1

Security Issues in Wireless Mesh Networks

Wei Zhang[1], Zhe Wang[2], Sajal K. Das[1], and Mahbub Hassan[2]

[1] Center for Research in Wireless Mobility and Networking (CReWMaN),
Department of Computer Science and Engineering, The University of Texas at
Arlington. Arlington, TX 76019. {wzhang, das}@cse.uta.edu
[2] School of Computer Science and Engineering, University of New South Wales.
Kensington, Sydney 2052, Australia. {zhewang, mahbub}@cse.unsw.edu.au

11.1 Introduction

Recent advances in wireless technologies such as multiple-input multiple-output (MIMO) systems and smart antennas, wireless mesh networks (WMNs) have attracted increasing attention as an alternative for large-scale deployment of metropolitan area wireless networks.

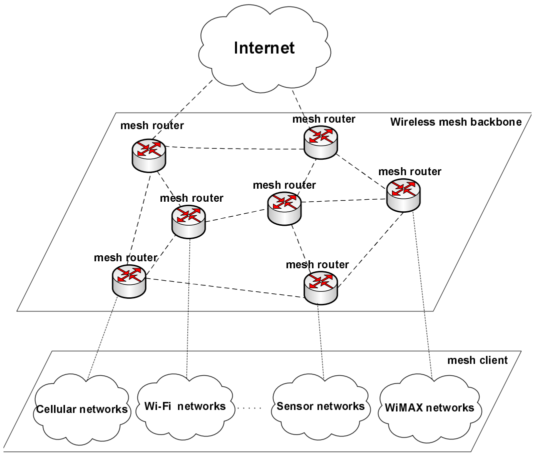

Fig. 11.1. Typical infrastructure of WMN [1]

Figure 11.1 illustrates a typical hierarchical architecture of a WMN [1], consisting of *mesh routers* and *mesh clients*. Mesh routers constitute the network infrastructure while mesh clients connect to them via wireless medium. Compared with conventional wireless routers, mesh routers are equipped with multiple wireless interfaces and the most common communication pattern is by multi-hop with lower transmission power. Mesh clients can be various devices, such as laptops, PDA, RFID readers, etc. Each mesh client usually has only one wireless interface. Moreover, although the mesh clients may also forward packets as a router, there is no gateway/bridge functionalities implemented in the mesh clients.

WMNs share some nice features with wireless ad hoc networks, including self-organization and self-configuration. In addition, since the mesh routers are either static or with minimal mobility, there exists infrastructure/backbone in WMNs. Thus, WMNs have the advantage of being extremely easy to deploy and relatively cheap in terms of both infrastructure and maintenance cost.

These desirable features make WMNs an appealing solution for a plethora of applications, such as broadband home networking, community networking, etc. However, there are still several challenges and issues preventing WMNs to be widely deployed in large scales. The first major issue is that the performance (throughput, delay, or packet loss rate) of WMNs drops sharply with increasing number of wireless hops the packets traverse through. The multi-radio, multi-channel technique ([2], [48]) is being researched to overcome this problem. The second major issue is the lack of an integrated cross-layer solution to provide *security* in WMNs, which has received meager attention in the literature. Clearly, without a well designed security solution, WMNs are vulnerable to various types of internal and external attacks that may cause significant inconvenience to the users and operators.

In this chapter, we will address the security issues in wireless mesh networks. The rest of the chapter is organized as follows. In Section 11.2 we discuss the security goals and challenges posed in WMNs. Section 11.3 surveys and analyzes the applicability of existing security techniques to WMNs. In Section 11.4 we point out the open problems in this area. Finally, we conclude in the end of this chapter.

11.2 Security Goals and Challenges

For any application (not necessarily on WMNs), the following general goals are desired to ensure security.

Confidentiality or *Privacy*: The communication between users must be secured such that the information cannot be disclosed to any eavesdroppers.

Integrity: The whole transmission paths must be protected to ensure the messages are not illegally altered or replayed during the transmission.

Availability: Applications should provide reliable delivery of messages against denial of service (DoS).

Authentication: When a user sends messages, there should be some processes to identify the user to ensure the messages are really sent by the claimed sender rather than fabricated by someone else.

Authorization: Before any user performs some tasks, there should be mechanism to ensure the corresponding users have the right to do them.

Accounting: When a user is using some services, some process should be able to measure the resources the user consumes for billing information.

Here we assume the existence of upper layer security mechanisms, such as anti-virus software and Secure Sockets Layer (SSL) protocol, and focus on additional security challenges posed by the unique features of WMNs.

11.2.1 WMN Specific Security challenges

The shared nature of wireless medium, the absence of globally trusted central controller, and the lack of physical protection of mesh routers pose the main challenges for securing WMNs.

First, like any wireless networks, the shared wireless medium makes it easy for attackers to launch jamming attacks, eavesdrop the communication between the mesh routers and inject malicious information into the shared medium. Given the fact that the correctness of routing messages is fatal to achieve wireless multi-hop routing in WMNs, the most harmful kind of malicious information is due to the fabricated routing messages.

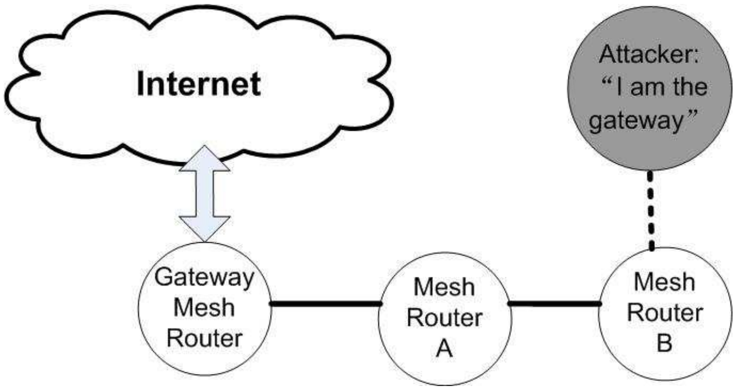

Fig. 11.2. The attacker fools mesh router B

Figure 11.2 illustrates a simple example of such attacks. The correct route for *Mesh Router B* to access the Internet is via *Mesh Router A* and the *Gateway Mesh Router*, while the attacker fools *Mesh Router B* by broadcasting the message: *"I am the gateway to the Internet."* If *Mesh Router B* could not detect such a message as faulty, it will direct all its Internet traffic to the attacker. Because the wireless medium is open, it is impossible to prevent the mesh routers from receiving such malicious messages. Therefore, an authentication mechanism is essential to distinguish the malicious information from the legitimate information.

