ISSN:0975-9646

Minimizing Malicious Eavesdropping Ability in Wireless Mesh Networks using SKeMS

Haarika Kandavalli, M.V.S.S NagendraNath
Sasi Institute of Technology and Engineering, Tadepalligudem, AndraPradesh, India.

Abstract: Wireless mesh networks (WMNs) capability for self-organization reduces the complexity of network deployment and maintenance, and thus, offers inexpensive wireless coverage over large areas via use of wireless multi-hopping to wire line gateway nodes. Securing WMNs is a great challenge of because they are subject to various kinds of attacks due to their dynamic wireless and distributed nature. Various security mechanisms based on cryptographic keys involving a high degree key management were used in WMNs. One such secure scheme SKeMS that implements an encryption key assignment and is very effective in reducing eavesdropping attacks, usual threat in WMNs. Compared with previous schemes, SKeMS assigns the available encryption keys among all the nodes in the network. We propose to use SkeMS in combination with an intrusion detection system to enhance overall security measures in WMNs. An implementation of the proposed scheme shows that it is resilient against malicious eavesdropping attack.

I.INTRODUCTION

Wireless Mesh Network (WMN) is an emerging new technology which is being adopted as the wireless internetworking solution for the near future. WMN has characteristics such as rapid deployment and self configuration. Unlike traditional wireless networks, WMNs do not rely on any fixed nfrastructure. Typical wireless mesh networks (WMNs) consist of mesh routers and mesh clients. Mesh routers, which are static and power-enabled, forms a wireless backbone of the WMNs and interwork with the wired networks to provide multi-hop wireless Internet connectivity to the mesh clients. Mesh clients access the network through mesh routers.

WMN is characterized by dynamic self-organization, selfconfiguration and self-healing to enable flexible integration, quick deployment, easy maintenance, low costs, high scalability, and reliable services. The development of this technology has to deal with the challenging security, architecture and protocol design issues. In WMNs, security is one of the crucial components that needs due attention. The emergence of new applications of WMNs necessitates the need for strong privacy protection and security mechanisms of WMNs.

In existing system, various security mechanism based on cryptographic keys are implemented in WMNS. However, their weakness such as high computational overhead, storage overhead and vulnerability to some kinds of attacks are undeniable.

Our proposed scheme differ from existing scheme where the network topology is known in advance, and we assign *K* keys among the nodes, in a way to provide a secured pre-established topology. Our scheme effectively reduce various other forms of network threats that ultimately lead to eavesdropping and DDoS attacks.

II RELATED WORK

A.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 due to which the verification process, which includes public key cryptography, may not be implemented. However, Elliptic Curve Cryptography (ECC) provides some energy and computation efficient techniques in implementing cryptographic algorithm, which can be suitable for mobile clients.

B. 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. 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.

C. Secure Routing: To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. There are two sources of threats to routing protocols. The first comes from external attackers. The second and also the more severe kind of threats come from compromise nodes, which might advertise incorrect routing information to other nodes. To protect from such attacks we can exploit certain properties of WMNs to achieve secure routing. Like, Multipath routing 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. Even if certain routes are compromised, the receiver may still be able to validate messages.

III SECURITY REQUIREMENTS

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

• Confidentiality - It means that certain information is only accessible to those who are authorized to access it.

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

Malicious altering – A message could be removed, replayed or revised by an adversary by a malicious attacker.

Accidental altering - Such as a transmission error, goals on the network which is regarded as malicious altering.

• Availability - Availability ensures the survivability of network services despite of denial of service (DoS) attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable.

• Authenticity - Authenticity is essentially, assurance that participants in communication are genuine and not impersonators

• Non-repudiation - Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. It is useful for detection and isolation of a node with some abnormal behavior.

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

• Anonymity -Anonymity means that all the information that can be used to identify the owner or the current user, should be kept private and not distributed to other communicating parties.

IV CHALLENGES AND THREATS

There are various challenges that we face in achieving security goals in WMN. First of all, wireless links in WMN makes it prone to active attacks, passive attacks and message distortion. In WMNs, passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation. 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.

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

Routing Protocol Threats: Wireless mesh networks may be susceptible to routing protocol threats and route disruption attacks. Many of these threats require packet injection with a specialized knowledge of the routing protocol. In a mesh network, the exploitability of these threats may vary greatly – a network based on a known protocol such as AODV is more susceptible than a proprietary routing protocol. Similarly, a mesh network that uses message integrity checking for routing messages and device authentication will substantially decrease the threat risk. These attacks have the potential to cause service degradation far beyond the reach of a single malicious transceiver.

Spoofing Of Wireless Infrastructure: Attacker used an “evil twin” or “man-in-the-middle” attack to execute an information disclosure threat.

