International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 7, July - 2014

Clustering of Certificate Revocation to Reinforce an Idea for Mobile Ad Hoc Networks

Prof.Steven Raj N
Assistant professor in GNDEC (CSE), Bidar

Sneha Kathare
M.techII year student (CSE)

***Abstract*--Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate with other nodes without any fixed infrastructure.MANET's have increased the attention in recent years because of their wireless and dynamic nature. MANET's provide the users anytime and anywhere services in the infrastructure less wireless network. Since MANET's have the dynamic nature there is a high possibility of violating the security attacks in the network.To reduce the attacks in the network,I introduced certificate revocation. Certificate revocation plays an important role for securing a network. When a certificate of a malicious node is revoked, it denies from all its activities and it is separated from the network. The main focus for certificate revocation is to revoke the valid certificate of a malicious node reliably and accurately. This paper proposes the clustering of certificate revocation to reinforce an idea for MANET for being able to quickly revoke attacker certificate and to recover falsely accused certificate. To increase the reliability, we recover falsely accused nodes to take part in certificate revocation process and to improve the accuracy, we propose threshold based mechanism to restore nodes accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANET. Simulation shows that the new method can effectively improve the performance of certificate revocation.**

Keyword:MANET, certificate revocation, threshold, recovery.

1.INTRODUCTION

Mobile Ad hoc Networks (MANETs) are a type of wireless ad hoc network. It is a self-configuring network of mobile devices and it does not need require any infrastructure. This type of mobile network is formed by a number of self-organizedmobile nodes such as cell phones, palm handheld computers, iPods, etc. These devices can act as both routers and as well as end users [5]. The reason for using MANET is it does not require any infrastructure support. So it is not assured that all the nodes in the network are trusted. It has all the functionalities of a traditional network such as seamless interaction, neighbor discoveryand data forwarding abilities. It provides flexible network architecture so that it can be able to provide

communication in the case of the limited connectivity range and resource constraints. It is able to do fast establishment of networks and using the service discovery protocol and also each node finds its neighbor node to transmit the packet to its destination [6].

Each device in MANET is free to join, free to move independently in any direction and then leave the network at any time without any restriction [1]. Due to the dynamic nature of MANET, it is vulnerable to any kind of attacks. If any intermediate node that does not transmit the data packet to its neighbor or it sends many numbers of acknowledgements for a single received packet, then this type of node is considered as a malicious node. This node violates the security of the network [10]. Protecting legitimate nodes in the network from malicious attacks must be considered. To improve security of the network, certificate revocation scheme is used. This scheme enhances the security and robustness of the network.

Certificate is a certificate provided by the Certificate Authority (CA) which makes the mobile node to joins the network. If any node wants to communicate with other nodes in the network then it has to get the valid certificate from the Certificate Authority. Thenode without the valid certificate cannot be able to communicate with other nodes in the network. Also each node can transmit packet to the other nodes which are in the transmission range only.

2. EXISTING SYSTEM

It is difficult to secure MANET because of its vulnerability and wireless network.Many kinds of certificate revocation techniques have been used to develop the network security.The existing system approach has been classified into two categories: voting based mechanism and non-voting based mechanism.

A.Voting based mechanism:

The voting based mechanism helps in revoking a malicious attacker's certificate through votes from valid neighboring nodes.

URSA [1] proposed by H. Luo. uses a voting based mechanism to evict nodes. Every node which is going to participate in the network must have a valid certificate along with it. When an existing node moves to a new location or a new node joins the network, it must have a valid certificate which is exchanged with its neighboring nodesto establish mutual trust relationship. Misbehaving nodes without valid certificate will be denied from all the network activities; therefore it is isolated from the mobile ad-hoc network.

The scheme proposed by G. Arboit *et al.* [2], referred to as the voting-based scheme, allows all nodes in the network to vote. In this scheme Certificate Authority (CA) does not exists in the network, and instead of CA each node monitors the behavior of its neighbor's nodes. MANET allows revoking the certificates of malicious node, by doing so the malicious nodes areeffectively separated froma particular MANET. This scheme is mainly designed to prevent malicious nodes from being able to use wrongful accusations to cause the revocation of the certificates of normal nodes. The value of a node determines the weight of its accusation. The weight is calculated from a node's reliability which is derived from its past behavior. The higher the reliability, the greater the weight will be. The certificate of a suspicious node can be revoked when the sum of the weights of the votes against the node reaches threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate during every vote, the communication overhead required to exchange voting information is quite high, thus increases the time needed to revoke the certificate.

