are efficient for Hop

Count authentication, a malicious node can still choose not to increase it. Other drawbacks of SAODV include PKI infrastructure usage and key distribution, too frequent signature computations, and extra overhead for exchanging signatures, which can be up to two signatures per message, makes SAODV computationally prohibitive. IEEE 802.11 TGs is evaluating these techniques and may incorporate some subset of SAODV for securing the default path selection protocol, HWMP. ARAN [14] and Ariadne [15] are two other techniques for securing AODV, which can be adapted for securing HWMP. ARAN provides authentication and non-repudiation services using pre-determined cryptographic certificates that guarantees end-to-end authentication. As a result, ARAN limits or prevents attacks that can badly affect other insecure protocols. ARIADNE is an on-demand secure ad-hoc routing protocol based on DSR that implements highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two communicating parties. Although ARIADNE is free from a flood of route request packets and cache poisoning attack, but it is immune to the wormhole attack and rushing attack.

3.2 Internal Attacks in WMN

The internal attacks in WMN also pose a serious threat. If an attacker gains full control of a legitimate node, the cryptographic approaches will not be able to prevent the attacks launched from the node because the node has valid cryptographic keys and the messages sent by the node are also cryptographically valid. The compromised nodes could attack the routing mechanisms by generating false routing information, scheduling the data packets forwarding for their own benefits, selectively forwarding the packets, or not forwarding any packet at all.

If an attacking node lures all traffic around it by installing an attractive node using powerful transmitters and high-gain antennas to emerge as high-quality routes, it is termed as **sinkhole attacks**. Detection of sinkholes is difficult [18] without higher-layer protections such as asking for acknowledgments from the final destinations for all messages. Another kind of internal attack is the **black hole attack** which is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets. In second step, the attacker consumes the packets and never forwards. In an advanced form, the attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. **Byzantine attack** [17] can be launched by a single malicious node or a group of nodes that work in cooperation. A compromised intermediate node works alone or set of compromised intermediate nodes work together to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services. **Rushing attacks** [17] are yet another kind of serious attacks which subvert route discovery process to increase the likelihood that hostile station will be included in the given route. At present there are no integrated mechanisms in the routing protocols to defend against these kinds of attacks. An attacker may leverage multiple attacking nodes and create low-latency and high-speed route tunnels between them. This strategy will make attacker's tunnel appear attractive over a multi-hop path and cause a wide area of nodes to attempt to use the tunnel. Black hole/gray hole/sinkhole attacks might follow. Unfortunately, wormhole attacks are effective even if the protocol/system provides authenticity and confidentiality. Given the use of strong identification credentials, e.g., strong entropy keys and unique identities, IEEE 802.11 TGs may be able to address some of the above attacks, but may still be susceptible to insider attacks. The Packet Leash solution [16] is to add some extra information to each message at the sender side in order to allow the receiver to determine if the packet has traversed an unrealistic distance. The extra information could be a precise timestamp, which requires extremely precise clock synchronization, or the location information with a timestamp, which requires less precise clock synchronization.

4 Intrusion Detection Techniques

Because WMN has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in WMNs. In [22, 23] a specific design of intrusion detection and response mechanisms is proposed. In [24] two mechanisms: watchdog and pathrater are proposed, which improve throughput in the presence of nodes that agree to forward packets but fail to do so. In WMNs, cooperation is very important to support the basic functions of the network so the token-based mechanism, the credit-based mechanism, and the reputation-based mechanism can be used to enforce cooperation. In the case of WMN the Authentication becomes very critical issue to handle. However we have briefly studied the Central and Distributed Authentication mechanism that can be applied in case of WMNs but there is more to do with it. Although the need for a distributed authorization service is necessary to cope with the WMN necessities, the challenge still resides in the establishment of trust inside the network. As explained before, a totally centralized approach is unlikely to be an ultimate solution for trust establishment inside a WMN. However, a scheme based on transitive trust within the network can also create security breaches.

Thus from the above discussions it is clear that all security procedures present in 802.11s only take care of the potential security attacks in network association and secure link establishment. Ensuring that the routing protocol is secure is not specified in the standard. Routing security is usually considered as out-of-scope work for an IEEE 802.11 standard. However, for 802.11s [25], since the routing functionality is specified in the link layer, it becomes imperative to specify a security mechanism for routing protocols in 802.11s standard. WMNs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To secure a WMN, Secure routing and wireless Intrusion detection systems are considered to be the major attributes in context of the present paper to prevent internal and external attacks.

5 Mesh Security

The conventional WLAN security mechanisms (e.g., such as WPA2/802.11i) provide standardized methods for authentication, access control and encryption between a wireless client and an access point. Since most wide-area mesh solutions strive to retain compatibility with commercial off-the-shelf WLAN client adapters, existing standardized WPA2 mechanisms are commonly retained (e.g., the mesh network "looks like" an access point to the client). However, there are many different types of wireless mesh architectures, where each type of architecture may use a different approach for wireless security. Many approaches for mesh security may be derived from ad-hoc security research, but any future commercial mesh products will standardize security through 802.11s (e.g., will be based primarily on 802.11i security mechanisms).