- Denial-of-service attack. A DoS attack could be launched at any layer of the network. For instance, on the physical and media access control layers, an adversary could employ jamming signal to interfere with communication on physical channels.
- Something-of-Death Attack: While protocols serve a specific purpose, there is always the danger that bad implementations open yet another door for DoS attacks where a malicious attacker sends forged and mal-formed frames with the intention of crashing the AP under attack.
-

V A SECURE KEY MANAGEMENT SCHEME

In order to have a secure WMN that is resistant to malicious eavesdropping attacks, a secure key management scheme (SKeMS) is implemented that seeks to minimize the malicious eavesdropping ability (*MEA*) in the network.

Given a network N and a set of encryption keys *K*, first, we initialize *keys* in each node in N to the empty set. For all nodes in N, find node, say X, that has the highest number of neighbors that do not have common keys with *x*. After choosing the node with the highest *NBR* we start assigning the keys between that node and all its neighbors. *The idea in this key assignment design is that we try to assign the keys among the nodes to be as different as possible, while keeping the network connected.* After choosing the node to start with, say node X, we start taking node X and one of its neighbors, say Y, as a pair of nodes and assign

a key on both nodes to be used as a shared key for secure communication.

If the chosen pair of nodes X and *Y* has not been assigned any key yet, we will choose the least used key from the set of available keys *K* and assign it on both nodes, so as to be used as an encryption key for their communications. If node X has previously been assigned some keys, in this case we will choose the least used key from *K* not been used on any neighboring nodes of node *X* or node Y, so as to make the assignment as diffrent as possible.

If node X has already assigned some keys, but it is not sharing any of them with node Y. In this case we will choose the least used key from the available keys not in Z, where node Z is a neighbor of node X, which already share a key with node X. Then we will add the key to both X and Y nodes. If both chosen nodes have been assigned some keys but there is no shared key between them, in this case we will choose the least used key from *K* not been used on either X *or Y*'s neighbors, if applicable, else we will choose the least used key from *K*.

Intrusion detection mechanism is combined with secure key management scheme, can be used to detect and respond to most of the network layer threats particularly for WMN environment. DoS in any form against any network, is regarded as a severe attack. The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack. If launched against a single node either to exhaust its battery or to isolate it from the network operations. Selfish mesh router attack in WMN and rogue BS attack is used to make services unavailable for a target area in wireless broadband networks. To counter dos attacks, intrusion detection scheme is implemented.

VI PERFORMANCE ISSUE

To measure the performance of our scheme, a static WMN is considered. First metric used for performance evaluation is *malicious eavesdropping ability ratio*, which is calculated as the neighbor compromise ability (*NCA*) divided by the total number of neighboring nodes that are vulnerable to eavesdropping attack. *Having smaller MEA ratio indicates that the network is more secured and more resistant against malicious eavesdropping attacks*. The second performance metric is the *running time*, which is defined as the running time that the scheme took to assign the keys among the nodes.

When compared with other key management schemes , our scheme can provide a better *MEA ratio by* increasing the number of available keys and different pool sizes doesn't effect our SKeMS scheme. By applying our SKeMS scheme to static WMNS, the *MEA ratio* is increasing while the number of nodes is increasing due to having more common shared keys between the nodes in the neighborhood. But our scheme's ratio is still better compared with the *MEA ratio* when applying the KMS scheme. Our SKeMS scheme provides a more secured network in less time compared to the existing scheme.

CONCLUSION

Initially cryptographic key management scheme KMS are implemented to achieve secure WMNs. But existing schemes are not effective against eavesdropping attacks that ultimately lead to DDoS attacks. In this paper, we implemented **S**ecure **K**ey management **S**cheme (SKeMS) in combination with an intrusion detection system, an effective solution that provides a key assignment and to enhance overall security measures in wireless mesh network. Our solution is resistant against malicious eavesdropping attacks. Our scheme, effectively reduce various other forms of network threats that ultimately lead to eavesdropping, DoS and DDoS attacks and construct an inexpensive WMNs that is Resilient and Robust.

REFERENCES

[1] Muhammad S. Siddiqui and Choong Seon Hong, "Security Issues in Wireless Mesh Networks," IEEE International Conference on Multimedia and Ubiquitous Engineering, 2007

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

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

[4] S. P. Chan, R. Poovendran, M. T. Sun, A key management scheme in distributed sensor networks using attack probabilities; *IEEE GLOBECOM' 05*, vol.2, pp.5, St. Louis, MO, USA.

[5]Dr. M.S.Aswal, Paramjeet Rawat, Tarun Kumar,"Threats and Vulnerabilities in Wireless Mesh Networks".

[6] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks; *ACM CCS'02*, Washington, DC, USA.

[7] Information Assurance Tools Report – Intrusion Detection Systems. Sixth Edition.

[8] R. L. Rivest, A. Shamir and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems", Comms of the ACM, v. 21-n.2, February 1978, pp. 120-126.

[9] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, Nov, 1976, pp. 644-654.