B.Nonvoting based mechanism:

In the nonvoting based mechanism, a malicious attacker will be identified by any node with a valid certificate.

J. Clulow[3] proposed the suicide for the common good scheme. In this scheme, the certificate revocation can be quickly completed with just an accusation,it not only revokes the certificate of the accused node but it also revokes accuser's certificate. In other words, at least one node has tosacrifice itself to remove an attacker from the network. This strategy dramatically reduces both the time required to evict a node and the communication overhead of the certificaterevocation procedures. However, owing to its suicide-based strategy, the application of this approach is limited. This scheme does not provide a mechanism to differentiate falselyaccused legitimate nodes from properly accused malicious nodes.

K. Park [4] proposed the certificate revocation cope with false accusation scheme which is responsible for managing the control messages. There will be warning list and black list created. The accuser node is put into the warning list and accused node will be put into the black list. The certificate of the malicious attacker node can be revoked by any one nearby node. There is a chance of false accusation that enables the falsely accused nodes to be removed from the black list.

3.IMPLEMENTATION

The proposed cluster based revocation scheme shows the quick revocation of an attacker node on receiving one accusation packet from neighboring node[11].The nodes in the network are classified into several clusters and identify the malicious nodes certificate throughCertificate authority.

First, 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) [7].Each CM belongs to two dissimilar clusters in order to provide robustness against changes in topology due to mobility.

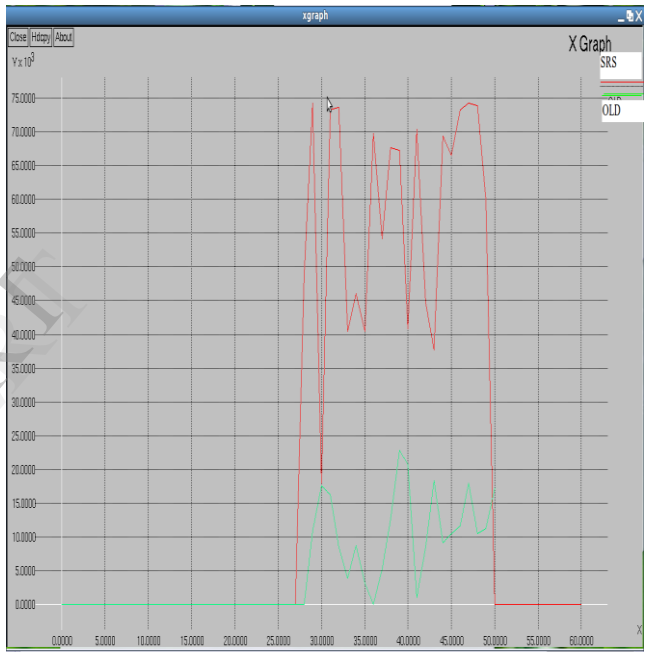
When a node takes part in the network, it is allowed to declare itself as a cluster head. When a node declares itself as a cluster head, it generates a CH hello packet to notify the neighbor nodes periodically. The nodes that are in the cluster head transmission range can accept the packet to participate in the particular cluster as a cluster member. When the node is declared as a cluster member, it has to wait for cluster head packet for a new link between cluster head and cluster member. If no cluster head packet is received by cluster member during a time period then the link is considered to be disconnected. On receiving cluster head packet, the cluster member replies with a cluster member hello packet to set up a new link with cluster head. Then cluster member joins the particular cluster, Cluster Head and cluster member keep in touch with each other by sending CH packet and CM packet in a time period.

