IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. III (Sep – Oct. 2014), PP 73-78
www.iosrjournals.org

Reduced Overhead Based Approach for Secure Communication in Mobile Ad Hoc Network

Sabeena Salam

Abstract: *Mobile ad hoc network (MANET) is an infrastructureless mobile networks where nodes can freely move and join. MANET has attracted much attention in recent years owing to the increased focus on wireless communication. It is a highly flexible network, vulnerable to various types of security attacks by malicious nodes. Ensuring network security is a major concern in the case of MANET. Certificate revocation play an important role in securing the network by isolating attackers from further participating in network activities. Certification Authority (CA) is responsible for revoking the certificates of attacker nodes. CA maintains two lists, warning list and black list to keep accusing and accused nodes respectively inorder to perform revocation process by considering the first arrived accusation packet. In this paper we focus on the problems of certificate revocation based on first accusation. A threshold based approach is proposed for certificate revocation with better performance, but there is some sort of overhead exist. Inorder to make the communication in MANET more secure we propose a reduced overhead based approach that enhances threshold based approach which introduce an additional list, intermediate list in the CA. The scheme is evaluated and results demonstrate that the proposed scheme is effective and efficient to provide secure communication in mobile ad hoc network.*

I. Introduction

Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks.. A mobile ad hoc network (MANET) is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure.

The network is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes.

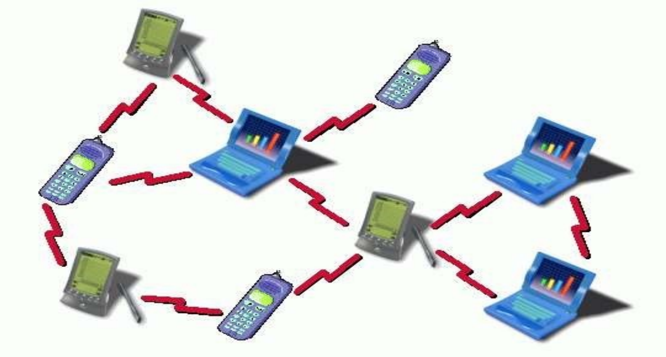

Fig. 1. Mobile Ad Hoc Network

Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources, e.g., military scenarios, rescue operations, data networks, device networks free internet connection sharing and sensor network

Mobile ad hoc network is vulnerable to many kinds of malicious attacks. Attacks on a wireless network can come from all directions and target at any node. Enormous research efforts are made to abate malicious attacks on 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. If any attack is identified, Certificate revocation plays a major task of enlisting and removing the certificates of nodes which have been detected to launch attacks on the neighbourhood. This helps in removing misbehaving nodes from the network and gets blocked from all its activities suddenly. Certificate revocation's basic security problem is aimed at providing secure communications in MANETs. The certificates of the node are signed by the Certificate Authority (CA) of the network, which is a trusted third party that is responsible for issuing and revoking certificates. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. Sometimes malicious nodes can potentially make false accusations so it is difficult for the CA to determine if an accusation is trustable. Therefore, the issue of false accusation must be taken into account in designing certificate revocation mechanisms.

The existing scheme [1], which is based on a clustering approach, able to quickly revoke certificates of accused nodes by considering the first accusation packet. But it has some drawbacks in the case of revoking the certificate. As a solution to this we propose a threshold based approach, which revoke a nodes certificate based on a threshold value. This scheme has better performance, but some sort of overhead exist. Inorder to reduce the overhead and ensure secure communication we propose a reduced overhead based approach. In this scheme CA maintains three lists, warning list, black list and intermediate list to perform certificate revocation.

II. Related Works

Nowadays secure communication in MANET has attracted substantial attention. Many researchers proposed different schemes for this.

In URSA [2] each networking node is required to carry a valid ticket in order to participate in network activities. Ticket serves as a passport for a networking nodes. A ticket is considered valid if it is certified and unexpired. URSA does not use a third-party trust system such as a CA. Only well-behaving nodes are granted access to routing and packet forwarding via valid tickets issued collectively by multiple local nodes. The tickets of the newly joining nodes are also issued by their neighbours. The vote of neighbours having responsibility for revoking tickets of malicious nodes. In URSA, each node performs one- hop monitoring, and exchanges monitoring information with its neighbours which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node. Although URSA is robust for false accusation attacks, there is still a remaining issue in coping with collusion attacks by multiple malicious attackers.

