Security Issues in Wireless Mesh Networks

Muhammad Shoaib Siddiqui, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University,
Sochen-ri, Giheung-eup, Yongin-si, Gyeonggi-do, 449-701, South Korea.
shoaib@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract

Wireless Mesh Network (WMN) is a new wireless networking paradigm. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Wireless internet service providers are choosing WMNs to offer Internet connectivity, as it allows a fast, easy and inexpensive network deployment. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we investigate the principal security issues for WMNs. We study the threats a WMN faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore approaches to secure its communication. [1]

1 Introduction

Wireless Mesh Networks (WMNs) represent a good solution to providing wireless Internet connectivity in a sizable geographic area; this new and promising paradigm allows network deployment at a much lower cost than with classic wireless networks. In WMNs, it is possible to cover the same area, as compared to WiFi, with less wireless routers, which makes the use of WMNs a compelling economical case; WMNs are thus suitable for areas that do not have existing data cabling or for the deployment of a temporary wireless network.

WMN has been a field of active research in recent years. However, most of the research has been focused around various protocols for multi hop routing leaving the area of security mostly unexplored [3]. At the same time, new applications of WMNs introduce a need for strong privacy protection and security mechanisms.

In this paper, first, we look at the characteristics of WMNs and the challenges these characteristics impose in section 2. In section 3, we analyze the basic high level security issues that every network has; such as availability, authenticity, integrity and confidentiality. We then look into the Secure Routing, Key management, Trust Management and Intrusion Detection Issues in WMNs, in section 4.

[1] This paper was supported by MIC and ITRC Project.

2 Characteristics of WMNs

WMN is a wireless co-operative communication infrastructure between a massive amount of individual wireless transceivers (i.e. a wireless mesh). This type of infrastructure is decentralized, relatively inexpensive, and very reliable and resilient, as each node need only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances, especially over rough or difficult terrain.

WMNs are extremely reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors simply find another route. Extra capacity can be installed by simply adding more nodes. Mesh networks may involve either fixed or mobile devices as shown in Figure 1. The principle is simple: data will hop from one device to another until it reaches a given destination. One advantage is that, like a natural load balancing system, the more devices the more bandwidth becomes available. Since this wireless infrastructure has the potential to be much cheaper than the traditional networks, many wireless community network groups are already creating wireless mesh networks.

2.1 Constraints

There are four main constraints in wireless mesh network or in any system which has mobile clients such as PDAs, cell-phones etc.

1. **CPU:** large computations on the end nodes are slow, as computing power of the processor is small.
2. **Battery:** total energy resource is very limited and it is not desirable to use the device for large computations and transmissions.

2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07)
0-7695-2777-9/07 $20.00 © 2007 IEEE

3. **Mobility:** nodes can be mobile, which can produce latency in the convergence of the network.
4. **Bandwidth:** bandwidth in amongst the mobile nodes is also limited.

2.2 Challenges

These constraints of WMNs pose challenges in achieving security goals. First of all, wireless links in WMN make it prone to active attacks, passive attacks and message distortion [1, 5]. In WMNs, passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation [5].

Secondly, we have the probability of node being compromised due to the lack of physical protection. Hence, the system becomes unprotected to malicious attack from outside of the network as well as attacks launched from within the network.

Thirdly, a WMN may be dynamic because of frequent changes in both its topology and its membership. This ad hoc nature can cause the trust relationship among nodes to change also.

Finally, as WMN has memory and computational constraints, the traditional schemes for achieving security are not applicable. Study of WMN's specifics [13] led to the following critical security challenges:

2.2.1. Detecting the Corrupted Nodes. For a WMN it is critical to identify the compromised nodes within it. First of all, the physical protection of the node is crucial. Then there is a possible attack by the removal or replacement of a node. This can be detected by the neighboring nodes when an unusual topology change is observed in the network. The second would be a passive attack on a node, which is very much difficult to identify. In the third case, the attacker might change the internal state of the node for attacking the routing algorithm etc. Finally, the fourth case can be cloning the captured device and installing replicas at some strategically chosen locations in the mesh network, which allows the adversary to inject false data or to disconnect parts of the WMN. This attack can seriously disrupt the routing mechanism.

2.2.2. Multi-Hop Routing. The routing mechanism in WMN needs to be secured. The attacker can affect the routing mechanism and the functionality of the WMN by inserting false routing messages. To alter the routing mechanism, the attacker may temper with the routing messages, modify the state of one of the nodes, use replicated nodes and/or perform DoS attacks [1].

