A Survey on Security in Wireless Mesh Networks

Ping Yi, Yue Wu, Futai Zou and Ning Liu

Network Information Security Research Center of the Ministry of Education, School of Information Security Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, People's Republic of China.

Abstract

Wireless mesh networks is a new emerging field with its potential applications in extremely unpredictable and dynamic environments. However, it is particularly vulnerable due to its features of open medium, dynamic changing topology, and cooperative routing algorithms. The article surveys the state of the art in security for wireless mesh networks. First, we analyze various possible threats to security in wireless mesh networks. Second, we introduce some representative solutions to these threats, including solutions to the problems of key management, secure network routing, and intrusion detection. We also provide a comparison and discussion of their respective merits and drawbacks, and propose some improvements for these drawbacks. Finally, we also discuss the remaining challenges in the area.

Keywords

Intrusion detection, Key management, Network, Secure network routing, Security, Wireless mesh networks.

1. Introduction

A wireless mesh network (WMN) is an emerging wireless networking technology. A WMN is multihop routing and forwarding by a middle wireless router. It has an ability to cover a wide geographic area with a limited transmit power accordingly. A WMN has several favorable features, such as dynamic self-organizations, self-configuration, self-healing, easy maintenance, high scalability, and reliable services. A WMN is different from a mobile ad hoc network (MANET) in that it relies on a high-speed back-haul network which is composed by WMN routers. A WMN optimizes network performance by using multiple radios. A WMN can provide gateways to the wired Internet and other wireless services. Due to its unique mesh structure, a WMN has an advantage over traditional MANET and wireless local area network (WLAN) in the areas of reliability, data throughput, antijamming, and extensibility. WMN has been advocated as a cost-effective approach to support high-speed last mile connectivity and ubiquitous broadband access in the context of home network, enterprise networking, community networking, or metropolitan area network [1].

A WMN may be defined as a dynamic, self-organized, self-configured wireless multihop network which is consisted of mesh routers and mesh clients. Each mesh router is responsible for setting up the ad hoc network and maintains mesh connections with other routers within its transmission range. A WMN evolves from the Advanced Tactical Communications Systems (ACTS) which was developed by DARPA and ITT Communication Systems to strengthen the reliability of tactical communication in military network dating back to 1997. In 2000, ACTS and its related technology are officially available for business and civilian application. The IEEE standard for mesh networking started as a Study Group of IEEE 802.11 in September 2003 and soon became a Task Group in July 2004. Currently, the IEEE 802.11 is still in a development stage [2].

Due to ubiquitous architecture and wireless transmit channel, WSN is vulnerable to many security threats, including eavesdropping, impersonation, packet replay, packet modification and denial of service [3].

In this article, we first have a peek into the vulnerabilities of a WMN and overview of merits and deficiencies existing in the solution. The rest of the article is organized as follows. Section 2 gives analysis of the unique security vulnerability in attribute to its network architecture; Section 3 describes key distribution and management; Section 4 compares some main protocols for secure routing; Section 5 discusses the structure and model of intrusion detection. The article concludes with final remarks and future research problems in Section 6.

2. Security Challenges of a Wireless Mesh Network

2.1 Vulnerabilities in Security

There are two types of nodes in a WMN-the mesh router (MR) and the mesh client (MC). MR provides a strong switch ability, minimum mobility, and ignorable battery restriction. Besides the traditional routing facility like gateway and bridge, the MR also supports routing functions specifically designed for a WMN as backbones of the WMN. Meanwhile, the MC could be designed with light architecture with the support of simplest routing ability and light-weighed communication protocols. Therefore, the MC only needs one wireless interface to achieve its function.

Security is a vital problem in the design of a WMN. The client should have end-point-to-end-point security assurance. However, being different from a wired and traditional wireless network, a WMN could easily comprise various types of attacks. Even the WMN infrastructure like MR could be relatively more easily reached and modified by attackers. Therefore, appreciate security measures should be taken. Some common security threats in a WMN are listed below: The designer of the network should try to avoid these threats and keep the reliability of a WMN:

2.1.1 *Physical Threat*

Generally, routers in wired networks are properly protected. Therefore, the attack toward the routers in a wired network is difficult. However, the routers of a WMN are usually deployed outdoors like on roofs of buildings or on street lamps. Therefore, physical protection to the routers of a WMN is very weak. This could cause the attacks to the routers like tempering the information in the router, stealing the private key for authentication stored in the router, or even replacing the router with a malicious one and hence the attacker will be able to connect to network as a legal node and send incorrect routing information. Therefore, secure routing protocols are essential to fight against this kind of attack.

2.1.2 *Confidentiality and Integrity*

Keeping the information sent out by the MR from being tempered or intercepted is very crucial in a WMN. This could be realized by employing encryptions in various layers. Hence finding a viable encryption policy for protecting confidentiality and integrity while minimizing the algorithm complexity and cost in management becomes the foremost problem. The existing WEP is not suitable due to its inherent flaws.

