International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, 2014
ISSN 2091-2730

Improved Reliable Based Node Classification Using Dissect Method in Mobile AD HOC Network

Mr. N. SENTHIL KUMARAN, M.C.A. , M.Phil.,[1]
ASSISTANT PROFESSOR & HEAD,
DEPARTMENT OF COMPUTER APPLICATION,
VELLALAR COLLEGE FOR WOMEN, ERODE, INDIA.
n.senthilkumaran@hotmail.com

R.MOHANA PRIYA,[2]
M.Phil- FULL TIME RESEARCH SCHOLAR,
DEPARTMENT OF COMPUTER SCIENCE,
VELLALAR COLLEGE FOR WOMEN, ERODE, INDIA.
monarangan@gmail.com, 9789692346

Abstract— Certificate Revocation mechanisms play an important role in securing a network[6]. Malicious nodes directly threaten the robustness of the network Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from malicious attacks must be considered in MANETs [1]. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this paper additionally uses two concepts: They are fixed window model and sliding window model of which the latter produces the best output with slight increased calculation overhead. In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In this paper, proposed scheme is based upon a improved reliable based node classification scheme, which outperforms other techniques in terms of being able to quickly revoke attacker's certificates and recover falsely accused certificates.

Keywords—Mobile Ad Hoc Networks, False Positive, False Accusation, Malicious Node, Intrusion Detection, Certificate Authority

I.INTROUCTION

An ad hoc network is a collection of mobile nodes forming a temporary network without the aid of any centralized administration[5]. A wireless ad hoc network is a decentralized type of wireless network which does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless network [3]. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks [3].Mobile ad hoc networks have attracted much attention due to their mobility and ease of deployment [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently[5]. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic[5]. Such networks may operate by themselves or may be connected to the larger Internet.

Security is one crucial requirement for these network services [1].The existing works maintains two different lists, warning lists and blacklist, in order to guard against malicious nodes. Determine 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.

The proposed work is based on improve the reliable of warned node to take part in certificate revocation process. To enhance the accuracy, proposed system used the threshold based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. The performances of the scheme are evaluated. In this paper the proposed system used two concepts; fixed window model and sliding window model of which the latter produces the best output with slight increased calculation overhead. In monitoring- based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In most cases, a node

only monitors its next hop in a route. In network if any node doing some malicious activity then we are revoking the certificate of that node, in other word we are removing that node from all communication links.

The main contributions of this paper are:

- To certificate revocation and provide secure communications.
- To find any attack should be identified as soon as possible.
- To verify that a public key belongs to an individual and to prevent tampering and forgoing.
- To mitigate malicious attacks on the network.

The rest of this paper is organized as follows: Section 2 presents the related work followed by the structure of the cluster based scheme and introduces the certificate revocation process describes in Section 3. Section 4 gives a brief explanation of the proposed approach. Section 5 presents the performance evaluation of our scheme. Finally, conclude the paper in Section 6.

II. RELATED WORK

Mobile ad hoc network gets much attention because in mobile ad hoc network topologies are dynamically formed, it is infrastructure less and mobile in nature[5]. Because of the mobility in nature it is difficult to provide security in the mobile ad hoc networks. Provide security in mobile ad-hoc network we forming the cluster and providing the valid certificate to each node present in that network[2]. By using that certificate nodes are securely communicating with each other. Suppose any node doing some malicious activity then in that case certificate of that node is revoked. For revoking the certificate of misbehaving node there are mainly two techniques: voting based technique and non-voting based technique [1]. The decision processes to satisfy the condition of certificate revocation is, however, slow.

In monitoring-based intrusion detection, each node monitors the forwarding behavior of its neighboring nodes. In most cases, a node only monitors its next hop in a route. For monitoring purpose, nodes keep track of a window of packets that it sent recently to its next hop. Two types of window can be used to keep track of monitoring: fixed window or sliding window.

To understand the similarities and differences between the fixed and sliding windows, assume that noise does not impact the overhearing of transmission within a node's radio range. In such a scenario, a malicious node can drop up to L-1 packets out of W on the average without risking suspicion by neighbors. The temporary drop rates can be different. The sliding window approach is free of this deficiency since in any consecutive W-transmitted packets, a malicious node may drop at most L-1 packets without risking suspicion by neighbors. To model state is sliding window–based monitoring using a discrete-time Markov chain.