2.2.3. Fairness. In WMNs, most of the nodes are working as message repeaters or forwarders (as previously discusses), therefore throughput obtained by a node can very significantly depend upon the topology of the network and nodes surrounding that node. The fairness issue in WMNs [15] is closely related to the number of hops between the nodes; this means that if the adversary manages to increase the number of hops between a given sender and receiver nodes, it can decrease the bandwidth share. A possible solution against this attack can be a periodic reconfiguration of the WMN; given that some nodes with higher computation power are static, the operator can define, based on the traffic in the WMN, the optimal configuration of the WMN and force the routes at the those nodes to the optimal routes. Once the network has an optimal configuration, it is possible to use the some sort of scheduling to ensure per-client fairness and to optimize the bandwidth utilization in the WMN.

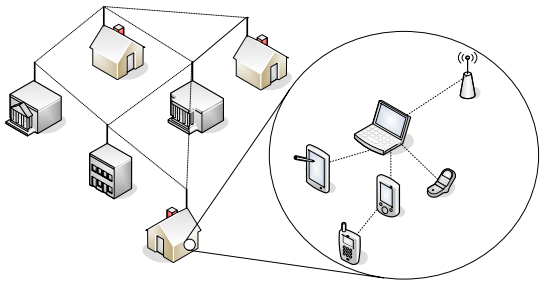

Figure 1. An example of Wireless Mesh Network

3 Security Issues

High level security issues for WMNs are basically identical to security requirements for any other communication system, and include following attributes:

3.1 Availability

Availability ensures the survivability of network services despite attacks. Availability does not come to mind as a security concern as quickly as do confidentiality and integrity. But the assurance of availability is very much a security issue. Long-term Denial of Service (DoS) attacks can severely hinder a network's ability to continue. In fact, DoS is often a successful tactic of network services warfare. Moreover, the processes required to prevent or mitigate the effects of loss of availability are very much within the realm of security methodology, because the basic concept of availability assures that authorized persons have uninterrupted access to the information in the system at hand. The availability in a WMN can be compromised by following ways.

3.1.1. Signal Jamming. On the physical and media access control layers, an attacker can attack on availability of the network by employing jamming to interface with communication on physical channel [2]. Orthodox defense mechanism includes spread spectrum and frequency hopping, which makes the attacker to widen the jamming range. One can also

complain the authorities for jamming and get the invader arrested.

3.1.2. Denial of Service (DoS). A DoS attack can be launched at any layer of wireless mesh network [2]. There are many ways of instigating a DoS. A common technique is to flood the target system with requests. The target system becomes so overwhelmed by the request that it could not process normal traffic. Firewall rules could be adjusted to stop request from a certain addresses or network. But modern attacks use 'zombies' systems all over the world. This attack is called distributed DoS [1] and it is nearly impossible to counter. Intrusion Detection and Prevention system are deployed to monitor (D)DoS attacks [7].

In a mesh network, DoS attack can be launched either externally or by a compromised node. Due to limited computation and battery life, IDS/IPS is difficult to deploy in WMNs.

3.1.3. Battery Exhaustion. Battery life is the most critical parameter for many nodes in a wireless mesh network. Battery exhaustion attack also known as 'sleep deprivation attack' is a real threat and is more hazardous than simple denial of service attacks. Attack on CPU computation may deny the availability of the service while battery exhaustion can disable the victim.

There are some battery management and monitoring system with the help of which one can estimate/ predict the amount of usable energy remaining provided that such process does not consume too much of the battery life itself.

3.2 Authenticity

Authenticity enables a node to ensure the identity of the peer node it is communicating with. Without authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes.

With the implementation of the concepts such as ubiquitous system, the abundance of networking nodes is reasonable. All these nodes should have an authentic communication within the network. The usual authentication mechanisms involve a centralized system which administers restriction on the basis of access list or capability certificates. In a mesh network, the presence of such a server is sometimes not possible. But there are some ways as mentioned below;

3.2.1. Secure Transient Association. The concept of secure transient association [4] is effective and simple. If a house has a device such as universal controller, then the user needs to be assured that it controls all and only her devices. That is, we need to have an association between the controller and devices. Now this association needs to be secure; that is, there is no such other controller in the hand of some other user by which he can control her devices. Then this association required being transient, also. After a device is no longer owned by her, then that device should not obey her controller.