2.1.3 *Authentication in the Wireless Mesh Network*

In order to prevent an unauthenticated node from connecting to the WMN, a strong authentication mechanism is necessary. Every node joining the WMN should be able to verify the identities of others. In a WMN, the lack of terminal facilities causes the necessity of a distributed authentication mechanism to verify every MR or a centralized authentication mechanism by appointing one particular MR as the authentication server. In both the cases, the authentication should be based on security associations outside the IEEE 802.11.

Currently, using traditional asymmetric cryptography for authentication in a WMN is problematic due to the energy limitation and weak computational ability of the MC (usually devices like mobile phone or PDA). It is not practical for these devices to perform such complex computation required by asymmetric cryptography since it will cause a large time delay and accelerate the depletion of the batteries. Besides, this will create a new denial of service (DoS) method by asking MCs to run the authentication program repeatedly, which will take most of the CPU time and deplete the power of the MC.

2.1.4 *Routing Security*

By attacking the routing policy of the WMN, attacker could affect the performance of the network by altering the topological information in the route packet. There are various reasons behind such attacks. The attacker could be reasonable, i.e., the attacker attacks only if the attack could bring benefits like saving the cost of connection or gaining better quality of services, while the attacker could also be malicious who just wants to isolate a part of the WMN or compromise the availability of the network. For example, a reasonable attacker could monitor the communication by attracting data flows to pass a malicious MR by tempering the routing information, or the attacker could start a DoS attack so that all clients could not get what they need.

Attacker could use the following measures to attack the routing mechanism:

Tempering the routing information
Modifying the status of one or more MRs
Start a DoS attack.

Among them, the DoS attack is a simple yet effective attack toward the routing mechanism. It is very easy to implement and penetrable to the defense. A DoS attack performed by a single node could be prevented by monitoring each node's frequency of sending route information and setting a valve of the frequency. However, attackers might also perform a distributed DoS, or DDoS. One method of defense to this kind of attack could be found in [4].

2.2 Possible Attack Types in the Wireless Mesh Network

2.2.1 *Tempering*

Routing protocols in the WMN assume that nodes in the network are cooperative which would not modify any information irrelevant to it while forwarding and hence do not check the integrity of the packet. This allows the attacker to easily temper any specific field in the packet, e.g., the sequence number and number of hops in AODV or node sequences in DSR, and hence results in wrong routing decisions like redirection or route loops, which degrades the performance of the entire network. The fundamental reason for the attacker's ability of tempering the routing information is the lack of integrity check.

2.2.2 *Pretending*

Since the routing protocols cannot verify the source address, attackers could claim themselves as some legal node to join the network. Even worse, the attacker could block the legal node, receiving and sending packet in the name of the legal node. The fundamental reason for the attacker's ability of pretending is the lack of source address verification.

2.2.3 *Forging*

Attackers could forge and broadcast wrong routing information such as declaring some certain link broken or replying with a nonexisting route. This might cause serious problems like loops, or isolated network or node. The fundamental reason for the attacker's ability of forging is the lack of packet data verification.

2.2.4 *Analysis on Topology and Data Flows*

Routing information exists in both the routing request packet and data packet. For example, the data packet in DSR contains the information of nodes from the source to the destination. An attacker could obtain the topological information position and the situation of neighboring nodes by analyzing this information and a further analysis on the amount of flows might even provide information about the function and the role of a particular node. According to this information, the attacker could precisely locate the network control node or, in situations like battles, the commander.

2.2.5 *Resource Depletion Attack*

Attackers could send a large amount of useless packets like a routing request packet or a data packet, depleting the resource of network and nodes, such as bandwidth, memory, CPU, or batteries.

2.2.6 *Wormhole Attack*

Two distant points in the network are connected by a malicious connection using a direct low-latency link called the wormhole link. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, long-range wireless transmission, or an optical link. Once the wormhole link is established, the attacker captures wireless transmissions on one end, sends them through the wormhole link, and replays them at the other end [5].

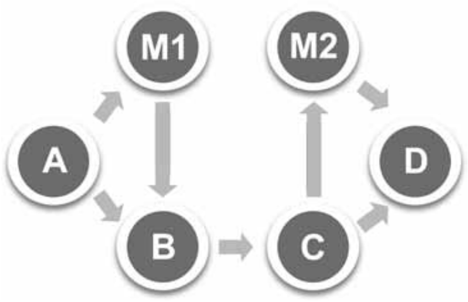

Figure 1: Illustration of a wormhole attack.

Figure 1 is a simple illustration of a wormhole attack. From node A to node D, the normal route should be A-B-C-D. However, if an attacker connects nodes M1 and M2 using a wormhole link, the route becomes S-M1-M2-D; the malicious nodes, i.e., M1 and M2, could then start dropping packets and cause network disruption. The attacker can also spy on the packets going through and use the large amount of information gained to launch other types of attacks and compromise the security of network.