Second, an authentication mechanism is usually implemented with the help of *Public Key Infrastructure* (PKI), which requires a globally trusted entity to issue certificates. However, it is impractical to maintain a globally trusted entity in WMNs. The details of authentication challenges are discussed in Section 11.3.1.

Third, the mesh routers are located outdoor, usually on roof tops or traffic light poles. They are not physically protected like the wired routers and wireless LAN access points. Therefore, it is much easier for attackers to capture the mesh routers and get full control of the device. If a router is fully controlled by attackers, the attacks can be launched from that router and the information sent by the attackers will be regarded as authenticated by other routers.

The cryptographic authentication schemes are thus broken and there must be another line of defense behind the authentication protection.

The above major challenges demand a set of cross-layer, self-adapted security mechanisms to protect WMNs.

In the following sections, we will discuss if and how some of the existing security solutions proposed for wireless ad hoc or sensor networks could be employed to protect WMNs by overcoming these challenges.

11.3 Security Concerns and Current Countermeasures

While the security of WMNs is a fairly new research topic, there exist several schemes to secure wireless ad hoc networks and wireless sensor networks which share similarities with WMNs to some extent. Let us analyze these solutions and discuss how to utilize them to secure WMNs.

11.3.1 Authentication

In wireless networks, authentication is very important because of the shared nature of the wireless medium. Any node, legitimate or malicious, with a suitable hardware device can send data into the network. Verifying that the data received is from a legitimate entity is critical for securing the network. Public key infrastructure (PKI) and certification authority (CA) provide two important mechanisms for authentication.

PKI and CA

Authentication is usually realized by implementing PKI based on asymmetric cryptography in which each user has a pair of cryptographic keys: *public key* and *private key*. The public key is widely distributed and known by all the users while the private key is only secretly kept by the user. One property of the pair of keys is that a message encrypted with the public key can only be decrypted with the corresponding private key and vice versa. By exploiting this, authentication can be achieved. For instance, a sender can digitally sign the packets using its own private key before sending them. If the receiver can successfully decrypt the messages with the sender's public key, it is assured that the packets are really sent by the claimed sender rather that someone else.

To check the validity of a digital signature, it is necessary to first verify that the sender's public key does belong to the sender, which requires a Certificate Authority (CA) be involved in the authentication procedure. The CA signs the binding of an entity's identity and its public key with its private key, and issues the signature as the entity's certificate. Any entity can validate the binding of sender's identity and public key by checking its certificate using CA's public key. A node may update its certificate periodically to reduce the chance of brute-force attack on its private key. So the CA has to stay on-line to reflect the periodically changing certificates. This scheme is based on the following assumptions: (a) the CA's public key is known by every entity in the network, (b) the CA's public key and signed certificates are globally trusted in the network, and (c) the communication channels through which the entities get other's certificate from CA are secure.

However, the absence of pre-established trusted network infrastructure in WMNs obstructs direct application of PKI. This is because it is impractical to deploy a CA that every node can trust and establish a secure communication channel with. A distributed CA scheme is thus required.

Distributed CA

An ingenious method is to distribute the functionality of the centralized CA to the whole network by applying *threshold cryptography* [15]. Basically, an $(n, t+1)$-threshold cryptography scheme allows n parties to share the ability to create a digital signature so that $t+1$ parties can jointly generate a valid signature, whereas it is infeasible for at most t parties to do so. The scheme is based on the assumption that the number of compromised parties will never exceed t.

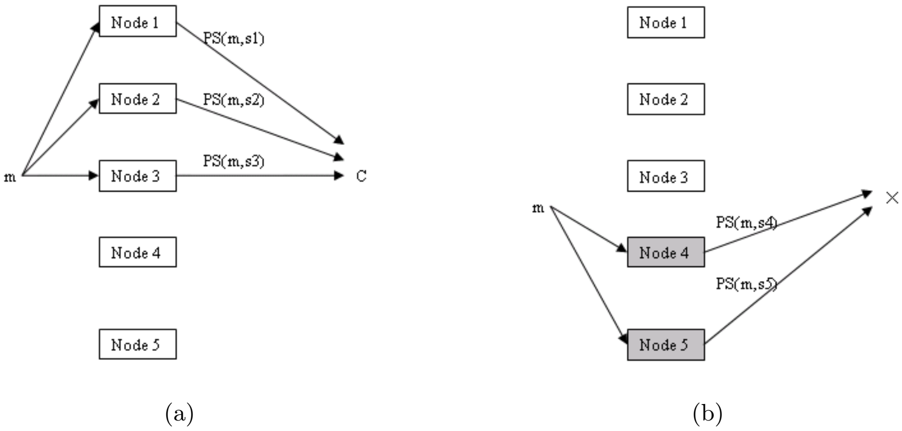

Fig. 11.3. (5, 3)-threshold signature

In WMNs, if the CA's public key is globally known and its private key is divided into n shares (one share for each node in the network), the threshold signature scheme [62] can be designed so that the certificate of a particular node is signed by combining $t+1$ partial signatures generated by $t+1$ nodes respectively, and the certificate can be verified by the CA's public key which is known by each node in the network.

Figure 11.3 shows a $(5,3)$-threshold signature scheme, in which the CA's private key is divided into 5 shares for each node: $s1, s2, ..., s5$. A message m (the identity and public key of a particular node) could be signed by any three of the nodes. In Figure 3(a), nodes $1, 2$ and 3 generate the partial signatures of message m as follows: $PS(m, s1)$, $PS(m, s2)$ and $PS(m, s3)$. The three partial signatures could be combined to obtain the certificate $\mathcal{C}$, which is the same as it is signed by the CA's private key. In Figure 3(b), nodes 4 and 5 are compromised by the attackers, but the two malicious nodes can not generate a valid certificate by themselves because at least three partial signatures are needed to be combined to sign a message.

This example shows that although a compromised node could also generate an incorrect partial signature, which would yield an invalid signature, a combiner can verify the validity of a computed signature using the CA's public key. In case the verification fails, the combiner tries another set of $t + 1$ partial signatures. This process continues until the combiner constructs the correct signature from $t + 1$ correct partial signatures.

The scheme described above was proposed in [62] for wireless ad hoc networks. Compared with ad hoc networks, WMNs are more favorable for utilizing the threshold cryptography key management scheme. First, WMNs is typically operator-managed, which makes it easier to pre-establish the distributed central authority (the CA's public key and private key shares) in WMNs than in ad hoc networks. Moreover, the nodes in WMNs are usually not mobile and hence do not rely on the battery power supply. Therefore, the asymmetric cryptography computation can be frequently processed in WMNs without much concern of the resource limitation.