5.1 Client Access Controls

Wireless mesh infrastructure networks provide access to wireless clients. In most 802.11-based wireless networks, clients are standard wireless LAN stations with no mesh networking capabilities. Some vendors, such as Motorola and PacketHop offer client mesh solutions, but all Metro-WiFi technologies are intended on providing access to non-mesh capable 802.11 stations. Client access security may vary depending on the type of network: a Metro-WiFi network may use open wireless authentication with a Layer 3 billing service access gateway, while an enterprise/private mesh network will typically use WPA2-compliant wireless access controls.

5.2 Inter-mesh Access Point Controls

While there are many progressive technologies available through ad-hoc security research, many commercially available mesh networks use a far more simple security model in advance of a mesh security standard. Most existing 802.11-based communication between mesh access points leverages a wireless-distribution system (WDS) mode-of-operation. A conventional (e.g., non-mesh) access point in WDS mode is simple wireless relay between wireless clients and wired access points. Many chipset vendors and mesh equipment providers offer communication protection between nodes using a static key to encrypt WDS links with WEP or AES. With the availability of fully compliant WPA2/802.11i chipsets, separate WPA2 security profiles can be defined for the WDS links (clients will be able to connect to the mesh APs with an alternate security profile – such as without encryption). Thus, there are two primary methods to protect inter-mesh AP communication in advance 802.11s standardization that are based mainly on WPA2/802.11i compliance levels for WDS mode:

- Static keys configured into the APs at both ends of the WDS link, providing WEP or AES encryptions between mesh nodes.
- WPA2/802.11i [22] specifies how key handshake works in ad-hoc mode, letting peers derive dynamic encryption keys. This makes it possible to apply the 802.11i four-way key handshake defined for ad-hoc mode to mesh APs connected by WDS. In other words, mesh traffic relayed using WDS modes for inter-mesh AP traffic is secured by WPA2. It is common for each mesh AP on the

network to be set with the same unique key, otherwise the mesh APs will not be able to communicate with one another. The number of session keys is directly proportional to the number of neighbors. Authentication is provided either through knowledge of a network-wide pre-shared key (e.g., in a similar manner as WPA-PSK), but some vendors already provide X.509v3-based authentication that derives unique pair-wise session keys per link. Challenges for mesh networks relate mainly to support for broadcast between mesh APs, which is an essential component of mesh routing protocols. Group session keys are used for broadcast messaging, while pair-wise keys are used for unicast routing messages. The 802.11s standardization efforts will provide authentication and communication protection in consideration of these factors, and the functional requirements of the mesh routing algorithms. The 802.11i security mechanisms and the associated WiFi-Protect Access (WPA2) profiles provide the basic building blocks for 802.11-based security (e.g., either in mesh networking or typical client access). The 802.11 security framework uses the 802.1X port-based access control mechanisms to prevent unauthorized wireless access. The client is the supplicant that requests authentication from an authentication server such as RADIUS where the authenticator gates access until the client is authenticated. The authentication exchange occurs between the client and the authentication server using the EAP protocol, which encapsulates the specific type of authentication. The Extensible Authentication Protocol (EAP) is a flexible protocol used to carry arbitrary authentication information, and rides on top of 802.1X and RADIUS to protocols to transfer data between the wireless client and an authentication server. EAP does not specify an authentication method. Commonly used methods are based on TLS/SSL technologies, where a secure tunnel and network-to-client authentication can be performed using a digital certificate, and clients can authenticate using either their own client certificate (e.g., EAP-TLS) or provide a username and password authentication exchange inside the secure TLS tunnel (e.g., EAPPEAP or EAP-TTLS). Upon success authentication, keying material is generated and distributed to enable encryption and integrity checking. The integrity checking prevents both message tampering and ensures an authenticated client cannot be impersonated. The WPA2 profile adds AES encryption and key management. The wireless security schemes for mesh networks are based on these fundamental capabilities.

5.3 Standardization

The IEEE is presently working on a standard for mesh networking through the 802.11s working group. The standard will use the WPA2/802.11i security methods to protect the wireless links, where the key principles in 802.11s security is summarized below:

- Standardization activities for security will focus on inter-AP security controls, where client access uses standard WPA2/802.11i authentication and encryption.
- Standardization on security between mesh access points is still being finalized within the standard. However, link-by-link security mechanism will be based on 802.11i, with a security architecture based on 802.1X authentication.

- Mesh APs may have supplicant, authentication and authentication server roles.
- All mesh routing must be authenticated using 4-way handshakes which can be attained using centralized 802.1X authentication. However, means of communicating between authentication server and remote mesh AP is presently not within the scope of the standard.

