ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue 1 Ver 2 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Rationalization of Certificate Revocation Based on Cluster for Mobile Ad Hoc Network

[I]Revathy.M, [II]Durgadevi.E, [III]Saravana Kumar.S
[I,II]2nd Year – M.E. CSE, [III]Asst. Professor / CSE
[I,II,III]Srinivasan Engineering College, Perambalur, Tamil Nadu, India
E-mail : [I]m.revathivino@gmail.com, [II]durgaelamaran@gmail.com, [III]Saravana.coolya@gmail.com

Abstract
A mobile ad hoc network is vulnerable to many kinds of malicious attacks, and it is difficult to ensure secure communications. Malicious nodes directly warn the robustness of the network as well as the accessibility of nodes. Defensive legitimate nodes from malicious attacks must be considered in MANETs. Certificate revocation mechanisms play on significant role in securing a network. It can be achievable through the use of Certificate revocation with vindication capability scheme. This scheme being able to quickly revoke attacker's certificates and recover falsely accused certificates. However, due to the limitation in this scheme certificate revocation and recovery mechanism, the communication overhead for exchanging voting information is quite high, thus increasing the time needed to revoke the certificate. To overcome this situation, cluster based routing protocol is used, for reducing the communication path and increasing the mobility.

Key Words
Mobile ad hoc networks (MANETs), certificate revocation, cluster based routing protocol and security.

I. Introduction

A MANET is a self structured wireless network which consists of mobile services. Security is one key requirement for these network services. Implementing security is as a result of main importance in such networks. Provisioning confined communications between mobile nodes in a hostile environment, in which a malicious attacker can initiate attacks to interrupt network protection, is a main concern. Among all security issues in MANETs, certificate management is commonly used method which serves as a means of conveying faith in a public key infrastructure to safe applications and network services. A comprehensive security elucidation for certificate management should include three components: avoidance, uncovering and revocation.

In such networks, a certificate revocation method which invalidates attackers' certificates is essential in keeping the network secured. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. Nevertheless, it is hard for the CA to decide if an accusation is trustable for the reason that malicious nodes can potentially make false accusations. A malicious node will try to remove legitimate nodes from the network by falsely accusing them as attacker. Therefore, the matter of false accusation must be taken into account in certificate revocation mechanisms. The earlier scheme, which is based on a clustering approach, outperforms other techniques in terms of being able to rapidly revoke certificates of accused nodes and also to clearly decide false accusations.

II. Related Work

Several special types of certificate revocation techniques have been developed for mobile ad hoc networks (MANETs).Various kinds of certificate revocation techniques have been anticipated to improve network security.

A. Review of certificate control Approach

The most admired method is a simple certificate control approach by using a Certificate Revocation List (CRL) which is managed by a single CA or shared among several CAs. A digital certificate which is valid for an assured time period is assigned to each node by the CA. Kong J and Hong X [3] proposed the CA revokes the nodes that can be accused by any other node with a valid certificate and the updated CRL is broadcasted throughout the entire network. Arboit G and Crepeau C [1] address the hierarchical trust model and web-of-trust models of localized certificate revocation in MANET.

B. Review of Ticket based Approach

The one more mechanism is the tickets of newly joining nodes are issued by their neighbours. Since there is no central authority, the tickets of malicious node is revoked by the vote of its neighbours. In this method nodes cannot communicate with other nodes without valid tickets. Luo H and Kong J [5] proposed the ticket issue approach of nodes to identify both well-behaving and misbehaving nodes. The primary goal is URSA is that nodes vote with variable weights.

C. Review of Voting-Based Mechanism

This mechanism revoking a malicious attacker's certificate through votes from valid nearby nodes. The certificates of newly join up nodes are issued by their neighbours. The basis of votes from its neighbours the certificate of an attacker is revoked. Luo H and Kong J [5] proposed all nodes perform one hop monitoring, and broadcasting the monitoring information with its nearby nodes. Once the numbers of negative votes exceed a predetermined number, the accused node's certificate will be removed. In URSA, there is no Certification Authority (CA) exists in the network, and as a substitute each node monitors the behaviour of its neighbours. Park K and Nishiyama H [4] proposed certificate revocation cope with false accusation. By doing this, the correctness of certificate revocation can be enhanced. In that, all nodes are required to participate in each voting, so there is only very smallest amount chance for false accusation.