There exists another public-key management scheme [41] in which two nodes can authenticate each other by finding a certificate chain between them. This scheme differs from the above in that it proposes a full-organized public key management system, where security does not rely on any trusted authority, not even in the initialization phase. Although the operator-managed WMNs do not require such a full self-organization key management, the certificate chain approach in [41] poses an interesting question: if A can authenticate B which in turn can authenticate C, is it 100% safe for A to authenticate C? In other words, even if A can authenticate B, should A fully trust what B trusts (that is, C is authentic)? Furthermore, we can regard the whole process of authentication as a trust evaluation problem: "do I trust that you are who you claim you are?" The trust model for securing WMNs will be discussed in Section 11.4.5.

11.3.2 Secure Routing

In WMNs, the data travel via multiple wireless hops from the source node to its destination. The routing protocols for WMNs are designed to achieve:

- Self- configuration of the routing tables.
- Self-adaptation to changes in the wireless link quality.
- Maximized performance metrics such as end-to-end delay, throughput and packet loss rate.

The routing protocols for wireless ad hoc networks have also similar requirements such as routing through wireless multi-hop links, self-configuration and self-adaptation. Although very few routing protocols have been proposed specifically for WMNs, the similarities between WMNs and wireless ad hoc networks make it feasible for WMNs to borrow the ideas from the domain of wireless ad hoc networks, which have been extensively studied in the literature. For example, in 802.11s [63], the IEEE 802.11 standard for wireless LAN mesh networking, the Ad hoc On Demand Distance Vector (AODV) protocol [46] is extended to Radio Metric AODV (RM-AODV), an on demand routing protocol for wireless LAN mesh networks.

The self-configured and self-adapted wireless multi-hop routing mechanisms rely on the fact that all participating nodes cooperate with each other without disrupting the operation of the protocol. Without proper protection, the routing mechanisms could be attacked by both *external* and *internal* attacks [4].

External Attacks

Due to the shared nature of the wireless medium, anyone with a suitable hardware is able to send information into the medium. Indeed, external attackers can inject fabricated routing information into the network or maliciously alter the content of routing messages exchanged between the nodes. Therefore, the correctness of routing information exchange is vital to any routing protocols.

To secure routing, some proactive ad hoc routing protocols, such as DSDV [45] and OLSR [11], require that the routing messages are exchanged periodically between all the nodes so that each node has a view of the whole network's topology, based on which the routing decisions are made. The malicious routing messages with false topology information will make some nodes getting an incorrect view of the topology. On the other hand, for reactive routing protocols, such as AODV and DSR [26], the routing messages are exchanged between the source, destination and the intermediate nodes in order to find the best route after the source node initializing a route discovery process sends a packet to the destination. The route discovery process will then end up with a false route with the existence of the malicious routing massages

To protect routing messages exchanging from attacks, the routing protocols need effective mechanisms to:

- Authenticate the received routing message to validate that it is sent by a legitimate node.
- Check the integrity of the received routing message to validate that it has not been altered by the attacker.

Such mechanisms are often achieved by employing cryptographic solutions.

Asymmetric Cryptography Approach:

As described in Section 11.3.1, asymmetric cryptography based authentication can prevent the fabricated routing information. When sending a routing message, the sender attaches the certificate signed by CA to the message and digitally signs the message with its private key. Upon receiving a routing message, the receiver first checks the validity of the certificate attached to the message using the CA's globally known public key and then checks the message's integrity using the digital signature and the sender's public key. ARAN [52] is an on demand protocol utilizing the digital signature scheme, in which the routing messages such as route discovery packet, reply packet and shortest path confirmation messages are signed by the sender and validated by the receiving node.

Symmetric Cryptography Approach:

In this scheme, a single secret key is used for both encryption and decryption.

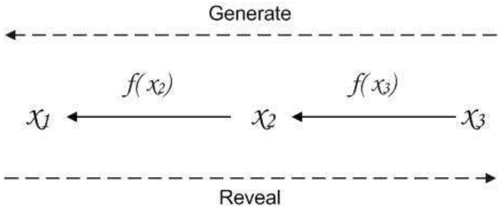

Fig. 11.4. One-way Hash Chain

One of the most common schemes is one-way hash chains. As cited in [4], *"A one-way hash function is a function that takes an input of arbitrary length and returns an output of fixed length"*. Computing the input of a hash function from the output requires a huge amount of computation resource, so hash functions are computationally expensive to reverse. A hash chain is generated by applying a given hash function $f()$ repeatedly (n times) to an initial input x and obtaining a chain of outputs $f_i(x)$, $i = 1, 2..., n$. The protocols utilizing one-way hash chains require that a shared secret, $f_j(x)$, exists so that the validity of $f_i(x)$ for $i < j$ can be checked by applying the hash function $j - i$ times on it and comparing the result with $f_j(x)$. Figure 11.4 is an example of a one-way hash chain with length three. The chain is generated by applying the hash function $f()$ on x_3 such that $x_2 = f(x_3), x_1 = f(f(x_3)) = f_2(x_3)$. Since x_1 is a shared secret, x_2 and x_3 could be validated by checking if $f(x_2) = x_1$ and $f_2(x_3) = x_1$.

For an instance, TESLA [47] is a broadcast authentication protocol based on one-way hash chains. In this protocol, the receivers need to buffer a message to wait for the delayed key disclosure from the sender, which requires time synchronization. TESLA is employed by a distance vector protocol, SEAD [24], and a source routing protocol, Ariadne [23].

Compared with the digital signature scheme, the one-way hash chain scheme has the advantage of light weight computation cost and no need to maintain a globally trusted CA, but it requires clock synchronization of all the nodes in network. Furthermore, in TESLA, a received message has to be stored in buffer waiting for the disclosed key to authenticate it before being processed, which degrades the performance of the network.

To overcome such limitations, a hybrid approach, SAODV [60] has been proposed where the non-mutable fields of the routing messages are signed by asymmetric cryptography while the mutable field, hop count, is authenticated using a hash chain so that the expensive asymmetric cryptographic computation is only needed for the source and destination nodes and the intermediate nodes authenticate the hop count using hash function.

