SECURE CLUSTER FORMATION AND CERTIFICATE REVOCATION FOR ADVERSARY NODES IN THE MANET'S

[1]K.Jeeva, [2]N.Swathynathini

[1]PG Scholar, Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri
[2]Assistant Professor, Department of Information Technology, Jayam College of Engineering and Technology Dharmapuri

Abstract: Certificate revocation is a major security component in mobile ad hoc networks (MANETs). Owing to their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. Certificate revocation mechanisms play an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this paper, I build upon on my proposed scheme, a clustering based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. However, owing to a limitation in the schemes certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This can eventually lead to the case where malicious nodes can no longer be revoked in a timely manner. To solve this problem, I propose a new method to enhance the effectiveness and efficiency of the scheme by employing a cluster id and node id to each clusters based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. Extensive simulations show that the new method can effectively improve the performance of certificate revocation.

Keywords: Mobile ad hoc networks (MANETs), certificate revocation, security, and threshold.

1. INTRODUCTION

MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment .A mobile ad hoc network is a self- organized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multi hop relaying, which is used for various applications, e.g., disaster relief, military operation, and emergency communications. Security is one crucial requirement for these network services. Implementing security is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks.

Certification is a prerequisite to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Any attack should be identified as soon as possible. Certificate revocation is an important task of enlisting and removing the certificates of nodes who have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. In our research, we focus on the

fundamental security problem of certificate revocation to provide secure communications in MANETs.

2. RELATED WORK AND MOTIVATION

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting based mechanism and non-voting- based mechanism.

2.1 Voting-Based Mechanism

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. URSA proposed by Luo etal. Uses a voting-based mechanism to evict nodes. The certificates of newly joining nodes are issued by their neighbors. The certificate of an attacker is revoked on the basis of votes from its neighbors. In URSA, each node performs one- hop monitoring, and exchanges monitoring information with its neighboring nodes. When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Determining the threshold, however, remains a challenge. If it is much larger than the network degree, nodes that launch attacks cannot be revoked, and can successively keep communicating with other nodes. Another critical issue is that URSA does not address false accusations from malicious nodes.

The scheme proposed by Arboit et al. allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and instead each node monitors the behavior of its neighbors. The primary difference from URSA is that nodes vote with variable weights. The weight of a node is calculated in terms of the reliability and trustworthiness of the node that is derived from its past behaviors, like the number of accusations against other nodes and that against itself from others. The stronger its reliability, the greater the weight will be acquired. The certificate of an accused node is revoked when the weighted sum from voters against the node exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

2.2 Non-Voting-Based Mechanism

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate. Clulow et al proposed a fully distributed "suicide for the common good" strategy, where certificate evocation can be quickly completed by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited.

Furthermore, this suicidal approach does not take into account of differentiating falsely accused nodes from genuine malicious attackers. As a consequence, the accuracy is degraded. Park et al. proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively.
The certificate of the malicious Attacker node can be revoked by any single neighboring node. In addition, it can also deal with the issue of false accusation that enables the falsely accused node to be removed from the blacklist by its cluster head (CH). It takes a short time to complete the process of handling the certificate revocation.

2.3 Motivation

As discussed above, we compare the advantages and disadvantages between voting-based and non-voting based mechanisms. The significant advantage of the voting-based mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision process to satisfy the

condition of certificate revocation is, however, slows. Also, it incurs heavy communications overhead to exchange the accusation information for each other. On the contrary, the non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. It is able to drastically simplify the decision making process for rapid certificate revocation as well as reduce the communications overhead. However, the accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded as compared with the voting-based method. We emphasize the significant performance difference between voting based and non- voting-based methods: the former achieves higher accuracy in judging a suspicious node, but takes a longer time; the latter can significantly expedite the revocation process. In this paper, we propose a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. Like our previously proposed cluster- based schemes ,the node closest to TD.

3. MODEL OF THE CLUSTERBASED SCHEME

In this section, we introduce the model of the proposed cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from neighboring node. The scheme maintains two different lists, warning list and blacklist, in order to guard against malicious nodes from further framing other legitimate nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the false revoked nodes. Owing to addressing only the issue of certificate revocation, not certificate distribution, the scheme assumes that all nodes have already received certificates before joining the network. On the other hand, we focus on the procedure of certificate revocation once a malicious attacker has been identified, rather than the attack detection mechanism itself. Each node is able detect it neighboring attack nodes which are within one-hop away.

3.1Cluster Construction

We present the cluster-based architecture to construct the topology. Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. Before nodes can join the network, they have to acquire valid certificates from the CA, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET. While a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. Note that neighbor sensing protocols, such as periodical broadcast of hello messages, are effective approaches used in routing protocols to check the availability of links between neighboring nodes.

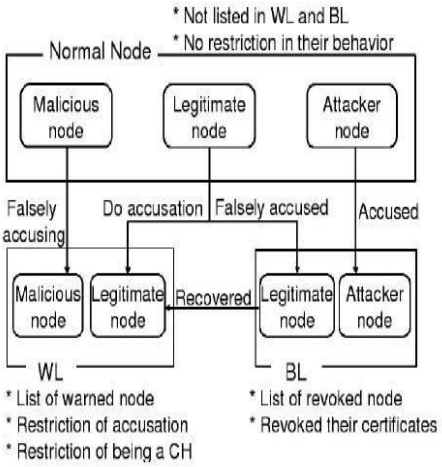

Figure 1: The classification of nodes in our scheme

A new link is detected if a node receives a new hello message. Otherwise, the link is considered disconnected if none of the hello messages is received from the neighboring node during a time period .In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members. On the other hand when a node is deemed to be a CM, it has to wait for CHP. Upon receiving CHP, the CM replies with a CM Hello Packet (CMP) to set up connection with the CH. Afterward, the CM will join this cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP in the time period Tu.We note that each CM is assumed to belong to two different clusters in order to provide robustness against changes in topology. In case a CM moves out of the transmission range of its CH, it has to search for other CHP to

participate in a new cluster. Especially, if the node does not receive any CHP for a certain period of time 2Tu, namely, there is no CH within its one-hop range, it will declare itself as a CH and propagate CHP to form a new cluster. On the other hand, in case a CH has no CM in its neighborhood range, but if there are other CHs in its neighborhood, this node assigns itself as a CM to communicate with two of the CHs.

