Secure Peer-Link Establishment in Wireless Mesh Networks

Swathi Bhumireddy, Somanath Tripathy, and Rakesh Matam

Department of Computer Science and Engineering
Indian Institute of Technology Patna
Patna, Bihar-800013
India
{som,b.swathi,m.rakesh}@iitp.ac.in

Abstract. Wireless Mesh Network (WMN) has become popular, as it allows fast, easy and inexpensive network deployment. It is observed that the current peer link establishment mechanism presented in IEEE 802.11s draft standard is vulnerable to various kinds of relay and wormhole attacks. In this paper, we propose a certificate-based peer link establishment protocol that employs location information to prevent such attacks. The security analysis shows that the proposed mechanism is resistant against different kinds of wormhole, relay and Sybil attacks.

1 Introduction

Wireless mesh networks (WMNs) have emerged as a promising technology to provide low-cost high-bandwidth wireless access services in a variety of application scenarios. A typical WMN is comprised of a set of stationary mesh routers (MRs) that form the mesh backbone and a set of mesh clients that communicate via mesh routers. WMNs have several advantages such as low-setup cost, increased coverage and most importantly reliable and flexible [1]. In spite of the above benefits, they are also constrained by the open wireless medium, varying channel conditions and interference. In addition to the above specified constraints, failing to meet the security requirements further restricts the extensive deployment of WMN. Designing of effective security mechanisms is a challenging task in WMN due to the open wireless medium which is more susceptible to attacks. The other limitation is the multi-hop cooperative communication that makes services more vulnerable to attacks especially coming from within the network.

The authenticated mesh peer-link exchange (AMPE) protocol presented in IEEE 802.11s standard (draft) [2] forms an key component in the deployment of a WMN. Vulnerabilities in the peer-link establishment mechanism makes the network susceptible to various kinds of attacks and wormhole attack is one such attack that has severe impact on performance of WMN. In a wormhole attack, an adversary can capture packets from one location and replay them at another location with the help of an out-of-band channel, simple packet encapsulation or high-powered transmission to establish a wormhole link. The route via the wormhole link would be naturally preferred by legitimate nodes as it offers a path

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 189–198.
springerlink.com

with lower hop-count and latency than any other multi-hop routes. The existing AMPE protocol cannot prevent such a wormhole attacks, as the attacker can relay peer-link establishment messages without modifying the packet contents.

Typically, a wormhole attack is handled at the routing layer in wireless mobile ad hoc networks. Various secure routing protocols have been proposed to enhance the security of such network. Few of the existing secure routing protocols are SAODV [3], SEAODV [4], LHAP [5] and ARAN [6]. It has been already shown that these protocols are vulnerable to wormhole attacks, an attack launched by colluding malicious nodes. Even though various other mechanisms exist in literature to detect and prevent wormhole attacks, the most effective way to prevent them in WMN is to secure the peer-link establishment process in WMN.

Therefore, in this paper we initially show that the current peer-link establishment process is vulnerable to relay and wormhole attacks and later propose a peer-link establishment mechanism to secure the WMN against such attacks. The rest of the paper is organized as follows. In section 2, we describe the wormhole attack in detail and its adverse effects on the network. In section 3, we present the related work on the detection and prevention of wormhole attacks. In section 4, we describe present our peer-link establishment mechanism to prevent wormhole attacks. In section 5, we present a detailed security analysis and finally section 6 concludes the paper.

2 Related Work

Several works have been carried out to specially address a wormhole attack in ad hoc networks. Most of the proposed mechanisms try to detect or prevent wormhole attacks during route discovery or data transmission. Packet Leashes [8] is one such mechanism that defends against wormhole attacks in a network. This mechanism can be used with any of the existing routing protocols. Typically with each packet, a leash(an information) is added to a packet to restrict the packet from travelling more than the maximum allowed transmission distance. The two types of leash are geographical and temporal leashes. To accommodate a geographical leash a node must know its location and all nodes must have loosely synchronized clocks. The sender includes in the packet, its own location and the time it sent the packet. The receiver compares these values to its location and the time it receives the packet. If the clocks of both sender and receiver are synchronized within some predefined bounds, then the receiver can compute a distance between itself and the sender. From the distance the receiver can estimate the minimum number of hops between the sender and itself, thereby detecting the presence of wormhole link.