The one-way hash chain scheme is more favorable for wireless ad hoc networks in which the nodes are battery-powered and the computation resource is limited. Furthermore, the node mobility in wireless ad hoc networks makes it difficult to maintain an online CA available for all the nodes. However, the nodes in WMNs are not mobile and they do not rely on battery power supply. So the digital signature scheme is a better choice for WMNs if the clock synchronization is hard to achieve.

Internal Attacks

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. Here, we discuss some countermeasures to internal attacks.

Packet Leash

In [25], a challenging attack, called the wormhole attack is defined. If an attacker gets control of two nodes with a wired communication link (tunnel) between them, the wormhole attacks could be launched by sending all the packets received from one node through the tunnel and replaying these packets at the other end of the tunnel. Figure 11.5 shows an example of wormhole attack [4]. Because the packets through the tunneled link ($A \rightarrow B$) arrive sooner than the packets through the multi-hop wireless links ($1 \rightarrow 2 \rightarrow 3 \rightarrow 4$), nodes 2 and 3 are excluded from the network, and the traffic between nodes 1 and 4 is completely under the control of the attacker.

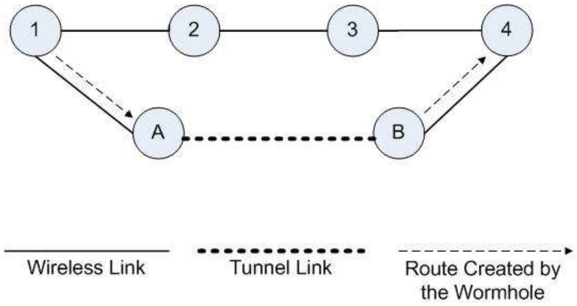

Fig. 11.5. A wormhole attack performed by colluding malicious nodes A and B

The Packet Leash solution [25] 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.

Neighbor Monitoring:

The neighbor monitoring approach to discover misbehaving nodes takes the advantage of the broadcast nature of wireless network: any packet sent in to the air can be overheard by the neighbor nodes. After a node sends a packet to its neighbor, it could monitor the behavior of its neighbor to see whether it forwards the packet to the next hop without any misbehavior. Each node maintains a rating record of all the nodes it knows, and the misbehaviors of a particular node being detected cause the rating to decrease. The low rating nodes are considered misbehaving or non-trust nodes so that they will not be included in the route of forwarding packets from source to the destination nodes.

Based on this approach, two other solutions [42] and [8] have been proposed to defend against packet forwarding attacks.

Byzantine Failure Resilience:

In [5], an on-demand secure routing protocol is proposed that is resilient to Byzantine failures caused by Byzantine behavior, which is defined as “any action by an authenticated node that results in disruption or degradation of the routing service”. The failure refers to “any disruption that causes significant loss or delay in the network”. The detection of such failures is based on acknowledgements (*acks*). The destination node sends an *ack* back to the source node when receiving a packet. If an *ack* is not received after a certain time, the source node assumes it has been lost. The number of lost (to the same destination) exceeding a threshold triggers the Byzantine fault detection.

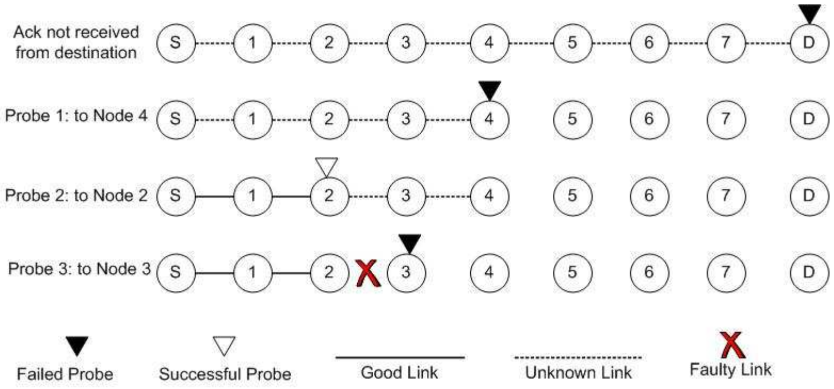

Fig. 11.6. Byzantine fault detection: the faulty link is located after 3 probes [5]

Figure 11.6 illustrates the detection process [5]. The source node launches a binary search of all the links along the path by probing the intermediate nodes. The normally behaving nodes sends *acks* back to the source when receiving the probe. Half of the links are excluded from the suspects of failure for each probe. The faulty link will be identified after $\log n$ probes, where n is the number of hops between the source and destination. After the failure is located, the source node will start a new route discovery process and try to bypass the faulty link.

Figure 11.7 summarizes various schemes for secure routing that may be applied to WMNs.

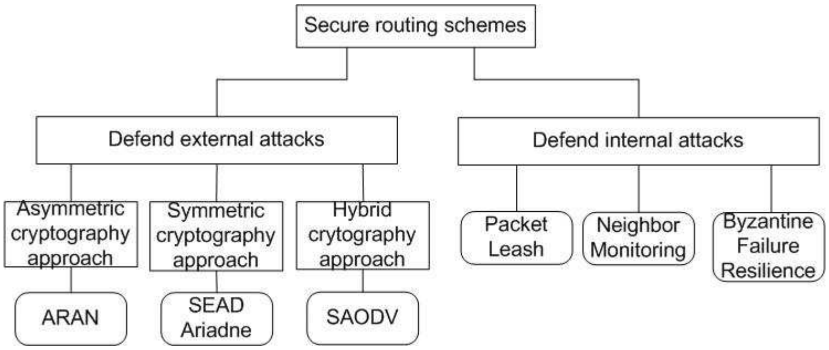

Fig. 11.7. Secure Routing Protocols

11.3.3 Secure Location Information

As mentioned before, most routing protocols in WMNs are adopted from ad hoc networks, including both topology-based and geographic routing schemes. For geographic routing schemes [19, 6, 12, 22], the location information of the mesh routers are crucial to multi-hop routing schemes and thus subject to attack.

For securing location information, two general methods are currently employed: correctly compute location information, and verify location claims.

Generally speaking, a mesh router's location can be determined either with the help of GPS or some location-known beacons. The goal of the first approach is to ensure the accuracy of location computation even when the calculation is under attack. For example, although GPS is the most common approach to get the geographic position information, no secure protection for public civilian GPS makes it vulnerable to different kinds of attacks [34]. As an example, a *signal-synthesis* attack can fool a receiver to connect to a device present at some pretended location. Similarly, *selective-delay* attack can convert a signal received at time t and position r into another signal that would have been received at earlier time t' and position r'.