3.2 Function of Certification Authority

A trusted third party, certification authority, is deployed in the cluster based scheme to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Blacklist, which are used to hold the accusing and accused nodes' information, respectively. Concretely, the BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node. The CA updates each list according to received control packets. Note that each neighbor is allowed to accuse a given node only once. This will be detailed in the threshold mechanism described in Section 4. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network.

3.3 Reliability-Based Node Classification

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security. A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers.

In particular, it is able to falsely accuse a legitimate node to revoke its certificate successfully. The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network. In our scheme, these nodes can be further classified into three categories based on their reliability: normal node, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal node with high reliability that has the ability to accuse other nodes and to declare itself as a CH or a CM. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes. Nodes that are listed in the warning list are deemed as warned nodes with low reliability. Warned nodes are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes (see Section 3.4.2). Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they are unable to accuse neighbors any more, in order to avoid further abuse of accusation by malicious nodes. The accused nodes that are held in the blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attackers deprived of their certificates and evicted from the network. The classification of these kinds of nodes is summarized in Fig. 1.

3.4 Certificate Revocation

3.4.1 Procedure of Revoking Malicious Certificates

We present the process of certificate revocation in this section .To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. There vocation procedure begins at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not. If not, the neighboring node casts the Accusation Packet (AP) to the CA, which the format of accusation packet is shown in Fig. 2a. Note that each legitimate neighbor promises to take part in the revocation process, providing revocation request against the detected node. After that, once receiving the first arrived accusation packet, the CA verifies the certificate validation of the accusing node: if valid, the accused node is deemed as a malicious attacker to be put into the BL. Meanwhile, the accusing node is held in the WL. Finally, by broadcasting the revocation message (see the format of broadcasting packet in Fig. 2b) including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.

4. WLMANAGEMENT

4.1 Normal Nodes Depreciation

Nodes enlisted in the WL by certificate revocation lose the function of accusation since the CA does not accept accusation packets from nodes enlisted in the WL in order to prevent further damage from malicious nodes.

Thus, as the number of malicious nodes increases, an increasing number of normal nodes are listed in the WL; subsequently, there will not be enough normal nodes to accuse the attacker nodes over time. Such scenario will affect the reliability of the scheme.

4.2 Node Releasing

As a solution to release nodes from the WL, we should first consider the two cases for nodes to be listed in the WL. As shown in Fig. 1, the first case is that a legitimate node correctly accuses an attacker node, thus resulting in the accusing node and accused node being listed in the WL and BL, respectively; the other case is the enlisting of a malicious node in the WL because it sends false accusation against a legitimate node. Hence, nodes in the WL may be legitimate nodes as well as malicious nodes. Therefore, to improve the reliability and accuracy, nodes must be differentiated between legitimate nodes and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL.

5. FUTURE WORK

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations. CHs always monitor their CMs and watch for false accusations by means of the node position or node verification algorithm. The cluster head is selected based on the high reliability value of FRD (fuzzy relevance degree). By constructing such clusters, each CH can be aware of false accusations against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM. Each cluster members are provided with C_ID (cluster id) and N_ID (node id) for an efficient detection of which cluster members belongs to which cluster.

Advantages

- The work load for every mobile node is reduced by cluster formation process
- Through cluster formation process, the mobile nodes monitoring and management of data is securable.
- The malicious node detection process results in trusted cluster formation.

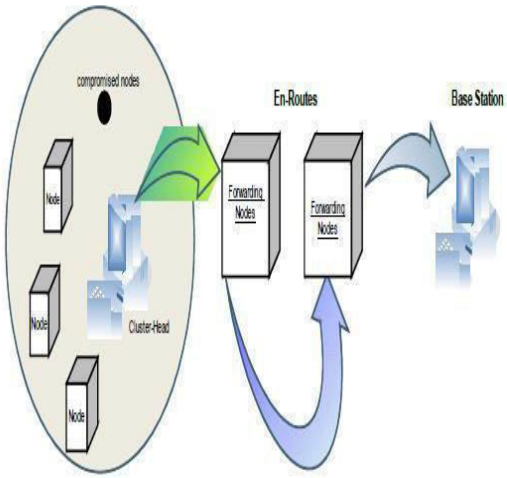

Figure 2: System Architecture

6. CONCLUSION

In this paper, we have addressed a major issue to ensure secure communications for mobile adhoc networks, namely, certificate revocation of attacker nodes. In contrast to existing algorithms, we propose a cluster-based certificate revocation with vindication capability scheme combined with the merits of fuzzy relevance clustering algorithm. The scheme can revoke an accused node based on a single node's accusation, and reduce the revocation time as compared to the voting-based mechanism.

REFERENCES

[1] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Network," Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.

[2] K. Park, H. Nishiyama N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conf. (VTC '10) May 16-19,2010

[3] H. Nakayama, S. Kurosawa, A.Jamalipour, Y. Nemoto, and N.Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology ,vol. 58, no. 5, pp. 2471-2481, June 2009

[4] Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad

Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[5] Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm.,vol. 14,no. 5, pp. 8-20, Oct. 2007.