Second, Certificate Authority (CA) is an entity that issues a digital certificate. [5] CA issues digital certificate that contains a public key and the identity of the owner [9]. Before nodes can join the network they have to acquire valid certificate from the CA. CA is responsible for managing and distributing certificates of all nodes, so that they can communicate with each other. CA is also responsible for maintaining two list:Warned List,Black List. Warned List (WL) is used to hold corresponding accusing node. Black List (BL) is responsible for holding the node accused as an attacker. CA updates each list according to received packets.The aim of using clusters is to enable Cluster Heads to detect false accusations. It requests for the Certificate Authority to recover the certificates of falsely accused nodes that can only be made from Cluster Heads. A Cluster Head will send a Certificate Recovery Packet (CRP) to the Certificate Authority to recover an accused node, only when it is a Cluster Member in its cluster. This is based on the fact that most types of attacks such as flooding attack, black hole attack and wormhole attack can be detected by any node within the communication range of the attacker.
Only normal nodes are allowed to become CHs and accuse attackers by sending Attack Detection Packets (ADPs) to the CA. Nodes in the Warning List cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions.

Third, When the CA receives an ADP from an accuser [8], the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked. The accuser of the attacker is then listed in the WL because the accuser might actually be making a false accusation.When the CA receives a CRP sent by a CH to request a node to be recovered from the BL, the recovered node is removed from the BL and registered in the WL. At the same time, the CH which sent this packet is also placed in the WL. Since this will cause the CH to lose its credentials, the cluster network will need to be reconstructed. This conservative strategy is designed to cope with collusion attacks where a CH works to falsely recover other malicious nodes listed in the BL. Since all nodes are initially classified as normal nodes upon joining the network, nodes with malevolent intentions also have a chance to become CHs and run false recovery. However, by adopting this conservative strategy, we can minimize the damage caused by collusion attacks. It should be noted that when the CA receives multiple ADPs or CRPs against the same target, the CA follows the procedure again and again when the first packet arrives.
Clustering based certificate revocation scheme provides the following advantages. The first benefit is quick revocation. As compared with the voting-based approaches in [1] [2], our scheme can immediately revoke the certificates of attackers once the first attack is detected because only one ADP is enough for the CA to decide that a node is an attacker. The second advantage is that the scheme incurs a small overhead. In contrast to other methods which require a large amount of messages to be exchanged in order to revoke a certificate, the communication overhead is limited to control traffic. Finally, our scheme resolves the problem of false accusations and achieves high accuracy. By allowing only highly reliable nodes to contribute to the certification process, the chances of false accusations can be lowered and falsely accused nodes can be recovered quickly.

4. RESULT

In the previous method when the number of rounds were increased the energy curve suddenly increases and this leads to the more energy loss (which is shown in red color) of the nodes in the network.But by using the new method, even if the number of rounds increases the energy loss is less when compared to the previous method (which is shown in green color)due to cluster head rotation in the network.



The graph is plotted by taking energy remaining versus number of rounds. One round consists of 5seconds. If we take less number of round then the energy loss will be less but if we take more number of rounds then energy loss will be more.

5. CONCLUSION

The proposed work shows the clustering of certificate revocation to reinforce an idea for MANET scheme which allows the fast certificate revocation process of falsely accused nodes. This scheme can quickly revoke the malicious device certificate, stop the device access to the network and enhances the network security. Our system is better than the all available methods of certificate revocation process. This proposed system achieves high accuracy in releasing legitimate nodes and also it takes short revocation time for normal nodes to revoke the certificate of an attacker.

REFERENCES

[1]. HaiyunLuo, Jiejun Kong, PetrosZerfos, Songwu Lu, Lixia Zhang "Security in MobileAd Hoc Networks: Challenges and Solutions," IEEE WirelessComm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2]. 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.

[3]. J. Clulow and T. Moore, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,"ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

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

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

[6]. M. L.VijjinStephi and Dr. B. Latha" Efficient Method for Secure Transmission from Malicious Node through Certificate Authentication "International Journal of Innovative Research in Computer and Communication Engineering.

[7]. Ambarish and Gowthamani "Secure Cluster Formation and CertificateRevocation Of Adversary Nodes In MobileAdhoc Network" International Journal of Innovative Research in Computer and Communication Engineering.

[8]. Ms.M.Revathy and Mr. S.Saravanakumar"Rationalization Of Certificate Revocation Based On
Cluster For Mobile Ad Hoc Network" International Conference on Science,Engineering and Management.

[9]. Z. Zhang, W. Susilo& R. Raad, "Mobile ad-hoc network key management with certificateless cryptography," in IEEE International Conference on Signal Processing and Communication, 2008, pp. 1-10.

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

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