To defend such attacks, an information-hiding based asymmetric security mechanism is proposed in [34]. The essence of the scheme is to introduce time asymmetry through a delayed disclosure of despreading key. Specifically, when a spread-spectrum broadcast signal temporarily hidden in the background noise is transmitted, the receivers store the whole radio band in buffer. And the despreading key is not published until the delay is larger than the uncertainty of the local clock in the receiver. In this way, both signal-synthesis and selective-delay attack can be easily detected.

For the schemes that utilize beacons, a cryptographic-based scheme, SeRLoc (Secure Range-independent Location), is proposed to enable the nodes to determine their location even in the presence of malicious adversaries [37]. In SeRLoc, some nodes which re equipped with directional antennas and have acquired the location and the orientation through GPS receivers are termed “locator”. Each locator transmits different beacons at each antenna sector containing its coordinates and the angles of the antenna boundary lines with respect to a common global axis. The nodes will collect the beacons from all locators they can hear and then determine their location. To protect the localization information, a global symmetric key is shared between nodes and locators. Moreover, every sensor shares a symmetric pairwise key with every locator so that the beacons from each locator can be authenticated. The analysis shows SeRLoc is robust against several attacks including wormhole attack, Sybil attack and compromised nodes. However, one limitation of this scheme lies in that it assumes locators are always trusted and cannot be compromised by an adversary.

Besides directly securing the location calculation, the location information may also be verified from spoofing. Due to the fact that the mesh routers in WMNs are usually static, a claim of location information made by the mesh routers to the mesh clients would often be more than just location calculation. Therefore, location verification would be more agreeable in WMNs. To validate a node is in a region of its position claim, different techniques such as exampling by public key based challenge-response protocol [7] and robust statistical methods [39, 40, 36] have been employed. In addition, by exploiting the physical properties of sound and RF signal propagation in wireless communication, a simple protocol called “Echo”, has been proposed [53] that requires no cryptography nor time synchronization. Another mechanism, called Verifiable Multilateration (VM), achieves both secure position computation and location verification [9]. All sch schemes proposed for wireless sensor networks seem to be applicable to WMNs as well.

11.3.4 Modeling Virus Propagation

Given the fast emergence of computer viruses in the host computers and the Internet, the threat of virus in wireless networks is not an unrealistic panic. In fact, there have been some viruses that spread over the air, such as the Brador virus [55] and the Cabir worm [18] for the mobile devices, the evil twin and the promiscuous client for Wi-Fi users [16].

In order to effectively defend the virus attack, one important issue is how to model the virus propagation to get a better understanding on the virus behavior in wireless networks. Inspired by biological modeling techniques, some researchers have adopted Epidemic theory to model the virus propagation problem.

Epidemic theory [3] is the study of the dynamics of how contagious diseases spread in a population, resulting in an epidemic. It can mathematically model the progress of the infectious diseases and measure its outcome in relation to a population at risk. In general, the population is divided into three groups: the *susceptible* (S), who are healthy and are subjective to catching the disease; the *infected* (I), who have the disease and can transmit it; and the *removed* (R), who have had the disease and are recovered now. In general, there are two popular models to characterize the infection spread: *Susceptible Infected Susceptible* (SIS) and *Susceptible Infected Recovered* (SIR). The difference between these two models is the following. For an individual who acquires infection, this individual can becomes susceptible again after some infectious period in the former model, while in the latter model, the individual becomes immune to further infections after recovery.

An important aspect in Epidemic theory is that the phase transition of the spreading process is dependent on an threshold of the epidemic parameter. That is, when the epidemic parameter is above the threshold, the infection will spread out and become persistent; on the contrary, if the parameter is below the threshold, the infection will die out. Therefore, identifying this threshold value is critical in the study of how an epidemic spreads and how it can be controlled [13].

Epidemic theory has been employed to investigate virus spreading problem not only in wirelined networks, but also in wireless networks. Here, we list two schemes that apply Epidemic theory to model the worm and compromised nodes propagation, respectively.

Topologically-Aware Worm Propagation Model (TWPM):

TWPM was proposed in [33] for wireless sensor network. By parameterizing the effects of physical, MAC and network layers on the worm propagation, the authors incorporate all these parameters in the SIS model and analytically derive the worm propagation model from a partial differential equation. With some assumptions including regular two-dimensional grid topology and constant infection rate, they also obtained a closed-form expression for the TWPM model.

Although this work is originally proposed for wireless sensor networks, it has the potential to adapt to WMNs by taking real topology into account. In WMNs, most mesh routers have a neighbor list, either for routing purpose or infrastructure maintenance. Unfortunately, the scanning worms, called *topologically-aware worms*, can take advantage of this list and spread the infection quite effectively by just communicating to its next-hop neighbors.

Modeling Node Compromise Spread:

Unlike TWPM using a differential equation approach to solve the problem, a network and graph theoretic based technique was proposed to model node compromise spread in wireless sensor networks [14].

In general, no matter whether its is sensor network or mesh network, for secure communication, a secret key used to encrypt the messages is shard between each communication party. However, without physical protection, the nodes are subject to capture. Once a node is captured, its keys are known by the attackers, thus affecting communications with all the compromised node involved. In [14] is studied how an adversary capturing one or two nodes and thereby extracting the secret keys, can possibly propagate the node compromise to the whole network.

By constructing a random graph model of the key sharing overlay graph of the sensor network and presenting the compromised propagation model as a poisson process, this work investigates the probability of a breakout (when the whole network is compromised) and also computes the size of the compromised clusters of nodes under no breakout. Additionally, the effects of two scenarios

– recovery and no recovery – on the compromised nodes recovery are analyzed in this work.

Although this scheme is proposed for wireless sensor networks, the essential idea and basic assumptions are still valid for WMNs. Therefore, they shed some light on modeling virus propagation in WMNs.

11.4 Summary and Open Problems

Wireless mesh networks (WMNs) possess some nice features and promise to offer better wireless network connectivity and larger coverage area. On the other hand, these features also pose significant challenges to the network security. In this chapter, we have reviewed some existing solutions that could potentially be employed to secure WMNs. The threshold signature and TESLA schemes could be utilized to realize the authentication between mesh routers. Such authentication schemes also help routing protocols such as ARAN, SEAD and Ariande to defend against external attacks. The Packet Leash, neighbors monitoring and Byzantine failure resilience solutions provide possible approaches to detect and countermeasure internal attacks to the wireless multi-hop routing protocols. The secure location information solutions for wireless sensor networks can help securing the geographic routing schemes. However, there are still a lot of open problems for security in WMNs that need further investigation. These are discussed below.