III MODEL OF THE CLUSTER-BASED SCHEME

In this section, we introduce the model of cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from a 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 falsely revoked nodes.

CLUSTER FORMATION

Cluster based [20] mechanism for formation of cluster in the mobile ad hoc network. Each cluster having the cluster head (CH),cluster members and the group of cluster having one CA. If any node comes in the particular range then firstly it take valid

certificate from the CA. These cluster heads are responsible for the routing process. A gateway is a node that has two or more cluster heads. Each cluster head has several cluster members. Due to the clustered structure there will be less traffic, because route requests will only be passed between cluster heads.

The steps for implementation of cluster

Step 1-If new node then first take valid certificate from CA.

Step 2- New node sends the CHP packet to the neighboring nodes.

Step 3-a) If that node doesn't getting any reply within time period T then it becomes CH.

b) If any node sending the CMP packet to new node then new node become the CH otherwise it become the cluster member.

Step 4-If CM moves from out of the range then wait for CHP. In time period T If getting the CHP then the cluster member otherwise it declare itself as a cluster head.

CERTIFICATION AUTHORITY

It is a trusted third party having authority of providing valid certificate to node present in the cluster as well as newly joining node. It is also having the responsibility of maintaining the updated warned list and black list. Warned list is containing the accuser node and black list containing the accused node present in the network[20]. Another responsibility of CA is to broadcast updated warned list and black list to node present in the entire network.

CLASSIFICATION OF NODE

In our scheme we are classifying the node into three types

1. Normal node / legitimate node-Those nodes that are secure and communicate with other node securely. It also is having the authority to revoking the certificate of accused node.
2. Malicious node- Those nodes that are insecure for communication. They are performing the malicious activity in the network and does not having any authority to revoking the certificate of node present in the network.
3. Warned node-warned node means those nodes that accusing the other nodes are consider as warned node. Also it does not having any authority to revoking the certificate of other malicious nodes. Only it is having the permission to communicate with other nodes along with some restriction.

CERTIFICATE REVOCATION

In the cluster if any node wants to communicate with other node then by using the valid certificate they securely communicate with each other. Suppose in the network some nodes are doing the malicious activity and it is found by the neighboring node then neighboring node first check the local black list [8]. If that node present in that black list then the certificate of the malicious node is directly revoked by that neighboring node by using non-voting based Scheme [1] otherwise it send the accusation packet (AP) to the CA. Accusation packet containing all the information of accuser, accused node and destination. After sending the information CA check the certificate of accuser[18]. If it is valid then it put accuser into WL and accused node in BL and the list is updated. Finally updated information is send to the all nodes that are present in the network[6]. If it is a malicious node then it will await for certification revocation. Once the node is revoked then it should remove from the network.

COPING WITH FALSE ACCUSATION

In this scheme it enable CH to detect false accusation present in the cluster. For finding the falsely accused node present in the cluster first he monitoring the all attacks done by the CMs [7]. After monitoring it sends recovery packet to the CA to recover the certificate of the falsely accused node.CA verify the recovery packet received from the CH and he remove the falsely accused node

from BL to WL. But here is another problem is the numbers of nodes in WL are increases and accuracy of revoking the certificate of malicious node in the network decreases, because no of normal nodes in the network are less.

Step 1: The CA disseminates the information of the WL and BL to all nodes in the network.

Step 2: CH E and F update their WL and BL, and determine that node B was framed.

Step 3: E and F send a recovery packet to the CA to revive the falsely accused node B.

Step 4: Upon receiving the first recovery packet (e.g., from E), the CA removes B from the BL and holds B and E in the W L, and then disseminates the information to all the nodes.

Step 5: The nodes update their WL and BL to recover node B.

IV. PROPOSED SCHEME

The proposed system contains all the existing system implementation. In addition, it extends the protocol model to consider the drop detection packet. Markov model is to determine analytically the expected time to suspect its next hop by a monitoring node. Markov models are commonly used to analyze the expected time to encounter a bug in a software system.

Fixed Window Protocol [FWP]

The fixed window protocol monitors the packet drops detection by checking the front and rear side of the packet. So the drop detection can be finding effectively. The sliding window protocol monitors the packet drop detection in the sequence of packets. It is possible to reduce the number of false positive due to monitoring by having higher threshold values, allowing a node to exceed the not-overheard threshold multiple times before labeled as suspicious, or both. This will mitigate the false positive problem in normal networks without attacks.