2.2.7 *Blackhole Attack*

While receiving the routing request, the attacker claims to have a link to the destination node even if there is not any and then forces the source to send the packet through it without forwarding the data packet to the next hop [6].

2.2.8 *Rushing Attack*

In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time keeping other nodes busy from processing legal routing request packets [7].

3. Key Management

Due to the dynamic and self-organized nature of the WMN, the traditional certification authority or key distribution center is unreliable in a mesh network. Any break-down of this infrastructure will lead to the single-point failure and denial of service. Second, a high BER in a wireless multihop network and the constant change of network will greatly prolong the service time and reduce the quality of service. Third, the standalone certificate authority will consume a bunch of bandwidth which may lead to congestion in the face of heavy traffic.

Several key management mechanisms have been proposed to meet the requirement of the WMN. They fall into two major categories:

3.1 Distribute Key Management

Lidong Zhou and Zygmunt J Haas proposed a distribution of trust in the key management service by using threshold cryptography [8]. An $(n, t + 1)$ threshold cryptography scheme allows n parties to share the ability to perform a cryptographic operation, so that any $t + 1$ parties can perform this operation jointly, where it is infeasible for at most t parties to do so, even by collusion. The algorithm divides the private key k of the service into n shares, assigning one share to each node. For the service to sign a certificate, each node generates a partial signature for the certificate using its private key share and submits the partial signature to be a combiner.

To prevent mobile adversaries [9] (in which an adversary might be able to compromise all nodes over a long period of time), share refreshing is enabled to compute new shares from old ones in collaboration without disclosing the service private key to any server. After refreshing, the server removes the old shares and uses the new ones to generate partial signatures. Because the new shares are independent of the old ones, the adversary is challenged to compromise the $t + 1$ server.

Seung Yi [10] implemented the above algorithm as MOCA and verified the performance by a network simulator. The advantage of MOCA is that it prevents single-point failure by distributing the single CA service to n nodes. As long as less than k nodes are compromised, the network is intact and robust. Main deficiencies are additional computation of nodes and extra traffic of the network by network-wide CREQ and CREP unicast response.

There is another similar implementation presented by Jiejun Kong [11]. During the system bootstrapping phase, a centralized CA gives k network nodes their valid certificate and secret shares. Then a self-initialization algorithm is practiced to deliver the secret share to the uninitialized entity by a local coalition of K secret share holders. Its implementation improves the algorithm availability in each network locality and is able to fully operate in a large-scale network.

Haiyun Luo [12] fine-tuned the above proposal by enabling the neighbor behavior monitoring in addition to certificate granting service. Once a predefined malpractice is observed, the suspect's certification is revoked or suspended. However, the cost to maintain and manage the private keys grows with the scale of a network.

3.2 Self-Organized Key Management

Jean-Pierre Hubaux first introduced self-organized public key infrastructure [13] and the algorithm was further developed and verified [14]. The algorithm is similar to PGP in the case that public-key certificates are issued by the users; however, it does not rely on certificate directories for the distribution of certificate. Instead, the certificates are stored and distributed by the public of the counterparts, and one tries to find an appropriate certificate chain to the counterpart in the merged repository. Once a positive certificate chain is identified, the authentication is considered successful. Figure 2 shows a certificate graph between users u and v.

This algorithm eliminates the need of a standalone CA to distribute and maintain certificate and prevent the single-point failure. However, this algorithm cannot prevent the participation of impersonated node or nodes with a fabricated certificate. The incomplete certificate information storage does not guarantee full authentication and the successful rate is closely related to the building process of the certificate repository which further leads to the increase in the cost and authentication overhead. Table 1 shows the difference between distribute key management and self-organized key management.

4. Solutions to Security Problems in Routing Protocols

Routing protocol is a vital part of the WMN for it directly determines the implementation of network function and its efficiency. Due to the special characteristics of a WMN, such as mobility of nodes and changeable topology, traditional routing protocols are not suitable for a WMN. In recent years, various WMN routing protocols have emerged, most of them adopting the ideas in MANET routing protocols like DSR [15], AODV [16], and DSDV. However, although these protocols give full consideration on mobility and self-organization characteristics of the WMN, they fail to take security factors in account which results in severe problems in security in the WMN. In this case, many secure routing protocols have come to existence. Some typical ones are introduced below:

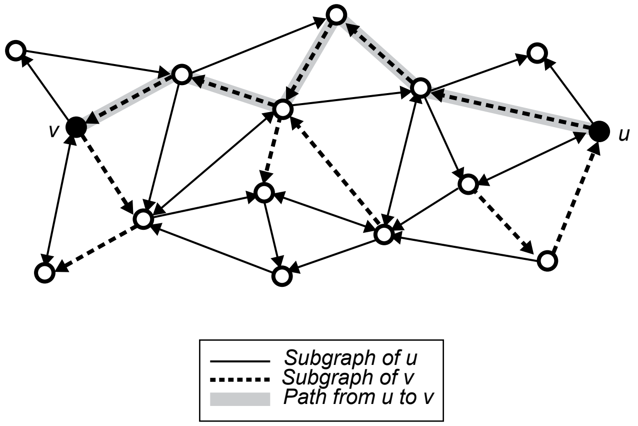

Figure 2: A certificate graph and paths of certificates between users u and v in their merged updated local repositories.