11.4.1 Secure Medium Access Control

The IEEE 802.11 medium access control (MAC) protocol has been adopted as the de facto MAC scheme of WMNs in many research projects and commercial products ([51, 10, 44]). The cryptographic approach for securing the 802.11 MAC protocol had evolved from Wired Equivalent Privacy (WEP) protocol to IEEE 802.11i standard [64].

In IEEE 802.11i, an authentication server (AS) is incorporated to authenticate the mobile node (MN) that tries to associate with the mesh access point (AP). IEEE 802.11s [63], the IEEE standard for wireless LAN mesh networking, utilizes IEEE 802.11i based security mechanism to provide link-by-link security in WLAN mesh networks. According to IEEE 802.11s, the AS is collocated with a mesh point (MP) or located in a remote entity to which an MP has a secure connection. It is assumed by the standard that an MP could establish a secure connection to the remote AS after establishing a secure connection with the MP that collocates with the AS or has a secure connection with the AS. But the standard neither proposes how to establish the secure connection nor evaluates the practicality of establishing such a secure connection. Furthermore, the 802.11i security framework is a centralized structure in which the MNs submit authentication request to AP which in turn communicates with AS to decide whether to authenticate or not. But such a hierarchical structure is not suitable for WMNs in which two MPs need to authenticate each other before they start communication; in other words the MPs are both the authentication supplicants and the authenticator. This mutual authentication requires that both MPs have a secure connection with AS, which is impractical in WMNs.

The cryptographic approach to secure the MAC protocol is to answer the question “who can utilize the mesh medium?” However, it does not address the issue of fair utilization of the medium. The attacks to the backoff scheme of IEEE 802.11 MAC protocol break the fairness of using the wireless medium. The IEEE 802.11 MAC protocol uses CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) scheme to reduce the probability of collisions in accessing the medium. If the sender senses the channel is busy before transmission, it defers the transmission for a random backoff time. Simulation results reported in [35] show that if a misbehaving node selects smaller backoff time than other nodes complying the protocol, it will obtain more than its fair share of the bandwidth and degrade the throughput of well-behaved nodes.

A modification to IEEE 802.11 protocol is proposed in [35] to countermeasure this attack. In this proposal, the sender does not decide the value of random backoff time. Instead, the receiver selects a backoff time value and sends it to the sender. The receiver can identify whether a sender deviated the protocol by monitoring the time intervals between the sender’s transmissions and comparing them with the backoff time assigned to the sender. If the deviation is identified, the receiver will penalize the sender by assigning larger backoff values to it than those assigned to normal nodes. Such a scheme could restrict the selfish nodes to get more bandwidth share, but it could do nothing to prevent the malicious nodes from attacking the backoff scheme if the malicious nodes that do not care how much bandwidth to share, keep transmitting data without backoff time at all. Such an attack is a denial of service (DoS) attack to the MAC layer protocol, which is still an open issue for the wireless networks relying on the CSMA/CA scheme.

11.4.2 Defense Against DoS Attacks

Denial of Service (DoS) attacks can reduce the availability of resource and result in massive service disruption. A robust WMN application should be resilient to DoS attacks and be able to defend against such attacks launched either by the end devices or other adversaries.

DoS attacks could happen at all the layers in the protocol stack from the physical to the application layer [56]. Usually different approaches have been employed in different layers of the protocol. For instance, at the physical layer, the most common defense against DoS (e.g., jamming) is spread spectrum. At the MAC layer, some special measures such as rate limitation and error correcting code may be used to defend against DoS attacks. Although most of routing schemes in WMNs are adopted from ad hoc networks, the characteristics of WMNs, especially multi-hop routing, should be taken into account for the defense mechanisms at the network layer. In particular, a poorly designed multi-hop routing scheme may introduce traffic unfairness or starvation, which even leads to DoS for some mesh routers that are close to the backbone network.

Even though there is no universal way to defend against DoS attacks, a systematic framework that can comprehensively consider all these issues at the beginning design phase would be more effective. Furthermore, an integrated, cross-layer security solution is more desirable.

11.4.3 Embedded Security Schemes vs. System Level Monitoring

The majority of the current security mechanisms are embedded in the network protocols, so they usually focus on some particular attacks at a specific layer and are efficient for outside (external) attacks.

An alternate approach is to design a cross-layer framework that can monitor in real time the whole network to detect attacks and respond promptly. Compared with the embedded schemes, the monitoring framework can work as an intrusion detection system (IDS) to detect any real-time abnormality. Since the intrusion includes not only the attacks launched by the outsiders but also the misuse from the inside, it is more effective and flexible to defend insider (internal) attacks.

However, WMNs pose new challenges for intrusion detection design. First, mesh routers that are usually not physically protected are subject to capture. Once a mesh router gets captured, all of its secret information including keys is disclosed to the adversary. These corrupted mesh routers not only compromise the whole network security, but can also modify the network configuration or inject false information to disturb the routing schemes. Moreover, the delay introduced by multi-hop communication causes difficulty for traffic monitoring. Therefore, how to detect the corrupted mesh routers and inform the whole network in a timely manner is still an open problem in WMNs.

11.4.4 Integration Issues

One main advantage of WMNs is that it enables us to integrate various existing networks such as Wi-Fi, cellular networks, sensor networks, etc, through the gateways. However, this benefit also brings related vulnerability in WMNs.

Various (heterogeneous) networks as part of WMN clients imply their properties may have significant differences as well. For example, although the public key cryptography is a common approach for most networks for authentication, it may be computationally too costly for sensor networks. Naturally, WMNs should be able to customize the security schemes according to the characteristics of network clients while not compromising the security features of the overall network. Therefore, the interworking of several different types of networks poses a new challenge to securing WMNs.

11.4.5 Trust Relationships

Some security issues, such as establishing certificate chains [41] and collaborating between mesh routers to implement routing protocols or reduce the authentication delay by sharing the security key [21], imply the existence of trust relationships between different entities of WMNs. A mechanism to define how to establish and quantify such trust relationships could help the mesh routers to make proper decisions in the presence of potential attacks, and thus improve the reliability and robustness of the networks.

Although the trust and reputation systems have been extensively and successfully applied in E-commerce applications [50, 57, 59], public key authentication [43, 49, 38, 20], peer-to-peer networks [32, 58], mobile ad hoc networks

[17, 54] and wireless sensor networks [61], some characteristics of WMNs differ from these networks or applications. Therefore, there is a need for new trust establishment and management in WMNs.