Temporal leashes require nodes to have tightly synchronized clocks such that the maximum difference between any two nodes clocks is δ and δ must be known by all network nodes. The sending node includes in the packet, the time at which it sent the packet and this value is compared by the receiving node to the time it receives the packet. The receiver can determine whether the packet travelled further based on the supposed transmission time and the speed of light. The

sender could also include an expiration time in the packet so that the receiver does not accept the packet after this time.

Another alternate wormhole detection approach that uses the nodes location information is proposed by lazos et.al [9] where only a small fraction of the nodes need to be equipped with a GPS receiver. These special nodes are called guards and it is also assumed that the guards have a larger radio range (denoted by R) than the other nodes. The guards broadcast their positions in their one hop neighborhood. Two nodes consider each other neighbor only if they hear a threshold number of common guards. The nodes use the location information broadcast by the guards to detect wormholes based on the following two principles: (i) since any guard heard by a node must lie within a range of radius R around the node, a node cannot hear two guards that are 2R apart from each other; and (ii) since the messages sent by the guards are authenticated and protected against replay, a node cannot receive the same message twice from the same guard. It is shown that based on these principles, wormholes can be detected with probability close to one. However, the disadvantage of this approach is that the guards are distinguished nodes in the network that differ from the regular nodes.

EDWA [10] is an end-to-end detection of wormhole attack (EDWA) in wireless ad-hoc networks. It proposes a wormhole detection which is based on the smallest hop count estimation between source and destination. If the hop count of a received shortest route is much smaller than the estimated value an alert of wormhole attack is raised at the source node. Then the source node will start a wormhole TRACING procedure to identify the two end points of the wormhole. Finally, a legitimate route is selected for data communication. Distance between the source and destination is estimated using Euclidean Distance Estimation technique. The protocol is proposed specifically proposed for a source routing protocol and does not work with other routing protocols and also requires the length of the wormhole to be large to accurately detect and identify wormhole links.

The protocol proposed in [11] to detect wormholes attacks employs local neighborhood information. The network topology is assumed to be static and the links are assumed to be bi-directional. However, they assume that the wormhole must change the topology structure of the network and they compute edge-clustering coefficient. The assumption is that in a dense network every two neighbours must have a common neighbour. A wormhole node is detected by one of its neighbours if that neighbour cannot reach one of the wormhole neighbours without using that node. However, it is very possible to come up with many scenarios with wormholes that will not satisfy any of the necessary conditions with this approach to detect the wormhole. This will only successfully detect open wormholes or closed wormholes that only connect one single node with another single node. If the wormhole connects a group of nodes (2) with another group of nodes, which is the most common form of wormhole, then the protocol will not detect the wormhole. The protocol can be shown to report high false-positive ratio due to the kind of design methodology employed by the protocol.

Thaier et.al. propose DeWorm [12], a protocol that uses routing discrepancies between neighbours along a path from the source to destination along a path from the source to destination to detect a wormhole. It is based on the observation that to have a successful impact on the network the wormhole must attract significant amount of traffic in the network and the length of the wormhole is significantly large. Most of the existing work tries to address the wormhole attack at the network layer while the most effective way to prevent a wormhole attack in WMN is to secure the AMPE protocol.

3 Network Assumptions and Adversary Model

3.1 Network Model and Assumptions

We consider a typical WMN architecture, where a set of mesh routers (MR's) form the backbone of the WMN. We assume that a public-key infrastructure administered by a Certificate Authority (CA) exists in the network that allows nodes to obtain and authenticate using digital certificates. The MR's are equipped with GPS systems to facilitate them to determine their location information. Few of the MR's are designated with an additional functionality and act as gateway (ROOT) nodes by connecting to the Internet. Each node obtains a valid certificate from the *CA* in prior to joining the network. We also assume that a root node maintains a local directory of the certificates of all the nodes in the network and they are updated whenever a node issues or re-issues a certificate. Every root node also maintains a directory about the nodes that are under its sub-network.

3.2 Adversary Model

We consider an adversary model where an adversary is capable of relaying packets with the help of an out-of-band high speed transmission link. The adversary can also compromise an MR and collude with it to launch an FRI-Attack [7]. We also assume that an adversary is capable of generating multiple identities to establish peer-links with nodes in the different parts of the network.

4 Proposed Peer-Link Establishment Mechanism

The proposed peer-link establishment mechanism prevents various kinds of wormhole attacks during the authenticated mesh-peering exchange in WMN.