A decentralized certificate revocation scheme [3] which utilizes certificates that are based on the hierarchical trust model. This scheme delegates all key management tasks except the issuing of certificates to the nodes in a MANET; and it does not require any access to online certificate authorities (CAs). All nodes are connected in the network to vote together and they vote with different weights. Each node monitors the behaviour of its neighbours. Node's weight is calculated in terms of reliability and trustworthiness of the node which is derived from its past behaviors that can be the number of accusations against other nodes and that against itself from others. The stronger its reliability, the acquired weight is increased. When the weighted sum from voters against the node exceeds a predefined threshold, the certificate of an accused node is normally revoked. 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 increasing the time needed to revoke the certificate. The scheme mainly uses hash chains for providing data origin and Integrity checks and it does not require time synchronization.

An effective and efficient credential revocation strategy [4] for self-organizing systems. It is the first fully decentralized revocation strategy that works even when nodes are highly mobile. A fully distributed "suicide for the common good" strategy, in which only one accusation completes certificate revocation quickly. As a result, this scheme exhibits good performance in terms of promptness and low operating overhead. In this approach not only the certificate of the accused node but also accuser's certificate is revoked. To remove an attacker from the network, the accusing node has to sacrifice itself. There is degradation in accuracy also. This strategy dramatically reduces both the time required to evict a node and the communication overhead of the certificate revocation procedures. However, owing to its suicide-based strategy, the application of this approach is limited. Also, the scheme does not provide a mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes.

A certificate revocation scheme [5] which can revoke the certification of attackers in a short time with a small amount of operating traffic. It is a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, control messages are managed by a trusted certification authority, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. Any single neighboring node can revoke the certificate of the malicious attacker node. Further, it also deals with the issue of false accusation that enables cluster head (CH) to remove the falsely accused node from the blacklist. The process of handling the certificate revocation is completed in short time. The performance of this scheme is evaluated in terms of promptness of revocation, operating overhead, and accuracy of revocation. By clustering nodes and introducing multi-level node reliability, this scheme can mitigate the improper certificate revocation due to false accusations by malicious users.

This paper [6] built upon the previously proposed scheme, a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. However, owing to a limitation in the scheme's certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This can eventually lead to the case where malicious nodes can no longer be revoked in a timely manner. As a solution a new method is proposed to enhance the effectiveness and efficiency of the scheme by employing a threshold based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs.Effectively improve the performance of certificate revocation. Reduce revocation time and communication overhead.

This paper [7] describes SCAN, a unified network layer security solution for such networks that protects both routing and data forwarding operations through the same reactive approach. SCAN does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to the malicious nodes. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. In essence, SCAN exploits localized collaboration and information cross validation to protect the network in a self -organized manner. It provides complete network layer security solution. And also monitor both routing and packet forwarding activities of each nodes.

It is the notion of certificate-based encryption. In this model [8], a certificate or, more generally, a signature acts not only as a certificate but also as a decryption key. To decrypt a message, a key holder needs both its secret key and an up-to-date certificate from its CA (or a signature from an authorizer). Certificate-based encryption combines the best aspects of identity-based encryption (implicit certification) and public key encryption (no escrow).This demonstrate how certificate-based encryption can be used to construct an efficient PKI requiring less infrastructure than previous proposals. The key idea is that certificate-based encryption enables implicit certification without the problems of IBE, and that implicit certification allows to eliminate third-party queries on certificate status, thereby reducing infrastructural requirements. It also described an incremental CBE scheme that reduces the CA's computation and bandwidth requirements to exceptionally low levels, even though the scheme does not use hash chains or trees like previous PKI proposals.