On one hand, the existence of infrastructure/backbone in WMNs favors the trust establishment. Unlike ad hoc networks supporting node mobility, most of the mesh routers are static. Intuitively, a trust infrastructure could be established on top of the fixed WMN backbone. And once it is created, the entities and their trust chains will be permanently present.

On the other hand, the erroneous and uncertain nature of wireless links cannot guarantee stable connectivity between the mesh routers even they physically exist. Moreover, the quality of wireless links may also change frequently. While in traditional applications, the trust relation are usually established and updated based on a long time observation. In WMNs, however, the trust infrastructure should have the capability to respond to temporary disconnections between the mesh routers. Hence the evaluation of the trust relation must be fast enough to promptly reflect the instantaneous changes in the environment.

Moreover, the mesh routers in WMNs can only monitor their neighbors with the radio range which means that the trust relation is establishment locally and thus distributed. Therefore, when the packets are routed via multi-hop links, the trust should be uniformly evaluated. As a result, it is necessary to develop some scheme that can manage the trust propagation. In [31], a method of Trust Network Analysis with Subjective Logic (TNA-SL) is designed based on graph simplification and trust derivation with subjective logic. TNA-SL expresses and propagates both positive and negative trust values and takes the confidence level (certainty) into account, which might make it an appropriate model for calculating and evaluating quantified trust in WMNs. There exist other works that have been proposed to define the trust transitivity and manage trust propagation [28, 30, 29, 27]. However, the validation and performance of such schemes under real WMNs applications needs further investigation.

Besides the above issues, a node in a WMN may not always be able to monitor its neighbors if they are using different radio interfaces. In addition, how to effectively make the trust relation globally available to the whole network is also a challenging problem in WMNs. However, the trust based system fits the characterizes of WMNs and provides a promising solution to secure WMNs.

Conclusion

In this chapter, we addressed some security issues in WMNs and survey state-of-the-art solutions that have either been applied to WMNs or have he potential to be adopted. It is worth noting that no panacea exists that can solve all the problems identified. In fact, there are currently more open problems that need further investigation than solutions to secure WMNs. Depending on the specific applications and requirements, some approaches need to work together to achieve the desired security, or a cross-layer solution should be developed while designing WMN applications.

References

1. I. Akyildiz and W. Wang, “A survey on wireless mesh networks”, *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23-S30, Sept. 2005.
2. M. Alicherry, R. Bhatia and L. Li, “Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks”, in *Proc. ACM MobiCom’05*,Cologne, Germany, 58–72 Aug, 2005.
3. R. M. Anderson and R. M. May, *Infectious Diseases of Human: Dynamics and Control*, Oxford Univ. Press, Oxford, 1991.
4. P. G. Argyroudis and D. O’Mahony, “Secure routing for mobile ad hoc networks”, *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3, pp. 2-21, Atlanta, GA, USA, 2005.
5. B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, “An on-demand secure routing protocol resilient to byzantine failures”, in *Proc. ACM WiSe’02*, pp. 21-30, Sept. 2002.
6. P. Bose, P. Morin, I. Stojmenovic and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks”, *Wireless Networks*, vol. 7, no. 6, pp. 609-616, Kluwer Academic Publishers, 2001.
7. S. Brands and D. Chaum, “Distance-bounding Protocols”, *EUROCRYPT ’93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, vol. 765 of LNCS.
8. S. Buchegger and J. L. Boudec “Performance analysis of the CONFIDANT protocol”, in *Proc. ACM MobiHoc’02*, pp. 226-236, Lausanne, Switzerland, Jun. 2002.
9. S. Capkum and J. Hubaux, “Secure positioning of wireless devices with application to sensor networks”, in *Proc. IEEE INFOCOM’05*, pp. 1917- 1928, Mar. 2005.
10. Overview: Wireless Mesh Networking,
http://www.cisco.com/en/US/netsol/ns175/
networking_solutions_products_generic_content0900aecd80529a46.html, 2007.
11. T. H. Clausen, G. Hansen, L. Christensen and G. Behrmann, “The optimized link state routing protocol, evaluation through experiments and simulation”, in *4th International Symposium on Wireless Personal Multimedia Communications*, Aalborg, Denmark, 2001.
12. S. Datta, I. Stojmenovic and J. Wu, “Internal node and shortcut based routing with guaranteed delivery in wireless networks”, in *Proc. IEEE International Conference on Distributed Computing and Systems Workshops, Cluster Computing*, pp. 461-466, April 2001.
13. P. De and S. K. Das, “Epidemic Models, Algorithms and Protocols in Wireless Sensor and Ad hoc Networks,” *Handbook on Wireless Sensor Networks*, John Wiley, 2007.
14. P. De, Y. Liu and S. K. Das, “Modeling node compromise spread in sensor networks using Epidemic theory”, in *Proc. IEEE WOWMOM’06*, pp. 237-243, Washington, DC, Jun. 2006.
15. Y. Desmedt, “Threshold cryptography”, *European Transactions on Telecommunication*, vol. 5, no. 4, pp. 449-457, 1994.
16. C. Elliott, *wireless threats to your business,*
http://www.microsoft.com/smallbusiness/resources/technology/
broadband_mobility/6_wireless_threats_to_your_business.mspx.
17. L. Eschenauer, V. Gligor and J. Baras “On trust establishment in mobile ad-hoc networks”, in *Proc. of 10th International Workshop on Security Protocols*, Cambridge, UK, April 2002.
18. P. Ferrie, P. Szor, R. Stanev and R. Mouritzen, “Security response: SymbOS.Cabir”, 2004. Symantec Corporation.