Sliding Window Protocol [SWP]

The sliding window protocol is a mechanism for reliable message delivery in a distributed setting where a sender and a receiver communicate over loss channels. Any message delivery protocol has the same basic four components, a sender, a receiver, a channel from the sender to the receiver, and a channel from the receiver to the sender.

In addition to the four components we model, there are two external users. The user on the sender side inputs the data to be sent by the sender and the user on the receiver side gets the data that the receiver delivers. The basic idea of the sliding protocol is that a window of size $\mathbf{n \geq 0}$ determines how many successive packets of data can be sent in the absence of a new acknowledgment. The window size may be fixed or may vary depending on the conditions of the different components of the protocol. In our model we will assume that **n** varies none deterministically. Each packet of data is sequentially numbered, so the sender is not allowed to send packet **i + n** before packet **i** has been acknowledged. Thus, if is the sequence number of the packet most recently acknowledged by the receiver, there is a window of data numbered **i + 1** to **i + n** which the sender can transmit. As successively higher-numbered acknowledgments are received, the window slides forward.

The acknowledgment mechanism is cumulative in that if the receiver acknowledges packet **k,** where $\mathbf{k \geq i + 1}$, it means it has successfully received all packets up to **k**. Packet is acknowledged by sending a request for packet **k+1**. Typically, transmitted data is kept on a retransmission buffer until it has been acknowledged. Thus, when **k** is acknowledged, packets with sequence number less than or equal to are removed from the retransmission buffer. Packets that are not acknowledged are eventually retransmitted. For our

modeling of the sliding window protocol we assume that sequence numbers are unbounded, we do not assume that the channels are FIFO

V. PERFORMANCE EVALUATION

The experiments were conducted using cluster based revocation certificate scheme. The result of proposed Marko Chain model is discussed and compared with existing routing protocol. To measures the performance of the works under packet drop threshold, attacker detection, and throughput are evaluated.

In packet drop threshold is normally sending the data from source to destination. Comparing existing delivery drop packet with proposed work is Marko chain model for hope by hope, multi-hop fixed window protocol [MFWP] and multi-hop sliding window protocol [MSWP] in communication mobile-ad-hoc networks. The packet drop were calculated so that their values lie in fixed and sliding window protocol is greater but in multi-hop fixed and sliding window protocol the drop count is lesser. In static threshold [1] accuracy of realizing normal node from WL is less. Performance for cluster based revocation certificate in dynamic threshold, first design a simplified mechanism to determine the number of neighboring nodes for any given node.

Within time Tv, the given node crosses through an area and meets a number of neighbors N. Since mobile nodes are assumed uniformly distributed in the network, we may approximate N by

$$N = (\pi r^2 + 2rvT_v)\rho,$$

Where r denotes the transmission range of nodes, *v* is the velocity, and *p* is the density of nodes in the network. Based on the obtained number of neighboring nodes N, we can on firm the value of threshold K. By this mechanism it is possible to remove the normal node from WL and allow that normal node to take a part in revocation process.

Comparison of both existing and proposed system experiment result is Fig 1.1 represents experimental result for existing system. The finding malicious node and revocation node process within minutes details. The Fig 1.2 represents experimental result for proposed system. The finding malicious node and revocation node process within minute's details as followed.