D. Review of Non-Voting-Based Mechanism

In the non-voting-based mechanism, a malicious attacker will be identified by any node with a valid certificate. Sakarindr P and Ansari N [7] address the Security in Group Communications over Wireless Infrastructure network. Certificate revocation can be quickly completed by only one accusation. Yang H and Luo H

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[9] addressed the certificate revocation based on characteristics of wireless network. However, certificates of mutually the accused node and accusing node have to be revoked concurrently. Although this approach considerably reduces both the time required to remove a node and communications overhead of the certificate revocation .Wei Liu, Hiroki Nishiyama [8] Proposed a trusted certification authority is responsible to manage control messages, asset the accuser and accused node in the warning list (WL) and blacklist (BL), correspondingly. The certificate of the malicious attacker node can be revoked by any on its own nearby node. In non-voting based mechanism there is the chance for false accusation because malicious attacker will be decided by any node in network.

III. System Design

This architecture shows the how the node are classified into different clusters and identify the malicious nodes certificate through Certificate authority. Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are placed within the communication range of their Cluster Head (CH). Each CM belongs to two dissimilar clusters in order to provide robustness against changes in topology due to mobility.

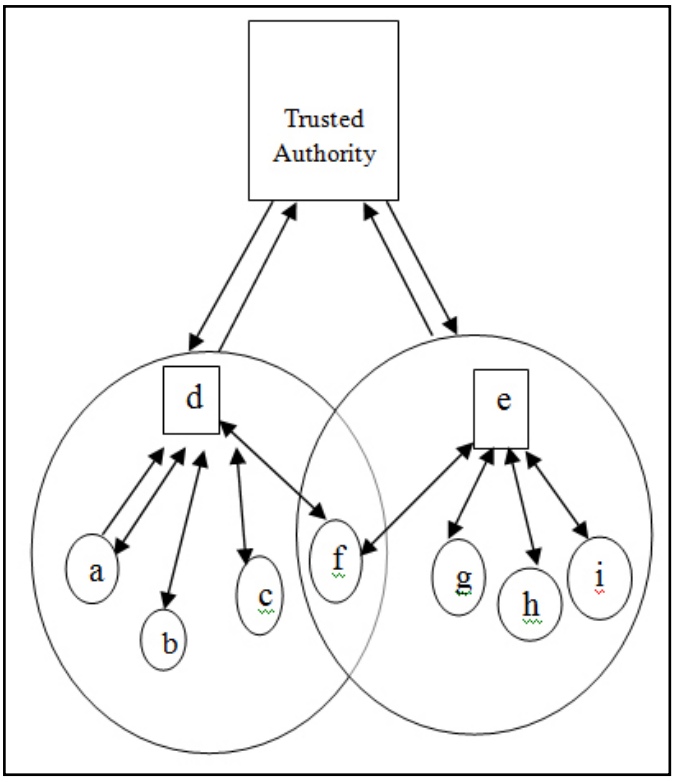

Fig.1: System Architecture

First a Source(s) nodes hello message to its Cluster Head (CH), attached with a destination name. If the destination comes under current CH means, it will forward message to that destination with source name. Else if destination not in its region means, it simply forward the message to next cluster head through the gate way. And this process will be continued still destination found or still reaching message to all cluster heads. Once if destination receives the message then it will replay for that message in the path and starts path minimizing also.

IV. Proposed Work

Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with some Cluster Members (CMs) that are positioned within the announcement range of their CH. Each CM belongs to two dissimilar clusters in order to provide robustness against changes in topology. It should be noted that because the clusters overlie, a node inside the communication range of a CH is not compulsory part of its cluster. Clustering information is used for managing certificates in the certification method. This provides a clear advantage as it enables the system to be used along with any kind of routing technology.

The aim of using clusters is to allow CHs to notice false accusations. This is based on the fact that nearly all types of attacks, like flooding attack, wormhole attack and Sybil attack can be identified by any node within the communication range of the attacker.

Contribution

Cluster based certificate revocation removes the malicious nodes certificate and message is exchanged in a minimized path. It also deals with the false accusation to improve the efficiency. 1) The nodes are classified into different clusters based on the range and forms network topology. 2) The minimized path is formed by routing protocol to reduce the overhead of the network and improve efficient message transmission. 3) The malicious nodes certificate is identified by Certificate Authority and revoked from network.

The main aim is to revoke the malicious node from the network by certificate revocation. The main challenge for certificate revocation is to revoke the certificates of malicious nodes quickly and accurately.

A. Network Topology

This network formed with authority, regions, cluster members and cluster heads. First trusted authority is formed and some regions were created by some coverage. Each node created by assigning some name and range. According to its range nodes were forms different clusters. Cluster head is elected for each region. Cluster head election is based upon their battery, memory, mobility. All these cluster heads can communicate with all the cluster members in that region.