19. H. Frey, "Scalable geographic routing algorithms for wireless a hoc networks", *IEEE Network Magazine*, Jul./Aug. pp. 18-22, 2004.
20. R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust", in *Proc. of International World Wide Web Conference*, pp. 403-412, May 2004.
21. J. Hassan, H. Sirisena and B. Landfeldt, "Trust-based Fast Authentication in Multiowner Wireless Networks", IEEE Transactions on Mobile Computing, in press.
22. M. Heissenbuttel and T. Braun, "BLR: beacon-less routing algorithm for mobile ad hoc networks", *Computer Communications Journal*, vol. 27, no. 11, pp. 1076-1086, July 2004.
23. Y. C. Hu, D. B. Johnson and A. Perrig, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in *Proc. ACM MobiCom'02*, pp. 12-23, Sept. 2002.
24. Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", in *Proc. WMCSA'02*, pp. 3-13, Jun. 2002.
25. Y. C. Hu, D. B. Johnson and A. Perrig, "Packet leashes: a defense against wormhole attacks in wireless networks", in *Proc. IEEE INFOCOM'03*, vol. 3, pp. 1976-1986, March/April 2003.
26. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks", *Mobile Computing*, Kluwer Academic Publishers, 1996.
27. A. Josang, "Trust-based decision making for electronic transactions", L. Yngstrom and T. Svensson, editors, in *Proc. NORDSEC'99*. Stockholm University, Sweden, Stockholm University Report 99-005, 1999.
28. A. Josang, "A logic for uncertain probabilities", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279-311, June 2001.
29. A. Josang and R. Ismail, "The Beta reputation system", in *Proc. of the 15th Bled Conference on Electronic Commerce*, Bled, Slovenia, June 2002.
30. A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, March 2007.
31. A. Josang, E. Gray and M. Kinateder, "Simplification and analysis of transitive trust networks", *Web Intelligence and Agent Systems Journal*, vol. 4, no. 2, pp. 139-161, 2006.
32. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in P2P networks", in *Proc. WWW'03*, pp. 640-651, Budapest, Hungary, May 2003.
33. S. A .Khayam and H. Radha, "A topologically-aware worm propagation model for wireless sensor networks", in *Proc. ICDCSW'05*, pp. 210-216, Washington, DC, USA, June 2005.
34. M. Kuhn, "An asymmetric security mechanism for navigation signals", in *Proc. of the Information Hiding Workshop*, pp. 23-25, May 2004.
35. P. Kyasanur and N. H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks", in *International Conference on Dependable Systems and Networks*, pp. 173-182, 2003.
36. L. Lazos, R. Poovendran and S. Capkum, "ROPE: robust position estimation in wireless sensor networks", in *Proc. IEEE IPSN'05*, pp. 324-331, April 2005.
37. L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless Sensor Networks", in *Proc. ACM WiSe'04*, pp. 21-30, Philadelphia, PA, USA, Oct. 2004.
38. R. Levien and A. Aiken, "Attack-resistant trust metrics for public key certification", in *Proc. of 7th USENIX Security Symposium.*, pp. 229-242, Jan. 1998.

39. Z. Li, W. Trappe, Y. Zhang and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks”, in *Proc. IEEE IPSN'05*, pp. 91-98, April 2005.
40. D. Liu, P. Ning and W. Du, “Attack-resistant location estimation in sensor networks”, in *Proc. IEEE IPSN'05*, pp. 99-106, April 2005.
41. H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, “Self-securing ad hoc wireless networks”, in *Proc. IEEE ISCC'02*, pp. 567-574, July 2002.
42. S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in *Proc. ACM MobiCom'00*, pp. 255-265, Boston, Massachusetts, USA, August 2000.
43. U. Maurer, “Modeling a public-key infrastructure”, in *Proc. Eru. Symp. Res. Comput. Security*, vol. 1146, pp. 325-350, Lecture Notes in Computer Science, 1996.
44. Motorola. Motorola's Mesh Networking Technology & Industry (IEEE) Standards, http://www.motorola.com/mesh/pages/technology/industry_standards.htm.
45. C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers”, in *Proc. ACM SIGCOMM'94* , pp. 234-244, London, UK, 1994.
46. C. Perkins, “Ad hoc On-Demand Distance Vector (AODV) routing”, *IETF RFC 3561*, 2003.
47. A. Perrig, R. Canetti, D. Tygar and D. Song, “The TESLA broadcast authentication protocol”, *RSA Cryptobytes*, vol.5, no. 2, pp. 2-13, 2002.
48. A. Raniwala and C. Tzi-cker, “Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network”, in *Proc. IEEE INFOCOM'05*, pp. 2223-2234, March 2005.
49. M. K. Reiter and S. G. Stubblebine, “Resilient authentication using path independence”, *IEEE Transactions on Computer*, vol. 47, no. 12, pp. 1351-1362, Dec. 1998.
50. P. Resnick and R. Zeckhauser, “Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system”, *The Economics of the Internet and E-Commerce*, M. R. Baye, editor, volume 11 of Advance in Applied Microeconomics, Amsterdam, Elsevier Science, 2002.
51. Roofnet. http://pdos.csail.mit.edu/roofnet.
52. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. M. BeldingRoyer, “A secure routing protocol for ad hoc networks”, in *Proc. IEEE ICNP'02*, pp. 78-87, Nov. 2002.
53. N. Sastry, U. Shankar and D. Wagner, “Secure verification of location claims”, in *Proc. ACM Workshop on Wireless Security*, pp. 1-10, San Diego, CA, 2003.
54. Y. Sun, W. Yu, Z. Han and K. J. R. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks”, *IEEE JSAC special issue on Security in Wireless Ad hoc Networks*, vol. 24, no. 2, pp. 305- 317, Feb. 2006.
55. R. Wong and I. Yap, “Security information: virus encyclopedia: technical details”, *Trend Micro Incorporated*, 2004.
56. A. Wood and J. Stankovic, “Denial of service in sensor networks”, *IEEE Computer*, vol. 35, no. 10, pp. 54-62, 2002.
57. B. Yu and M. P Singh, “A social mechanism of reputation management in electronic communities”, in *Proc. of the 4th International Workshop on Cooperative Information Agents*, pp. 154-165, July 2000.
58. B. Yu, M. Singh and K. Sycara, “Developing trust in large-scale peer-to-peer systems”, in *Proc. of 1st IEEE Symposium on Multi-Agent Security and Survivability*, pp. 1-10, Aug. 2004.
59. G. Zacharia, A. Moukas and P. Maes, “Collaborative reputation mechanisms in electronic marketplaces”, in *Proc. IEEE HICSS'99*, pp. 8026, Jan. 1999.

60. M. G. Zapata and N. Asokan, “Securing ad hoc routing protocols”, in *Proc. IEEE WiSe’02*, pp. 1-10, Atlanta, GA, USA, 2002.
61. W. Zhang, S. Das and Y. Liu “A trust based framework for secure data aggregation in wireless sensor networks”, in *Proc. IEEE SECON’06*, pp. 60-69, Sept. 2006.
62. L. Zhou and Z. J. Haas, “Securing ad hoc networks”, *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.
63. “Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs, 2006”.
64. “IEEE Std 802.11i/D4.1”, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements*, 2003.