4.1 Existing Peer-Link Establishment Mechanism

The mesh peering management framework enables mesh STAs to establish, manage and tear down peering between mesh STAs. The AMPE protocol uses Mesh Peering Open frames, Mesh Peering Confirm frames, and Mesh Peering Close frames to establish, manage, and tear down a mesh peering. Mesh STAs shall

not transmit frames other than the ones used for candidate peer mesh STA discovery, mesh peering management, and simultaneous authentication of equals (SAE) to a neighboring mesh STA until a mesh peering has been established with the mesh STA. This prevents a mesh STA from gaining unauthorized access to the network resources. When a mesh STA discovers one or more neighbor mesh STAs through scanning process either through beacon or probe response frames, it may try to become a member of the mesh BSS of which the discovered mesh STA is already a member, and establishes a mesh peering with that neighbor mesh STA with the help of authenticated mesh peering exchange protocol (AMPE). The AMPE protocol requires the existence of shared pair wise master key (PMK) security association established between two candidate peer mesh STAs. If the shared Mesh PMKSA is not identified, the mesh STA shall execute an authentication protocol to mutually authenticate with the candidate peer mesh STA.

As a mesh STA accepts and processes information elements from only STAs that are registered as peers, most of the external attacks are effectively prevented. To launch any kind of external attack, the attacker should manipulate information elements to register himself as a legitimate peer. This can be carried out by exploiting the vulnerabilities in the peer-link management protocol that allows an attacker to convince two nodes located far-away as peers by relaying peer-link messages between them. An attacker can also gain access to the network with the help of a single compromised node.

Table 1. Notations employed by the proposed peer-link establishment mechanism

Notation	**Meaning**
CA	Certification Authority
Pos_A	Position locations of MR_A
$Cert_A$	Initial certificate issued by the CA to MR_A
$CertPos_A$	Certificate with position information of MR_A
R_i	i_{th} Root Node in the network
ReqCertPos	An attribute for requesting a certificate with position information
RepCertPos	An attribute in the packet the CertPos of a node RemLink
RemLink	An attribute to tear down a peer-link

4.2 Proposed Peer-Link Establishment

For a candidate MR to establish a peer link, it should pocess a certificate with position information (CertPos). To obtain such a certificate, it initiates a peer-link establishment process by presenting its initial certificate with location information. A MR needs to revoke a CertPos whenever it changes its location. We present a detailed procedure carried out by a node to obtain a CertPos. Later,

we present the revoking of the CertPos. Finally, we present how a node uses position enabled certificate (CertPos) to form wormhole free peer-links.

– **Initial Certificate Request with Position Information** A node A intended to join the mesh network presents a valid certificate (CERT) issued by CA. A node that receives a request to establish a peer-link checks for the position information. Lack of position information indicates a node trying to establish a peer-link for the first time. A peer node that receives CERT, requests for a new certificate with position information (CertPos) on behalf of the potential node intended to join the network on receiving a authentication frame with the contents ReqCertPos, Source address, Target Address, CERT and Pos from the potential node wishing to join the network. The request process is shown in Fig.1(a).

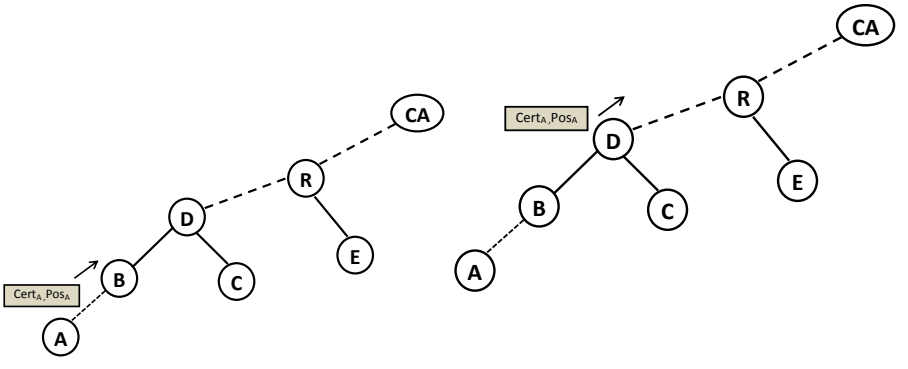

Fig. 1. (a) Step one (b) Step two

On receiving a authentication request, a peer node B checks the position information presented by A by verifying whether A is in its range of transmission. On validating the position information it propagated the authentication request to the nearest root node as only root nodes are capable of communicating with CA. The entire request process is shown in Fig.1(b). The peer node caches the information about A till it receives a CertPos. The root node propagates the authentication request to the CA as shown in Fig.2 and caches the information similar to node B.