Table 1: Distribute key management compared with self-organized key management

Category	Distribute key management	Self-organized key management
Algorithm foundation	Threshold cryptography	PGP
Preliminary	All nodes in the system know the public key. The algorithm di vides the private key *k* of the service into *n* shares, assigning one share to each node	Each user maintains a local certificate repository that contains a limited number of certificates by certificate exchange
Certificates management	For the service to sign a certificate, each node generates a partial signature for the certificate using its private key share and submits the partial signature to be a combiner	Node produces its certificate
Authentication	Check node certificate through the public key	Their local certificate repository
Advantage	To prevent a single point of failure	To prevent a single point of failure
Disadvantage	Increased computing load and network traffic	An attacker may issue a false certificate

4.1 Secure Routing Protocol

Secure routing protocol (SRP) [17] extends the existing on-demand routing protocols with the ability of identifying and discarding false routing information and hence eliminates attacks of tempering, replaying, and forging routing. SRP ensures acquiring correct topological information. The prerequisite condition of SRP is that the source and the destination nodes have a shared key for verification and communication.

4.2 Ariadne - A Secure On-demand Routing Protocol for Ad Hoc Networks

Ariadne is a SRP [18] using TESLA [19] technology based on DSR. TESLA is a broadcast verification mechanism, which verifies the data packet by messenger authentication code (MAC) and prevents forging MAC by employing time synchronization and delayed key exchanging. The source node establishes the time interval by considering about the latency of whole networks. The source node sends the messenger and MAC. After the time interval, the source node discloses TESLA key for other node to verify. The target node buffers the messenger until source nodes can release the corresponding TESLA keys, and then verifies it by using the key. To ensure the order of MAC and key, time synchronization is needed. The prerequisite conditions of Ariadne are that the source and the destination nodes must have a shared key, every node in the network must possess the initial verification value of other nodes, and their clocks must be approximately synchronized. Figure 3 shows how to process the packet in a route request.

$$\mathrm{S}: h_0 = MAC_{K_{SD}}(REQUEST, S, D, id, ti)$$

$$\mathrm{S\text{-}}\ .\ \text{*}:(REQUST,S,D,id,ti,h_0,(),())$$

$$\mathrm{A}: h_1 = H[A,h_0] \quad M_A = MAC_{K_{A_{ti}}}(REQUEST, S, D, id, ti, h_1, (A), ())$$

$$\mathrm{A}\!-\!> *: (REQUST, S, D, id, ti, \underline{h_1}, (A), (\underline{M_A}))$$

$$\mathrm{B}:\ h_2\ 5\ H[B,h_1]$$

$$M_B = MAC_{K_{B_{ti}}}(REQUEST, S, D, id, ti, h_2, (A,B), (M_A))$$

$$\mathrm{B}\!-\!> *: (REQUST, S, D, id, ti, \underline{h_2}, (A,\underline{B}), (M_A, \underline{M_B}))$$

$$\mathrm{C}:\ h_3\ 5\ H[C,h_2]$$

$$M_C = MAC_{K_{C_{ti}}}(REQUEST, S, D, id, ti, h_3, (A,B,C), (M_A, M_B))$$

$$C\!-\!> *: (REQUST, S, D, id, ti, \underline{h_3}, (A,B,\underline{C}), (M_A, M_B, \underline{M_C}))$$

$$\mathrm{D}: M_D = MAC_{K_{DS}}(REPLY, D, S, ti, (A,B,C), (M_A, M_B, M_C))$$

$$\mathrm{D}\!-\!> C: (REPLY, D, S, ti, (A,B,C), (M_A, M_B, M_C), \underline{M_D}, ())$$

$$\mathrm{C}\!-\!> \mathrm{B}: (REPLY, D, S, ti, (A,B,C), (M_A, M_B, M_C), M_D, (\underline{K_{C_{ti}}}))$$

$$\mathrm{B}\!-\!> \mathrm{A}: (REPLY, D, S, ti, (A,B,C), (M_A, M_B, M_C), M_D, (K_{C_{ti}}, \underline{K_{B_{ti}}}))$$

$$\mathrm{A}\!-\!> \mathrm{S}: (REPLY, D, S, ti, (A,B,C), (M_A, M_B, M_C), M_D, (K_{C_{ti}}, K_{B_{ti}}, \underline{K_{A_{ti}}}))$$

Figure 3: The process for a route request in Ariadne.