This approach can be implemented in a WMN, to ensure authenticity. A person's device would only entertain its owner's devices. Hence, within a certain part of a network, some authentication can be achieved. For the communication with the outer part of the network, we can implement authentication mechanism on the basis of public key cryptography, using a node which has better computational power. The main controller of the user can provide authenticity on the behalf of the node and within the local network authenticity is ensured by secure transient association.

3.2.2. Imprinting. The mechanism by which devices acquire the self-signed mediator's certificate is called imprinting. A network node will recognize as its owner the first entity that sends it a secret key. As the new node receives this key, the device will always stay faithful to its owner. If the new node is surrounded by more than one node then the first one which sends the key would become the owner. Same as to the chick hatched from the egg considers the first thing it sees as its mother.

But like a chick, death is inevitable for a network node. Either there is a timeout for obtaining a new secret key, or it is a fault in the network or in the device itself. The third cause may be that the owner node asks the child node to become dead and reborn.

The timeout death helps in the defense of an attacker that is, even if a secret key is revealed, it would be replaced after a while. If a node is compromised and the owner node comes to know about it then it can make the child node die. Whenever, a node dies and comes back to life, it always looks for its owner the same way, as it did the first time.

In a mesh network, the child nodes can be the mobile clients, PDAs, appliances etc and the owner nodes can be the main access point or the home PC. A hierarchical approach for imprinting would be better with static nodes in upper layers and mobile nodes in the lower layers of the tree.

3.3 Integrity

The concept of integrity ensures that the contents of data or correspondences are preserved intact through the transfer from sender to receiver. Integrity embodies the guarantee that a message sent is the message received, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways: by the intentional alteration of the data for vandalism or revenge or by the unintentional alteration of the data caused by operator input, computer system, or faulty application errors.

The usual mechanism, to ensure integrity of data, is using hash functions and message digestion [5]. Encryption is another method. Sometimes, message digestion along with encryption is used to implement data integrity and confidentiality at the same time.

3.3.1. Cryptography & Digital Signatures. If the nodes can produce digital signatures and check them; then the solution is straight forward. While one node can verify the other nodes signature using public key cryptography, both nodes will establish a common secret key, using imprinting techniques, and will be able to accept messages protected by secret key. But many of the nodes in a WMN have computation and battery constraints (as discussed in section 2) due to which the verification process, which includes public key cryptography, may not be implemental. However, Elliptic Curve Cryptography (ECC) [17] provides some energy and computation efficient techniques in implementing cryptographic algorithm, which can be suitable for mobile clients.

3.3.2. Pair-Wise Key Sharing. In WMNs, symmetric cryptography is possible as it requires less computation than asymmetric cryptographic techniques. Or a better solution would be using the Diffie-Hellman (D-H) key exchange [5]. Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish shared keys over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

3.4 Confidentiality

The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. Whether the data contains trade secrets for commercial business, secret classified government information, or private medical or financial records, confidentiality implies that data is protected from breaches from unauthorized persons and the damage that would be done to the organization, person, and governmental body by such breaches.

Though breaches to confidentiality are not as well-publicized as denial-of-service (DoS) attacks (which are primarily aimed at compromising availability), they can have serious implications to a network service's competitiveness, a mission's success, and/or personal privacy and safety.

For confidentiality, authenticity needs to be implemented first. It is pointless to attempt to protect the secrecy of a communication without first ensuring that one is talking to the right principal. Once, authenticity is achieved, confidentiality is simply a matter of encrypting the session using mechanism discussed above [5].

4 Security Goals

WMNs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To secure a WMN, we consider the following attributes:

4.1 Secure Routing

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Several routing protocols for WMNs have been proposed [13]. A majority of these protocols assume a trustworthy collaboration among participating devices that are expected to abide by a "code-of-conduct". But there lie several security threats [18], some arising from shortcomings in the protocols, and others from the lack of conventional identification and authentication mechanisms. Some attacks on routing mechanism (discussed in [6]) are highlighted in table 1.

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing.

The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult as merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys.

To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, (see section 3). However, this defense is ineffective against attacks from compromised servers. Detection of compromised nodes through routing information is also difficult in a WMN because of its dynamic topology changes.