On receiving a authentication request, the CA verifies the CERT and issues a certificate with position information in it (CertPos). The process is shown Fig.2. CA then multicast the CertPos to every root node in the network as shown in Fig.3.

All the root nodes that receive the packet from CA update their information about certificates of all the nodes in the network. The root nodes

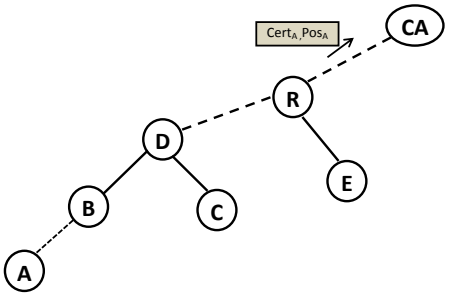

Fig. 2. (a) Step three

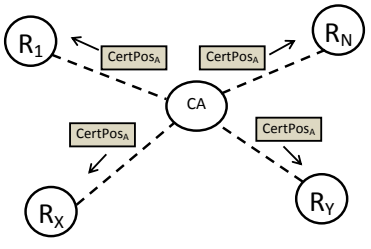

Fig. 3. Step four

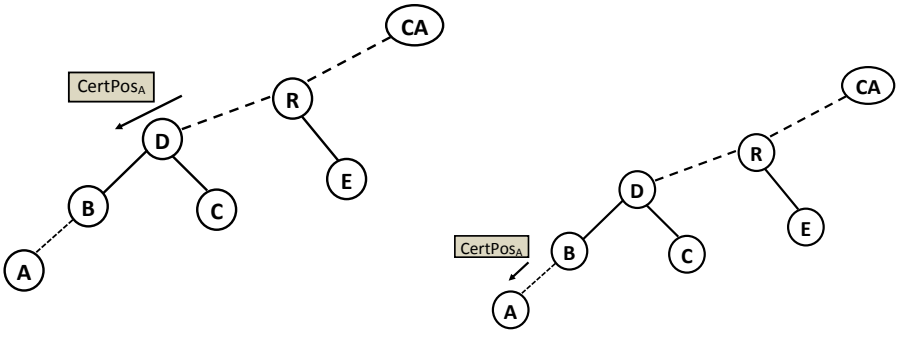

Fig. 4. (a) Step five (b) Step six

matches the CertPos with the cached information while sending the request. The only root node that has propagated the request packet forwards the authentication reply packet to the node from which it has received the request packet. As the requesting node most probably joins its sub-network, it stores the information about the node in an active directory containing the information of nodes in its sub-network.

In the final step, when the peer node receives the reply packet with the CertPos of node A, it checks its local cache to verify whether it has forwarded such a request. After verifying it propagates the reply to the node that has requested one. Finally, the new node A that has requested for a CertPos receives one form the CA through the intermediate nodes.

– **Re-issuing Certificate with modified Position Information**

Whenever a node part of the network changes its position, it has to re-issue the CertPos for establishing mesh peer links with the new peer nodes. The procedure is similar to that of a node requesting for CertPos. It only differs in the fourth and fifth steps. In the fourth step, when the root nodes receives a request with the RepCertPos attribute, it checks if there exists a node in its sub-network for which the CertPos has been already issued. If it does exist, then the root node creates a packet with the address of the node that requested CertPos and a RemLink attribute. The root node multicast's the packet to all the nodes in its sub-network.

In the fifth step, nodes in the network that receive a packet with RemLink attribute act on the information if they share peer-links with the node's present in the packet and is marked as stale. Once this process is completed, a new certificate with position information is issued to the requesting node.

– **Peer-Link Establishment** A node that possesses a CertPos wishes to establish a peer link with the nodes that it has discovered through beacon frames or probe response frames, it sends a mesh peer link establishment request packet with its CertPos appended to the authentication frame. The peer nodes that receive this packet, verifies whether the node is in its range of transmission by using the locations of the node that can it obtained from CertPos. If it does not fall in its transmission range, it simply discards the packet. On receiving a valid CertPos (meeting transmission range constraints), it sends a request to the nearest root node asking to validate the CertPos of the node with which it wishes to establish a mesh peer link. The root node that receives the validation request, verifies the CertPos and replies accordingly. In case of a valid certificate, it updates the sub-network directory and replies to the requesting node. On receiving the reply that the CertPos is genuine, the node forms a mesh peer link with the requested node.