4.3 Authenticated Routing for Ad hoc Networks

Authenticated routing for ad hoc networks (ARANs) [20] are suitable for on-demand routing protocols. The ARAN uses a public key certificate and a trusted CA to verify the routing information. The prerequisite conditions of the ARAN are that a trusted certificate server is needed to distribute and manage the certificates and every node should obtain a public key certificate from the server prior to join the network. Figure 4 shows how to process a packet in a route request.

S- . *:[REQUEST, D, CERT$_S$, N, t]K$_s$2

A- . *:[[REQUEST, D, CERT$_S$, N, t]K$_s$2] K$_A$2, CERT$_A$

B- . *:[[REQUEST, D, CERT$_S$, N,t]K$_s$2] K$_B$2, CERT$_B$

Figure 4: The process for a route request in ARAN.

4.4 Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks

SEAD [21] is a secure routing protocol extending from DSDV where the basic idea is to use the elements in a hash chain to verify the sequence number and number of hops in a routing update packet. Because of the one-way characteristic of the hash chain, this could prevent an attacker from forging a sequence number larger than the real one or declaring a smaller number of hops than the real one. When a node receives an update routing packet, it uses its hash value to verify the packet; if the verification is passed, it modifies its route table, else it discards this packet.

The advantage of this method is the adaption of the one-way hash chain to verify the authentication which largely reduces the computational complexity. The disadvantage of this method is that a trusted entity is needed in the network to distribute and maintain the verification element of every node because the verification element of a hash chain is detached by a trusted entity. This is prone to cause single-point failure. If the trusted entity is compromised, the entire network will be broken.

4.5 Secure Ad Hoc On-demand Distance Vector

SAODV [22,23] is a secure routing protocol based on AODV. Its prerequisite condition is to dispatch the public keys of and to all nodes for signature. It employs two mechanisms to ensure the security on AODV. One is the digital signature which ensures the integrity of data in the packet that does not need to be modified while forwarding. The other one is the one-way hash chain to verify changeable part like number of hops in the packet.

Its advantage is using a intermediate node signature mechanism to solve the problem of verification the answers to the routing request of intermediate nodes. The disadvantage is that it uses asymmetric cryptography which consumes a lot of recourses on intermediate nodes.

4.6 Secure Link State Routing for Mobile Ad Hoc Networks

SLSP [24] is a secure protocol based on link states and protects the routing protocol using a link state like ZRP [25]. The prerequisite condition of this protocol is that every node has a pair of public and private key and the public key is dispatched to other nodes.

SLSP has two functions. For one, it could prevent IP address tempering; for two, it could record the packet sending frequency of neighbors and if it is higher than a given value, this neighbor is then classified as an attacker and its packets are no longer processed. This could restrict the DoS attack like flooding in a very small area.

The advantage of this algorithm is that it uses the mechanism of monitoring its neighbors to prevent a DoS attack. The disadvantage is that it uses asymmetric cryptography which consumes vast recourses on intermediate nodes. Table 2 gives a comparison of these secure routing protocols.

5. Intrusion Detection

The academic research and industry practice have proved that there is no absolute secure proposal for a network system especially a mesh network which is highly dynamic and prone to insider attacks. Next handy weapon in our toolkit is intrusion detection.

Table 2: Comparison of secure routing protocols

Protocol name	Suitable for	Prerequisite conditions	Main security tech	Verification part	Advantage	Disadvantage
SRP	DSR	Key shared between the source node and destination node	Messenger authentication code	Source address, destination address, messenger ID	Simple algorithm, wide application situations	Lack of protection for routing maintenance messenger, intermediate nodes cannot reply to the routing request
ARIADNE	DSR	Dispatches the TESLA verification key, key shared between the source node and destination node, public key certificates	One-way hash chain messenger authentication code	Whole packet, routing sequence	Uses symmetric cryptography and TESLA technology, low computational complexity and overhead of management	Needs time synchronization, bandwidth wasted in sending keys, latency in verification
ARAN	AODV DSR	Establishes a certificate server responsible for issuing and maintaining the public key certificate of every node	Digital signature	Whole packet	Ensures authentication, integrity, and nonrepudiation	High computational complexity, CA is needed, intermediate nodes cannot reply to the routing request
SEAD	DSDV	Dispatches the verification initialization value	One-way hash chain	Sequence number, number of hops	Low complexity in computation	A trusted entity is needed to dispatch and maintain the verification elements of all nodes
SAODV	AODV	Dispatches public keys of nodes	Digital signature, one-way hash chain	Whole packet	Intermediate nodes could reply to the routing request	High computational complexity due to the asymmetric cryptograph
SLSP	ZRP	Dispatches public keys of nodes	Digital signature, one-way hash chain	Whole packet	Prevents DoS attacks by monitoring neighbor nodes	High computational complexity due to the asymmetric cryptograph

Since the intrusion includes not only the attacks launched by the outsiders but also the misuse from inside, intrusion detection is more effective and flexible to defend insider attacks. However, a WMN poses new challenges for designing intrusion detection schemes. 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 by multihop 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 a difficult problem.