On the other hand, we can exploit certain properties of WMNs to achieve secure routing. Note that routing protocols for WMNs must handle outdated routing information to accommodate the dynamically changing topology. False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies in WMNs. If routing protocols can discover multiple routes (e.g., protocols in ZRP, DSR, TORA, and AODV [13] all can achieve this), nodes can switch to

an alternative route when the primary route appears to have failed.

Multipath routing [16] takes advantage of multiple routes in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. For example, if there are 'n' disjoint routes between two nodes, then we can use 'n−r' channels to transmit data and use the other 'r' channels to transmit redundant information. Even if certain routes are compromised, the receiver may still be able to validate messages.

To address the security attacks on Routing mechanism, several secure routing protocols have been proposed: such as SAODV, Ariadne, SEAD, CSER, SRP, SAAR, BSAR, and SBRP [6].

Table 1. Attacks on Routing

Routing Phase	Security Attack
Routing Discovery Phase	Routing table overflow attack, Routing cache positioning attack
Route Maintenance Phase	False Route Control Message
Data forwarding phase	Route Data Dropping
Advanced / sophisticated attacks	Wormhole attack, Blackhole/sinkhole attack, Byzantine attack, Rushing attack, Resource Consumption attack, Location disclosure attack

4.2. Intrusion Detection Systems

Because WMN has features such as an open medium, dynamic changing topology, and the lack of a centralized monitoring and management point, many of the intrusion detection techniques developed for a fixed wired network are not applicable in WMNs. Zhang [7] gives a specific design of intrusion detection and response mechanisms. Marti [8] proposes two mechanisms: watchdog and pathrater, which improve throughput in the presence of nodes that agree to forward packets but fail to do so. In WMNs, cooperation is very important to support the basic functions of the network so the token-based mechanism, the credit-based mechanism, and the reputation-based mechanism can be used to enforce cooperation.

IDS collects activity information from all the nodes and then analyzes it to determine whether there are any activities that violate the security rules. Once the IDS determine that an unusual activity or an activity that is known to be an attack occurs, an alarm is generated to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.

The optimal IDS architecture for a WMN may depend on the network infrastructure itself [9]. On the basis of architectures IDS can be classified as:

1. **Stand-alone Intrusion Detection Systems:** IDS run on each node independently to determine intrusions.
2. **Distributed and Cooperative Intrusion Detection Systems:** (Proposed by Zhang et all [7]) Every node participates in intrusion detection and response by having an IDS agent running on them. An IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.
3. **Hierarchical Intrusion Detection Systems:** Clusterheads act as control points to provide the functionality for its child nodes.

To have separate IDS on each mobile client is not feasible that is why, Distributed IDS and Hierarchical IDS are suitable for WMNs.

4.3. Trust Management

Trust and Security are two mutually dependant concepts, which cannot be segregated. For example trust cannot be assured without the scrutiny of secure communication, similarly security attributes such as cryptography requires trusted key exchange to work. WMNs are based on naive "trust-your neighbor" relationships. As the overall environment is cooperative, these trust relationships are extremely susceptible to attacks. Also, the absence of fixed trust infrastructure, limited resources, ephemeral connectivity and availability, shared wireless medium and physical vulnerability, make trust establishment virtually impossible. Therefore, the unique properties of trust management in WMN, as opposed to traditional centralized approaches, are: uncertainty and incompleteness of trust evidence, locality in trust information exchange; distributed computation, trust evaluation is employed individually.

To overcome these problems, trust has been established in WMNs using a number of assumptions including pre-configuration of nodes with secret keys, or presence of a central trust authority. Direct trust can be established between two parties using the authentication techniques described in section 3.2. Third party trust is implemented using certificate authority, which is computationally expensive and hard to implement due to the ad hoc nature of WMNs.

There have been several works on trust computation based on interactions with one-hop physical neighbors, such as [11] and [10]. Some modals are also proposed that use distributed trust environment [12]. Here, trust computation is distributed and restricted to only local interactions. Each node, as an autonomous agent, makes the decision on trust evaluation individually. The decision is based on information it has obtained by itself or from its neighbors. Although no single node is trustworthy in a WMN because of low physical security and availability, we distribute trust to an aggregation of nodes. Assuming that any n + 1 nodes

will unlikely to be all compromised, consensus of at least n + 1 nodes is trustworthy.

4.4. Key Management

All key-based cryptographic schemes demand a key management service, which is responsible for keeping track of bindings between keys and nodes and for assisting the establishment of mutual trust and secure communication between nodes.