6 Conclusion

WMN has the several research challenges which need immediate attention. Study of WMN's specifics led to many critical security challenges which have been discussed in detailed in the paper. While the techniques and standardization considerations discussed in this paper can deter certain attacks in WMN, there is a limitation to the effects of prevention attacks. There is no single efficient and reliable security solution suitable for WLAN mesh as many of those solutions may be compromised due to vulnerabilities of channels and nodes in shared media, absence of reliable links to infrastructure, and dynamic topology changes. Use of cryptographic extensions in HWMP is also desirable to provide authenticity and integrity of routing messages and prevents unauthorized manipulation of mutable fields in the routing information elements. It therefore becomes evident that much work remains in developing integrated framework which can collectively battle multi-protocol attacks as well as detect and prevent intrusion in WMNs. Furthermore, an integrated, cross-layer security solution is more desirable.

References

1. http://www.ietf.org/html.charters/manet-charter.html
2. IEEE STD 802.11-2007. Wireless Local Area Networks, IEEE, WLAN Standard (2002)
3. Xuyang, D., Mingyu, F., Xiaojun, L., Dayong, Z., Jiahao, W.: Multi-path based secure communication in wireless mesh networks. Journal of Systems Engineering and Electronics 18(4), 818–824 (2007)
4. Zhang, W., Rao, R., Cao, G., Kesidis, G.: Secure Routing in Ad Hoc Networks and a Related Intrusion Detection Problem. In: Proceedings of IEEE Military Communications Conference, October 2003, vol. 2, pp. 735–740 (2003)
5. Bahr, M.: Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s. In: Proc. in IEEE International Conference on Mobile Adhoc and Sensor Systems, October 8-11, pp. 1–6 (2007)
6. Wu, B., Chen, J., Wu, J., Cardei, M.: A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Wireless Network Security. Network Theory and Applications, vol. 17. Springer, Heidelberg (2006)
7. Cheung, S.: An Efficient Message Authentication Scheme for Link State Routing. In: 13th Annual Computer Security Applications Conference, pp. 90–98 (1997)
8. Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., Levkowetz, H.: Extensible Authentication Protocol (EAP). Internet Draft draft-ietf-eap-rfc2284bis-06.txt (September 29, 2003)
9. Heffernan, A.: Protection of BGP Sessions via the TCP MD5 Signature Option. RFC 2385 (August 1998)

10. Batina, L., Mentens, N., Sakiyama, K., Preneel, B., Verbauwhede, I.: Low-cost Elliptic Curve Cryptography for Wireless Sensor Networks. In: 3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, pp. 6–17 (2006)
11. Basagni, S., Herrin, K., Rosti, E., Bruschi, D.: Secure Pebblenets. In: Proceedings of the Second Symposium on Mobile Ad Hoc Networking and Computing, October 2001, pp. 156–163 (2001)
12. Hu, Y.-C., Johnson, D.B., Perrig, A.: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In: Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), June 2002, pp. 3–13 (2002)
13. Zapata, M., Asokan, N.: Securing Ad hoc Routing Protocols. In: ACM Workshop on Wireless Secuirty (WiSe) (September 2002)
14. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M.: A Secure Protocol for Adhoc Networks. In: IEEE International Conference on Network Protocols, ICNP (2002)
15. Hu, Y., Perrig, A., Johnson, D.: Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks. In: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM) (September 2002)
16. Hu, Y.C., Johnson, D.B., Perrig, A.: Packet leashes: A defense against wormhole attacks in wireless networks. In: Proc. IEEE INFOCOM 2003, March/April 2003, vol. 3, pp. 1976–1986 (2003)
17. Glass, S., Portmann, M., villipuram: Securing Wireless Mesh Networks, pp. 1089–7801. IEEE Computer Society, Los Alamitos (2008)
18. IEEE Std 802.11i/D4.1, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements (2003)
19. Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs (2006)
20. Luo, H., Zerfos, P., Kong, J., Lu, S., Zhang, L.: Self-securing ad hoc wireless networks. In: Proc. IEEE ISCC 2002, July 2002, pp. 567–574 (2002)
21. Zhang, W., Das, S., Liu, Y.: A trust based framework for secure data aggregation in wireless sensor networks. In: Proc. IEEE SECON 2006, September 2006, pp. 60–69 (2006)
22. Tsakountakis, A., Kambourak, g., Gritzalis, S.: Towards effective Wireless Intrusion Detection in IEEE 802.11i. In: Proc. of Third International Workshop on Security Privacy and Trust in Pervasive and Uniqiutous Computing, IEEE SecPerU (2007)
23. Zhang, Y., Lee, W., Huang, Y.: Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal (ACM WINET) 9(5) (September 2003)
24. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proceeding of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, pp. 255–265 (2000)
25. Wua, T.-W., Hsieh, H.-Y.: Interworking wireless mesh networks: Problems, performance characterization, and perspectives. National Taiwan University, Journal Parallel Distributed Computing 68, 348–360 (2008)
26. Gerkis: A Survey of Wireless Mesh Networking Security Technology and Threats, SANS Institute InfoSec Reading Room (September 2006)