CLUSTER SYSTEM FOR MANET USING CERTIFICATION REVOCATION PROCESS

P. Joselin Vinisha¹, D. Brintha Sweetly²
¹Assistant professor, Department of computer science, Nanjil Catholic College of Arts and Science, Kaliyakavilai, K.K.Dist
²Assistant professor, Department of computer science, Nanjil Catholic College of Arts and Science, Kaliyakavilai, K.K.Dist

Abstract - Mobile Ad Hoc Network is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. 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. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus on the issue of certificate revocation to isolate attackers from further participating in network activities.

Index terms- MANET, Threshold, Certification Revocation and Clustering.

I. INTRODUCTION

MOBILE ad hoc Networks have received reaching 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, 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.

II. MOTIVATION AND RELATED WORKS

A Cluster-based Certificate process is like a cluster-based schemes clustering is incorporated, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. It can quickly revoke the malicious device’s certificate, stop the device access to the network, and enhance network security. It has lower overhead as compared to the voting-based scheme. The reliability and accuracy is improved as compared to the non-voting-based scheme.

III. CERTIFICATION REVOCATION

The process of certificate revocation is used to revoke a malicious attacker’s certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation 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 Cluster Authority (CA), which the format of accusation packet that each legitimate neighbour 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.
IV. NODE DESCRIPTION

Nodes enlisted in the WL (Wait List) 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. Intuitively, if there are sufficient normal nodes around malicious attackers, the scheme is efficient in revoking attackers rapidly. On the contrary, if no normal node is available around an attacker node which is launching attacks to the neighborhood, the scheme cannot detect and revoke this attacker immediately until a normal node roams into the attacker’s transmission range.

V. NODE REALISING

We should first consider the two cases for nodes to be listed in 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 differentia
t e d b e t w e e n legitimate no d e s and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL. To distinguish legitimate nodes from malicious nodes, we propose a node releasing mechanism to evaluate and release legitimate nodes from the WL. First of all, we design a counter for the CA to record the number of accusations against each accused node. Moreover, the CA continues to receive accusations against the accused node following a voting period of time, T which is used for collecting accusations and releasing legitimate nodes from the WL, and subsequently compare the number of received accusations with the threshold K. In this method, we consider the accused node as a real attacker if and only if the number of accusations reaches threshold K. In the mean time, we can finally vindicate the corresponding accusing node as a legitimate node so as to release it from the WL as well as restore its function as the normal node. Otherwise, if the number of accusations fails to reach threshold K, the related accusing node will be detained in the WL. Particularly, in a special case, if the time T is set to infinite, our scheme is similar to the non-voting based scheme since the legitimate node in the WL cannot satisfy the release condition. As a consequence, determining the value of threshold K is essential for reliability and accuracy of our scheme. Conventional voting mechanisms set the threshold K as a constant value; for example, K is greater than the number of malicious nodes in the MANET. However, if the threshold is set too big, it will take a long time to determine whether a warned node is a legitimate node because the scheme has to wait for more accusations to reach the verdict a malicious attacker may never be identified because of lack of adequate support from neighboring nodes.

VI. MANET CHALLENGES

Fundamental takes with a vulnerability node to the challenge MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well defined place/infrastructure where we may deploy a single security solution. Moreover, portable devices, as well as the system security information they store, are vulnerable to compromises or physical capture, especially low-end devices with weak protection. Attackers may sneak into the network through these subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system. The stringent resource constraints in MANETs constitute another nontrivial challenge to security design. The wireless channel is bandwidth-constrained and shared among multiple networking entities. The
computation capability of a mobile node is also constrained. For example, some low-end devices, such as PDAs, can hardly perform computation-intensive tasks like asymmetric cryptographic computation. Because mobile devices are typically powered by batteries, they may have very limited energy resources. The wireless medium and node mobility poses far more dynamics in MANETs compared to the wire line networks. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network on their own will. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay.