Youngguang Zhang and Weeke Lee proposed an agent-based distributed and cooperative intrusion detection scheme [26]. The IDS agent can be structured into six pieces including local data collection, local detection engine, cooperative detection engine, local detection engine, local response, global response, and secure communication. Figure 5 shows a conceptual model for an IDS agent. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is desired, the neighboring IDS agent will cooperatively participate in the global intrusion detection action. In the anomaly detection model, a broad data set or/and specific training is needed to realize the detection of instruction in the routing layer. A cross-layer design is desired to improve the rate of intrusion detection. The proposal introduced the distributed and cooperative intrusion detection model which facilitates local detection by the IDS agent resided in the node and further improves the detection rate by discovering intrusion activities in other layers. Main deficiencies of this model lie in the fact that anomaly detection requires thorough and complete data training which is not applicable to mesh networks; moreover, an IDS agent on each node consumes quite a lot memory and computation resources.

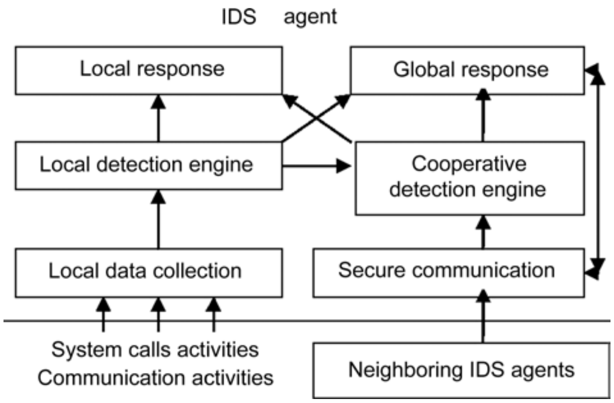

Figure 5: A conceptual model for an IDS agent.

Olge Kachirski and Ratan Guha proposed another scheme which reduces the number of IDS agents by deploying a monitoring agent on specific nodes [27]. Chin-Yang Tseng proposed a specification-based monitoring scheme which employs distributed nodes to monitor the query process in an AODV network [28]. A network monitor employs a finite state machine for detecting incorrect RREQ and RREP messages and take predefine actions if it transits from a normal state to suspicious or alarm states. This scheme is expected to have a higher detection rate and relatively low false alarm.

Ping YI proposed a timed automata-based intrusion detection algorithm which divided the network into independent zone with one randomly selected monitoring node [29]. After manually constructing the timed automata from the routing protocol, the monitoring node is able to collect behavior information from its neighbors and discovers malicious attackers automatically. This intrusion algorithm performs well without initial data training. Table 3 gives a comparison of the above-mentioned intrusion detection schemes.

Other well-known schemes include the Markov Chain-based anomaly detection algorithm proposed by Bo Sun and Udo W Pooch [30], the SNMP MIB-based intrusion detection architecture by P Alerbs [31], Bhargava and Agrawal intrusion and response model [32], AODV sequence forgery detection [33], Subhadrabandhu misuse detection which includes two optimized approximation algorithm [34], and a specification-based intrusion detection model proposed by Chinyang Henry Tseng [35].

Any information collected by distributed nodes is incomplete and only neighbor monitoring and coordinated detection is feasible in this network architecture. Agent-based intrusion detection architecture relies on built-in agents to monitor network traffic, share information, and coordinate the intrusion detection process. This distributed IDS performs well at the cost of bandwidth consumption and exceeded computation overhead which could be greatly eased by dividing the network into independent zones and appointing an dedicated

Table 3: Comparison between two intrusion detection schemes

Category	Agent-based distributed scheme	Specification-based monitoring scheme
Executor	Agents in nodes	All nodes
Detect method	Abnormal detect	Automata-based detect
Advantage	Cooperative intrusion detection and response within all agents	No need for training data
Disadvantage	The need for training data	The need for prior analysis of routing protocols.

agent per zone. Another approach to determine the misbehavior of the network is to deploy movable agents in the network which moved toward places where a suspicious activity is spotted and distinguish network breakdown from intrusion behavior.

6. Conclusion

The unique mesh structure of the WMN requires a dedicated security solution in addition to a traditional security scheme. This article reviews some specific solutions regarding key management, routing security, and intrusion detection and how these proposals can be tailored for a mesh network security solution. The security architecture of the WMN is a growing and promising field of wireless networking. It is desired to invest more efforts in the following fields:

6.1 Defense against DoS Attacks

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.

6.2 Cross-layer Security Architecture

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 some special 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.

6.3 Security Protection for Multicast

Multicast can effectively reduce duplicate data traffic in wireless environment; however, most security schemes only focus on the integrity of the routing message and the authentication of a single node. Special consideration regarding multicast is desired.

6.4 Protection of Traffic Flow and Location for Information Privacy

Given the traffic information collected over a period of time, an attacker is able to identify key infrastructure in the network.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No.60932003), the Natural Science Foundation of Shanghai, China (Grant No. 09ZR1414900), the National High Technology Development 863 Program of China (Grant No.2006AA01Z436, No.2007AA01Z452, No.2009AA01Z118).