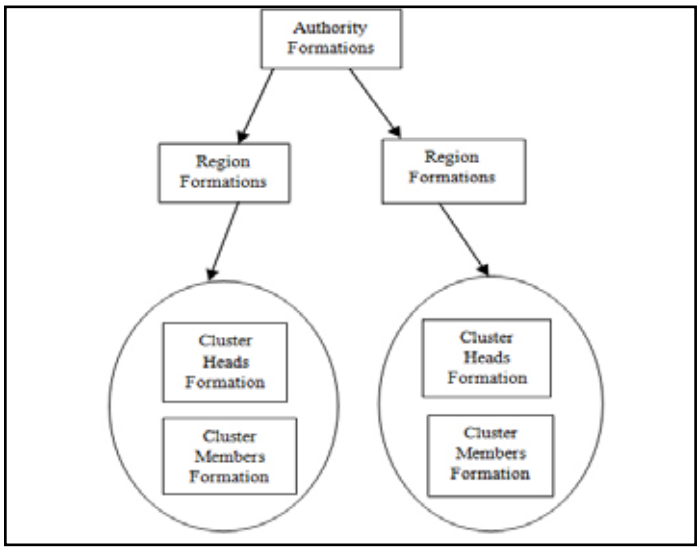

Fig. 2: Network Topology

B. Cluster Based Routing Protocol

Cluster based routing protocol for mobile ad hoc network uses clustering's structure to improve the average packet delivery ratio. In path finding, first a Source(s) nodes hello message to its Cluster Head (CH), attached with a destination name. If the destination comes under current CH means, it will forward hello to that destination with source name. Else if destination not in its region means, it simply forward the mess to next cluster head through the gate way. And this process will be continued still destination found or still reaching mess to all cluster heads. Once if destination receives the message then it will replay for that message in the path and starts path minimizing also.

C. Certificate Revocation

If any node in network is trying to do some malicious activity and it is detected by some other node means, the detector will intimate about the accused node to destination, claiming that nodes as accuser. Once trusted authority receives this complaint, it forward that accuser name to all cluster heads to know it is malicious or not. And all clusters heads forwards that information to all nodes except to accuser and complained node. So now all nodes checks with their buffer that this node is previously performed malicious activity or not.

Once cluster heads receives all replays, it sends total no of attack counts and non attack counts to trusted authority. Now trusted authority will have all nodes replies about that accuser. If maximum number of nodes tells that, accused node is attacker means, that node is added to block list and intimated to all nodes through cluster heads. Else non attacker count is more means, the node in block list will be released and intimated node will add to that list.

V. Conclusion

In this paper, to revoke the malicious nodes certificate by using voting based mechanism. It is aimed to revoke the malicious nodes certificate from further participating in the network. First nodes are grouped into cluster based on range or distance. The voting based mechanism will identify, whether newly arriving node in the particular cluster is legitimate node or malicious node. This required only minimal bandwidth consumption and lover operational traffic. The Cluster Based Routing Protocol (CBRP) is proposed for the message transmission or root establishment between the source and the destination. The false accusation also deals with by voting based mechanism. This also provides the minimized path and timely message transmission.

VI. Acknowledgment

We would like to thank our college Srinivasan Engineering College, principal Mr.K.Elangovan, our HOD Mrs.S.Jayanthi, my guide Mr.S.Saravana Kumar and other staff for their continuous support and for their helpful comments on the earlier drafts of this paper.

References

[1] *Arboit G, Crepeau C, Davis C.R, and Maheswaran M, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17- 31, Jan. 2008.*

[2] *Chan H, Gligor V, Perrig A, and Muralidharan G, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," IEEE Transaction. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.*

[3] *Hu Y, Perrig A and Johnson D, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.*

[4] *Hegland A.M, Winjum E, Rong C, and Spilling P, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.*

[5] *Kong J, Hong X, Yi Y, Park J.S, Liu J, and Gerla M, "A Secure Ad-Hoc Routing Approach Using Localized Self-Healing Communities," Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing, pp. 254-265. 2005.*

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

[7] *Luo H, Kong J, Zerfos P, Lu S., and Zhang L, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.*

[8] *Park K, Nishiyama H, Ansari N, and Kato N, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc. IEEE 71st Vehicular Technology Conference, May 16-19, 2010.*

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

[10] *Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato "Cluster-Based certificate revocation with Vindication capability for Mobile Ad Hoc Networks" IEEE Transactions, Feb. 2013.*

[11] *Yang H, Luo H, Ye F, Lu S, and Zhang L, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb.2004.*

[12] *Yang H, Shu J, Meng X, and Lu S, "SCAN: Self Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no.2, pp. 261-273, Feb. 2006.*

[13] *Yi P, Dai Z, Zhong Y, and Zhang S, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.*

[14] *Zhou L, Cchneider B, and Van Renesse R, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.*

[15] *Zhou L and Haas Z.J, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.*