ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Threshold Technique for Mobile Ad-Hoc Networks Using Secured Revocation Check

D.C. John Thangaraj, R.Tamilarasi

PG Student, M.E (Embedded Systems), AMS Engineering College, Namakkal, Tamilnadu, India[1]

PG Student, M.E (CSE), Christian CET, Oddanchatram, Dindigu, Tamilnadu, Indial[2]

ABSTRACT - In Mobile Ad Hoc Network (MANET) adopting certification systems, it becomes possible to exclude identified attackers from the network permanently by revoking the certifications of the attackers. A simple way to identify attackers is to collect information on attackers from nodes in the network Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined 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.

I. INTRODUCTION

MOBILE ad hoc Networks (M A N E T s) h a v e received inc reaching attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A simple way to identify attackers is to collect information on attackers from nodes in the network Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. 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 (PDA), 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 networks. To meet this challenge, certificate revocation is an important integral component to secure network communications.

II. RELATED WORK

In this project, we proposed a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. Like our previously proposed cluster-based schemes clustering is incorporated in our proposed scheme, 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

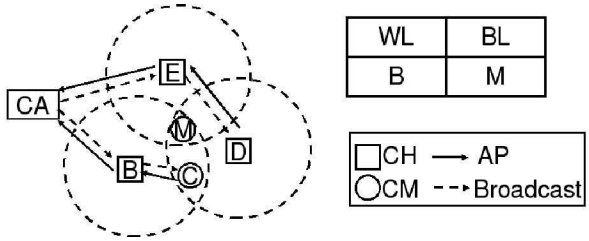
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. -PROCESS MODELING

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 CA, which the format of accusation packet 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 including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network. As discussed above, we compare the adv ant age s 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 t o satisfy t h e condition of certificate revocation is, however, slow. Also, it incurs heavy communications overhead to exchange the accusation information for each other.

IV. NODE UTILIZATION

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. 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. In a MANET, mobile nodes are assumed to be uniformly distributed over a coverage area so as to satisfy the binomial distribution B ðn; q Þ [21], which denotes the probability of a number of nodes existing in a special area.



Here, n denotes the total number of cells where a MANET is divided into; q is the probability that one cell is occupied by a single node. When n is very large and q is very small, the binomial distribution Bð n; q Þ is approaching the Poisson distribution with parameter , which is equal to the number of nodes NQ.

V. NODE SECURITY

Security is an important issue for ad hoc networks, especially for security-sensitive applications. To secure in ad hoc net- work, we consider the fallowing attributes: *availability, dentiaiulity, integrity, nutlienticalion,* and *non repudiation. Availability* ensures the survivability or network services despite denial-of-service attacks. **A** denial-of-service attack could be launched any layer of in ad hoc network. On the physical and media access control Layers, an adversary could employ jamming to interfere with communication on physical channels. the network Layer, an adversary could disrupt the routing protocol and disconnect the network. On the high- Once such target is the key in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

essential service for any security framework. *Confidentiality* that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic tactical military information, requires confidentiality. Leakage of such in for cases because the information might be valuable for epidemics cases because the information might be valuable for epidemics.

VI. MANET CHALLENGES

One fundamental vulnerability of 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/infra- structure 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 band- width-constrained and shared among multiple networking entities. Second, the security solution should span different layers of the protocol stack, with each layer contributing to a line of defense. No single-layer solution is possible to thwart all potential attacks. Third, the security solution should thwart threats from both outsiders who launch attacks on the wire- less channel and network topology, and insiders who sneak into the system through compromised devices and gain access to certain system knowledge. Fourth, the security solution should encompass all three components of prevention, detection, and reaction, that work in concert to guard the system from collapse. Last but not least, the security solution should be practical and affordable in a highly dynamic and resource-constrained networking scenario.

VII. LOWEST ID CLUSTER ALGORITHM

Lowest ID Cluster algorithm is an algorithm in which a node with the minimum *id* is 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.

VIII. ADAPTIVE MULTI HOP CLUSTERING

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 clusters and reports to its cluster head. Thus, a cluster head can know the number of mobile nodes of each neighboring cluster. Adaptive multi hop clustering sets upper and lower bounds (U and L) on the number of cluster members within a cluster that a cluster head can handle.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IX. 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 favor ways 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 nonvoting 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, Student Member , IEEE , Hiroki Nishiyama, Member , IEEE, Nirwan Ansari, Fellow, IEEE, J ie Yang, and Nei Kato, Senior Member , IEEE.

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

[3] Security and Trust Management in Self-organizing Wireless Ad hoc Networks, Ling Liu, Distributed Data Intensive Systems Lab.

[4] Subir kumar sarkar, T G Basavaraju Ad hoc wireless networks.

[5] Review of efficient clustering algorithms used in MANET, Kanika garg and Lalit Kumar.

[6] J . L iu, X . J iang, H . N is h iyam a, and N . K ato, "Delay and capacity in ad hoc m obile networks with f- cast relay algorithms ," *IEEE Trans. Wireless Commun.* , vol. 10, no. 8, pp. 2738–2751, Aug. 2011.

[7] C. R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks," *IEEE JSAC*, vol. 15, pp. 1265–75, Sept. 1997.

[8] T. J. Kwon *et al.*, "Efficient Flooding with Passive Clustering an Overhead-Free Selective Forward Mechanism for Ad Hoc/Sensor Networks," in proceedings of *IEEE*, vol. 91, no. 8, pp. 1210–20, Aug. 2003

[9] J.-H. Ryu, S. Song, and D.-H. Cho, "New Clustering Schemes for Energy Conservation in Two-Tiered Mobile Ad- Hoc Networks," in proceedings of *IEEE ICC'01* , vo1. 3, pp. 862–66,June2001.