References

1. I.F. Akyildiz, X. Wang, and W. Wang. “Wireless mesh networks: a survey”, Comp Net, vol.47, no.4, pp. 445-87, 2005.
2. J. Camp, and E. Knightly. “The IEEE 802.11s extended service set mesh networking standard”, IEEE Communicat Magaz, vol.46, no.8, pp.120-6, 2008.
3. S. Ben, Naouel, and J.P. Hubaux. “Securing wireless mesh networks”, IEEE Wireless Communicat, vol.13, no.2, pp. 50-5, 2006.
4. P. Yi, Y.P. Zhong, S.Y. Zhang, and Z.L. Dai. “Flooding attack and defence in ad hoc networks”, J Syst Engineer Electro, vol. 17, no.2, pp.410-6, 2006.
5. F. Naït-Abdesselam, B. Bensaou, and T. Taleb. “Detecting and avoiding wormhole attacks in wireless ad hoc networks”, IEEE Communicat Magaz, vol.46, no.4, pp.127-33, Apr. 2008.
6. I. Aad, J.P. Hubaux, and E.W. Knightly. “Impact of denial of service attacks on ad hoc networks”, IEEE/ACM Trans Network, vol.16, no.4, pp.791-802, 2008.
7. Y.C. Hu, P. Adrian, and J. David. “Rushing attacks and defense in wireless ad hoc network routing protocols”, In Proceedings of the ACM Workshop on Wireless Security (WiSe 2003), San Diego, California, USA, pp. 30-40, Sep. 19, 2003.
8. L. Zhou, and Z. J. Haas. “Securing ad hoc networks”, IEEE Networks Special Issue on Network Security, vol.13, no.6, pp.24-30, Nov/ Dec. 1999.
9. R. Ostrovsky, and M. Yung. “How to withstand mobile virus attacks”, Proc of the 10th ACM Symposium on Principles of Distributed Computing, pp. 51-9,1991.
10. S. Yi, and K. Robin. “MOCA: Mobile certificate authority for wireless ad hoc networks”, Proc of 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland, pp. 52-64, Apr. 2003.
11. J. Kong, Z. Petros, H. Luo, S. Lu, and L. Zhang. “Providing robust and ubiquitous security support for mobile ad-hoc networks”, IEEE 9th International Conference on Network Protocols (ICNP’01), Riverside, California, pp. 251-60, 2001.
12. H. Luo, J. Kong, Z. Petros, S. Lu, and L. Zhang. “Self-securing ad hoc wireless networks”, Proc of the Seventh IEEE Symposium on Computers and Communications (ISCC’02), Italy, pp. 567-74, 2002.
13. J.P. Hubaux, B. Levente, and C. Srdjan. “The quest for security in mobile ad hoc networks”, Proc of the 2001 ACM International Symposium on Mobile ad hoc networking and computing 2001, Long Beach, CA, USA, pp.146-55, 2001.
14. C. Srdjan, N. Levente, and J.P. Hubaux. “Self-organized public-key Management for mobile ad hoc networks”, IEEE Transactions on mobile computing, vol.2, no.1, pp. 52-64, Jan-Mar. 2003.
15. DB. Johnson, DA. Maltz, and YC. Hu. “The Dynamic Source Routing Protocol (DSR) for mobile ad hoc networks for IPv4”, RFC4728, Available from: http://www.ietf.org/rfc/rfc4728.txt [cited in 2007 Feb].
16. E. Charles, M. Elizabeth, and R. Samir. “Ad hoc On-Demand Distance Vector (AODV) routing”, RFC 3561, Available from: http://www.ietf.org/rfc/rfc3561.txt [cited in 2003 Jul].
17. P. Papadimitratos, and Z. Haas. “Secure routing for mobile ad hoc networks”, in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, Jan. 27-31,2002.
18. Y.C. Hu, P. Adrian, and B. David. “Ariadne: A secure on-demand routing protocol for ad hoc networks”, in Proceedings of the MobiCom 2002, Atlanta, Georgia, USA, Sep. 23-8,2002.
19. A. Perrig, R. Canetti, D. Song, and J.D. Tygar. “Efficient and secure source authentication for multicast”, in Proceedings of Network and Distributed System Security symposium, pp. 35-46, Feb. 2001.
20. S. Kimaya, D. Bridget, NL. Brian, S. Clay, and M. Elizabeth. “A secure routing protocol for ad hoc networks”, In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Nov. 2002.

21. YH. Hu, B. David, and P. Adrian. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), IEEE, Calicoon, NY, pp. 3-13, Jun. 2002.

22. GZ. Manel. "Secure ad hoc on-demand distance vector routing", ACM Mobile Computing and Communications Review (MC2R), vol. 6. no. 3, pp. 106-7, Jul. 2002.