Key distribution and key agreement over an insecure channel are at high risk and suffer from potential attacks. In the traditional digital envelop approach, a session key is generated at one side and is encrypted by the public-key algorithm. Then it is delivered and recovered at the other end. In the Diffie-Hellman (DH) [5] scheme, the communication parties at both sides exchange some public information and generate a session key on both ends. Several enhanced DH schemes have been invented to counter man-in-the-middle attacks [1]. In the symmetric approach, the sequence number or a nonce could be included to prevent the replay attack on setting up a session key. In addition, a multi-way challenge response protocol, such as Needham-Schroeder [14], can also be used.

There are three types of key management that can be applied on WMNs [14]: the first one is virtual CA approach, the second one is certificate chaining, and the third one is composite key management, which combines the first two.

5. Conclusion

In this paper, we analyze the security concern of Wireless Mesh Network and their possible solutions in the light of the applied characteristics and constraints commenced by WMN. Due to the ad hoc nature of WMNs and power and computational constraints, it is hard to implement the security attributes. But an optimal solution may be implemented with a tradeoff between security and resource consumption.

References

[1] S. Hansman and R. Hunt, “A Taxonomy of Network and Computer Attacks Computers and Security”, Elsevier, Vol 24, No 1, 2005, pp. 31-43.

[2] X. Gu and R. Hunt, “Wireless LAN Attacks and Vulnerabilities”, in the proceeding of IASTED Networks and Communication Systems, 18-20 April, 2005, Thailand.

[3] N. B. Salem and J-P Hubaux, “Securing Wireless Mesh Networks”, in IEEE Wireless Communication, Volume 13, Issue 2, April 2006 pp. 50 - 55.

[4] F. Stajano and R. Anderson, “Resurrecting Duckling: Security Issues for Ubiquitous Computing” in Computer, Volume 35, Issue 4, April 2002, pp. 22 - 26.

[5] William Stallings, “Network Security Essentials”, Third Edition, Prentice Hall, July 2006;

[6] W. Zhang, R. Rao, G. Cao and G. Kesidis, "Secure Routing in Ad Hoc Networks and a Related Intrusion Detection Problem", in the proceedings of IEEE Military Communications Conference, Oct. 2003, Volume: 2, pp. 735- 740

[7] Y. Zhang, W. Lee, and Y. Huang, “Intrusion Detection Techniques for Mobile Wireless Networks" in ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[8] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, in proceeding of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 2000 pp 255-265.

[9] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches" in the proceedings of 1st Int. Workshop on Wireless Information Systems (WIS-2002), April 2002, pp. 1-12.

[10] T. Jiang and J. S. Baras, “Autonomous Trust Establishment” in the proceedings of 2nd Int. Network Optimization Conference, March 2005, Portugal.

[11] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The Eigen Trust Algorithm for Reputation Management in p2p Networks”, in proceedings of the 12th Int. World Wide Web Conference, Hungary, 2003, pages 640–651.

[12] C. Tchepnda and M. Riguidel, "Distributed Trust Infrastructure and Trust-Security Articulation: Application to Heterogeneous Networks", in proceeding of 20th Int. Conference on Advanced Information Networking and Applications, (AINA), April 2006, Volume: 2, pp. 33- 38.

[13] I. F. Akyildiz, X. Wang and W. Wang, "Wireless Mesh Network: A Survey", in Computer Networks and ISDN Systems, Volume 47, Issue 4, March 2005.

[14] B. Wu, J. Chen, J. Wu, and M. Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks” in “Wireless Network Security”, Y. Xiao, X. Shen, and D. -Z. Du , Springer, Network Theory and Applications, Vol. 17, 2006, ISBN: 0-387-28040-5.

[15] N. B. Salem and J.-P. Hubaux. “A Fair Scheduling for Wireless Mesh Networks”, in proceedings of WiMesh, 2005, September 2005, Santa Clara, CA.

[16] J. J. Garcia-Luna-Aceves and M. Mosko, “Multipath Routing in Wireless Mesh Networks”, in first IEEE Workshop on Wireless Mesh Networks (WiMesh 2005); September 2005, Santa Clara, CA.

[17] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, "Low-cost Elliptic Curve Cryptography for Wireless Sensor Networks" in 3rd European Workshop on Security and Privacy in Ad hoc and Sensor Networks, 2006, pp. 6-17.

[18] S. Murphy, “Routing Protocol Threat Analysis”, Internet Draft, draft-murphy-threat-00.txt, February 2002.