VII. SECURITY SOLUTIONS

Detection is the wireless channel open for each node can perform localized detection by overhearing ongoing transmissions and evaluating the behaviour of its neighbours. However, its accuracy is limited by a number of factors such as channel error, interference, and mobility. A malicious node may also abuse the security solution and intentionally accuse legitimate nodes. In order to address such issues, the detection results at individual nodes can be integrated and refined in a distributed manner to achieve consensus among a group of nodes. An alternative detection approach relies on explicit acknowledgment from the destination and/or intermediate nodes to the source so that the source can figure out where the packet was dropped.

Localized Detection Watchdog is used to monitor packet forwarding on top of source routing protocols like DSR. It assumes symmetric bidirectional connectivity: if A can hear B, B can also hear A. Since the whole path is specified, when node A forwards a packet to the next hop B, it knows B’s next hop C. It then overhears the channel for B’s transmission to C. If it does not hear the transmission after a time-out, a failure tally associated with B is increased. If the tally exceeds a threshold bandwidth, A sends a report packet to the source notifying B’s misbehavior. It adds a next hop field in AODV packets so that a node can be aware of the correct next hop of its neighbors. Each independent detection result is signed and flooded multiple such results from different nodes can collectively revoke a malicious node of its certificate, thus excluding it from the network.

VIII. CLUSTER FORMATION

Lowest ID cluster algorithm (LIC) is an algorithm in which a node with chosen as a cluster head. Thus, the ids of the neighbors of the cluster head will be higher than that of the cluster head. A node is called a gateway if it lies within the transmission range of two or more cluster heads. Gateway nodes are generally used for routing between clusters. Each node is assigned a distinct id. Periodically, the node broadcasts the list of nodes that it can hear (including itself). A node which only hears nodes with id higher than itself is a cluster head. The lowest-id node that a node hears is its cluster head, unless the lowest-id specifically gives up its role as a cluster head (deferring to a yet lower id node). A node which can hear two or more cluster heads is a gateway.

Adaptive multi hop clustering is a multi hop clustering scheme with load-balancing capabilities. Each mobile node periodically broadcasts information about its ID, Cluster head ID, and its status (cluster head/member/gateway) to others within the same cluster. With the help of this broadcast, each mobile node obtains the topology information of its cluster. Each gateway also periodically exchanges information with neighboring gateways in different cluster heads.

Mobility Based Metric for Clustering proposes a local mobility metric for the cluster formation process such that mobile nodes with low speed relative to their neighbors have the chance to become cluster heads. By calculating the variance of a mobile node’s speed relative to each of its neighbors, the aggregate local speed of a mobile node is estimated. A low variance value indicates that this
mobile node is relatively less mobile to its neighbors. Consequently, mobile nodes with low variance values in their neighborhoods are chosen as cluster head. For cluster maintenance, timer is used to reduce the cluster head change rate by avoiding re-clustering for incidental contacts of two passing cluster heads. However, the mobility behavior of mobile nodes is not always considered in cluster maintenance, so a cluster head is not guaranteed to bear a low mobility characteristic relative to its members during maintenance phase. As time advances, the mobility criterion is somewhat ignored. This scheme is effective for MANETs with group mobility behavior, in which a group of mobile nodes moves with similar speed and direction, as in highway traffic. Thus, a selected cluster head can normally promise the low mobility with respect to its member nodes. However, if mobile nodes move randomly the performance may reduce.

IX. NODE CLUSTERING

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 are constructed in the proposed scheme. While each cluster consists of one CH and CMs lying within the CH’s transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster. Only normal nodes having high reliability are allowed to become a CH. Nodes except CHs join the two different clusters of which CHs exist in the transmission range of them. 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. The reason why each node except CH belongs to two different clusters is to decrease the risk of having no CH due to dynamic node movement.

X. CONCLUSION

In this paper, to ensure secure communications for mobile ad hoc networks namely, certificate revocation of attacker nodes. Additional threshold mechanism and related mechanisms are used favorways of detecting the hacker nodes. In contrast to existing algorithms, we propose a cluster-based certificate revocation with vindication capability scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. 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. In addition, we have adopted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting-based mechanism.

REFERENCES

[1] Cluster based certification revocation and vindication capability for mobile ad hoc networks, Wei Liu, StudentMember, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Je Yang, and Nei Kato, Senior Member, IEEE.