23. GZ. Manel and N. Asokan. "Securing ad-hoc routing protocols", In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pp. 1-10. Sep. 2002.

24. P. Papadimitratos, and ZJ. Haas. "Secure link state routing for mobile ad hoc networks", IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, Jan. 28,2003.

25. ZJ. Haas,and MR. Pearlman. "The performance of query control schemes for the zone rounting protocol", ACM/IEEE Trans.net, vol.9, no.4, pp. 407-38, Aug. 2001.

26. Y. Zhang, and W. Lee. "Intrusion detection techniques for mobile wireless networks", Mobile Networks and Applications, vol.9, no.5, pp. 545-56,2003.

27. K. Oleg, and G. Ratan. "Intrusion detection using mobile agents in wireless ad hoc networks", IEEE Workshop on Knowledge Media Networking (KMN'02), Kyoto, Japan, pp. 153-8,2002.

28. CY. Tseng, B. Poornima, K. Calvin, L. Rattapon, R. Jeff, and L. Karl. "A specification-based intrusion detection system for AODV", 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), Fairfax, VA, USA, Oct. 31,2003.

29. P. Yi, X. Jiang, and Y. Wu. "Distributed intrusion detection for mobile ad hoc networks", J System Engineer Electron, vol. 19, no. 3, pp. 851-9,2008.

30. B. Sun, K. Wu, and UW. Pooch. "Routing anomaly detection in mobile ad hoc networks", Proceedings of 12th International Conference on Computer Communications and Networks (ICCCN 03), Dallas, Texas, Oct. 2003, pp. 25-31.

31. P. Albers, O. Camp, J.M. Percher, B. Jouga, L. Mé, and R. Puttini. "Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches", In Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002), Apr. 2002.

32. S. Bhargava, and DP. Agrawal. "Security enhancements in AODV protocol for wireless ad hoc networks", Vehicular Technology Conference, 2001, vol. 4, pp. 2143-7.

33. W.Wang, L. Yi, K. Bhargava. "On vulnerability and protection of ad hoc on-demand distance vector protocol", in Proceedings of 10th IEEE International Conference on Telecommunication (ICT), 2003.

34. D. Subhadrabandhu, S. Sarkar, and F. Anjum. "A framework for misuse detection in ad hoc networks—Part I", IEEE Journal on Selected Areas in Communications, vol.24, no. 2, pp. 274-89, Feb. 2006.

35. C.H. Tseng, S. Tao, B. Poornima, K. Calvin, and L. Karl. "A Specification-based intrusion detection model for OLSR", RAID 2005, LNCS 3858, pp. 330-50,2006.

AUTHORS

Ping Yi was born in 1969. Currently, he is an Associate Professor at School of Information Security Engineering, Shanghai Jiao Tong University in China. He received the B.Sc. degree at the Department of Computer Science and Engineering from the PLA University of Science and Technology, Nanjing, in 1991. He received the M.Sc. degree in computer science from the Tongji University, Shanghai, in 2003. He received the Ph.D. degree at the Department of Computing and Information Technology, Fudan University, China. His research interests include mobile computing and ad hoc networks security. He is a member of IEEE Communications and Information Security Technical Committee, is the Associate Editor for Wiley's *Security and Communication Networks* (SCN) journal, and editor for *Journal of Security and Telecommunications*, and a member of the Technical Program Committee (TPC) for the ICC'09 CISS (ICC 2009 Communication and Information Systems Security Symposium) and the GC'08 CCNS (IEEE Globecom 2008 Computer and Communications Network Security Symposium).

E-mail: pyi_edu@yahoo.com.cn

Yue Wu is an Associate Professor and Director of Wireless Network Security Laboratory in the School of Information Security Engineering at Shanghai Jiaotong University, He got his Ph. D degree from Dept. of Radio Engineering, Southeast University, Nanjing, P. R. of China in 2004, his current interests include wireless networks QoS and security. He is a member of IEEE, member of IEEE Communications and Information Security Technical Committee and member of International Conference on Computer Sciences and Convergence Information Technology.

E-mail: wuyue@sjtu.edu.cn

Futai Zou was born in 1973. Currently he is working as Lecture at School of Information Security Engineering, Shanghai Jiao Tong University in China. He received his Ph.D degree in Computer Science from the department of Computer Science &Engineering, Shanghai Jiaotong University in 2005. His research interests include P2P computing and mobile computing security.). He has published about 20+ research papers in refereed journals and conferences.

E-mail: zoufutai@sjtu.edu.cn

Ning Liu was born in Jinan, China, 1979. He received the B. S. degree in communication engineering and M. S. degree in communication and information system from Informational Engineering University, Zhengzhou, China, in 2002, and 2005, respectively. He is currently a Ph. D. candidate in communication and information system at the School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, China. His research interests include wireless communication, wireless mesh network and information security.

E-mail: ningliu@sjtu.edu.cn.

DOI: 10.4103/0256-4602.58969; Paper No TR_118_09; Copyright © 2009 by the IETE