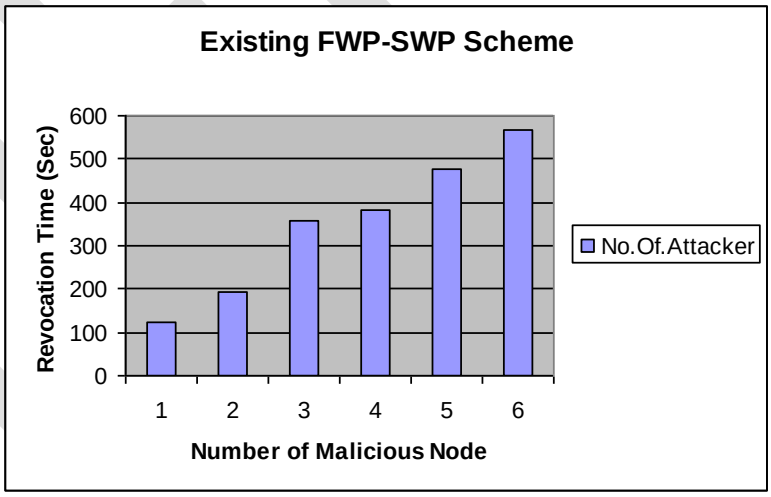

FIG 1.1 FWP-SWP- Number of Attacker

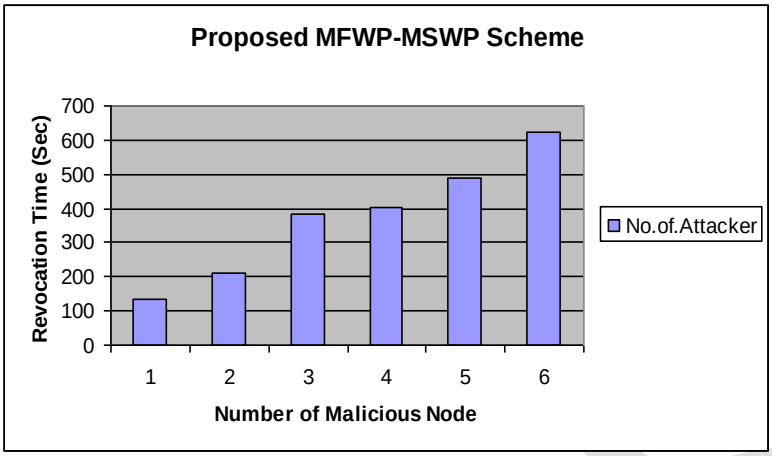

FIG 1.2 MFWP-MSWP- NUMBER OF ATTACKER

ACKNOWLEDGMENT

I am greatly obliged to **Dr. (Mrs.) S. K. JAYANTHI,** Associate Professor and Head, Department of Computer Science, Vellalar College for Women (Autonomous), Erode -12 for providing me all the facilities, and an inspiration to complete the research Paper. I take this golden opportunity to express my profound and grateful thanks to my beloved Guide, **Mr. N. SENTHIL KUMARAN, M.C.A., M.Phil.,** Assistant Professor & Head, Department of Computer Applications**,** Vellalar College for Women (Autonomous), Erode-12 for his exemplary guidance and help, with valuable and creative suggestions and constant encouragement for the successful completion of the paper.

VI.CONCLUSION

In this paper, we have enhanced our previously clustering-based certificate revocation scheme which allows or fast certificate revocation. In order to address the issue of the number of normal nodes being gradually reduced, we have developed threshold based mechanism to restore the accusation function of nodes in the WL. The effectiveness of our proposed certificate revocation scheme in mobile ad hoc networks has been demonstrated through extensive results**.** In the proposed work is detecting attacker and improve certificate authority in mobile ad hoc network. In this model, they are several certificate issue solving and communication between nodes with cluster member. The proposed protocol MFWP and MSWP model applied for mobile ad hoc network is to improve and effective management for BL and WL maintains communication process. In contrast to existing system, we propose a improved reliability based node classification 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

REFERENCES:

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato, "Cluster Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Network", IEEE Transactions on Parallel and Distributed Systems, Vol.24, No.2, Feb 2013.

[2] Pratik Gite, Sanjay Thakur, " Different Security issues over MANET", International Journal of Computer Science Engineering & Information Technology Research, Vol.3, Issue 1, March 2013.

[3] Gagandeep, Aashima, Pawan Kumar, " Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Vol.1, Issue-5, June 2012.

[4] Scalable Network Technologies: Qualnet, http://www.scalable-networks.com, 2012.

[5] Priyanka Goyal, Vinti Parmer, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications", International Journal of Computational Engineering and Management, Vol.11, Jan 2011.

[6] 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.

[7] 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.

[8] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks " School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.

[9] P. 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.

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

[11] H. Yang, J. Shu, X. Meng, and S. Lu, "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

[12] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. CRYPTO '84, 1984, pp. 47–53. and Computing, pp. 254-265. 2005.

[13] Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "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.

[14] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, 2005.

[15] 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

[16] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.

[17] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Net-works," IEEE Trans. Mobile Computing, vol. 2, no. 3, pp. 257-269, July-Sept. 2003.

[18] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROC RYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293, 2003.

[19] IEEE-SA Standards Board, "IEEE Std. 802.15.4," IEEE, 2003.

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