5 Security Analysis

Security analysis of the proposed peer-link establishment mechanism depends on the ability to successfully thwart hidden wormhole, FRI-attack and sybil attack. It allows MRs to accurately verify the geographical position of nodes making authentication requests. The security of the proposed scheme is analysed for all the above mentioned attacks.

- **Hidden Wormhole Attack:** In a hidden wormhole attack, an adversary captures a peer-link establishment message and relays it to the other part of the network. A MR that receives such a peer-link message verifies the certificate and confirms the peer link establishment process thus forming a non-existent peer-link. The position certificate (CertPos) issued by the CA prevents a MR from establishing a peer-link with a node outside its transmission range. Even though an adversary can successfully relay (in-band or out-of-band) peer-link establishment messages, the CertPos prevents nodes from establishing such non-existent peer-links.
- **FRI-Attack:** In fraudulent routing information attack, an adversary has access to all the keying-material of a legitimate MR that is required to obtain a valid certificate from the CA. The proposed mechanism does not prevent an adversary from obtaining a certificate instead it prevents the adversary from colluding with the compromised MR_C. The CA that generates a revised CertPos for MR_C, broadcasts it to all the ROOT nodes to allow them to update the current node information. A ROOT node that has an entry for MR_C broadcasts a message in the sub-network to allow the MRs to invalidate the existing peer-links with such a node MR_C. Even in a case where an external adversary gains access to the network with the help of compromised MR, all the nodes that share peer-links with such a compromised MR are invalidated. Thus the proposed mechanism prevents the adversary from exploiting and disrupting the network with the help of compromised MRs effectively.
- **Sybil Attack:** A Sybil attack is the form of attack where a malicious node creates multiple identities in the network, each appearing as a legitimate node. It can disrupt network services like packet forwarding, routing, and collaborative security mechanisms. The proposed peer-link establishment mechanism inherently prevents a sybil attack as it allows a single active instance of a node identity in the WMN.

6 Conclusion

In this paper we proposed an improved peer-link establishment protocol that successfully prevents the peers from forming links with far-away nodes in the network. The proposed mechanism incurs additional overhead when compared to the existing peer-link management mechanism but it out-weighs the existing mechanism in terms of security. It also prevents stealthy attacks such as sybil attack, relay, FRI-attack and wormhole attack.

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: A survey. Computer Networks and ISDN Systems (2005)
2. IEEE P802.11s/D5.0 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)specifications, Amendment 10: Mesh Networking
3. Zapata, M., Asokan, N.: Securing ad-hoc routing protocols. In: Proceedings of ACM Workshop on Wireless Security, pp. 1–10 (September 2002)
4. Li, C., Wang, Z., Yang, C.: Secure Routing for Wireless Mesh Networks. International Journal of Network Security 13(2), 109–120 (2011)
5. Zhu, S., Xu, S., Setia, S., Jajodia, S.: LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks. In: Proceedings of ICDCS International Workshop on Mobile and Wireless Network, Providence, Rodhe Island, pp. 749–755 (May 2003)
6. Sangiri, K., Dahil, B.: A secure routing protocol for ad hoc networks. In: Proceedings of 10th IEEE International Conference on Network Protocols, pp. 78–89 (2002)
7. Matam, R., Tripathy, S.: FRI Attack: Fraudulent Routing Information Attack on Wireless Mesh Networks. In: Proc. of IEEE Xplore, ACWR (2011)
8. Hu, Y., Perrig, A., Johnson, D.: Packet leashes: A defence against wormhole attacks in wireless networks. In: Proc. of the Twenty-second IEEE International Conference on Computer Communications (April 2003)
9. Poovendran, R., Lazos, L.: A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. ACM Journal of Wireless Networks 13(1), 2759 (2005)
10. Wang, X., Wong, J.: An end-to-end detection of wormhole attack in wireless ad-hoc networks. In: Proc. of the Thirty-First Annual International Computer Software and Applications Conference (July 2007)
11. Wang, Y., Zhang, Z.: A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information. In: IEEE Fifth International Conference on Networking, Architecture and Storage, NAS (2010)
12. Hayajneh, T., Krishnamurthy, P., Tipper, D.: Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks. In: Proceedings of the IEEE Symposium on Network and System Security (2009)