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. This article [9] focus on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. It identify the security issues related to this problem, discuss the challenges to security design, and review the state of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

In this paper [10] two routing attacks that use non-cooperative network members and disguised packet losses to deplete ad hoc network resources and to reduce ad hoc routing performance is studied. These two routing attacks have not been fully addressed in previous research. It propose the design of "self-healing community" to counter these two attacks. This design exploits the redundancy in deployment which is typical of most ad hoc networks; namely, it counters non-cooperative attacks using the probabilistic presence of nearby cooperative network members. To realize the new paradigm, localized simple schemes to (re)configure self-healing communities in spite of random node mobility is devised. It develop a general analytic model to prove the effectiveness of the design. Then implement the secure ad hoc routing protocols in simulation to verify the cost and overhead incurred by maintaining the communities. This study confirms that the community-based security is a cost-effective strategy to make off-the-shelf ad hoc routing protocols secure.

Table-driven routing algorithms in flat networks have the scalability problem due to the need for global topology updates. To reduce update cost, networks are hierarchically organized. Clustering algorithms organize flat networks into hierarchical networks. One important problem, which has not been adequately addressed so far, is to evaluate how good a clustering algorithm is. In other words, it is useful to know what the desired properties of hierarchical networks are. This paper [11], address this issue by considering the routing update cost, which can be measured by the total routing table size and the variance of cluster size distribution. It provide a set of desired properties of clustering algorithms. Applying these properties to the cluster structure generated by an algorithm, can determine how good a clustering algorithm is. Specifically, discuss how to choose appropriate number of hierarchy levels, number of clusters, and cluster size distribution, such that the topology update cost is minimized. The desired properties obtained from the analysis can be used as guidelines in the design of clustering algorithms for table-driven hierarchical networks. Apply the idea developed in this paper to evaluate three routing algorithms, namely the lowest ID algorithm, the maximum degree algorithm, and the variable degree clustering algorithm. It show how the variable degree clustering algorithm, which takes into account these desired properties, improves routing performance.

III. Proposed System

Our proposed system, reduced overhead based approach has better performance and reduced overhead than the existing cluster based certificate revocation (CCRV) scheme. In CCRV scheme certification revocation is performed based on first accusation from neighbouring nodes. Revocation process is performed by Certification Authority (CA). For this CA has two lists, warning list (WL) and black list (BL).

In CCRV if a legitimate node make accusation against an attacker node, the certification authority keeps the legitimate node in the WL and attacker node in the BL. CA disseminates the revocation message to all nodes in the network for revoking the certificates of nodes in the BL. In the case of false accusation a malicious node make false accusation against legitimate node. Certification authority place malicious node in the WL and legitimate node in the BL. Before revoking the certificate CA disseminates this list to all nodes in the network. If the nodes does not detect any attack from the nodes enlisted in the BL, they sends recovery packet to CA.CA will recover this node from the BL upon receiving the first recovery packet. The problem is that if the accusation is made first time, there is no experience for the nodes to say that whether it is a legitimate or malicious node. Even though the accusation is true, due to lack of experience they may felt that it is a false one. This may badly affect the certificate revocation process resulted in reduction in delivery probability and performance. Inorder to overcome this situation we propose a threshold based approach and the more enhanced scheme reduced overhead based approach.

3.1 Node classification

Nodes are classified into three types based on the behaviour: legitimate, malicious, and attacker nodes.

A **legitimate node** can make secure communications with other nodes. It is able to detect attacks from malicious attacker nodes and accuse them positively. Thus the CA revoke attacker nodes certificates in order to guarantee network security.

A **malicious node** does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. It is able to falsely accuse a legitimate node to revoke its certificate successfully.

An **attacker node** is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.

3.2 Certification Authority

Certification Authority (CA) is a trusted third party responsible for distributing and managing certificates of all nodes. It is responsible for revoking the certificates of the nodes, who has been accused as an attacker node. Inorder to perform the certificate *revocation* process CA maintains some list.

In our proposed threshold based approach CA is in charge of two lists; warning list (WL) and blacklist (BL). The BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node. The CA updates each list according to received accusation packets. Each neighbor is allowed to accuse a given node only once. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network. The enhanced reduced overhead based approach keeps an additional list called intermediate list (IL) along with WL and BL. In this approach, IL holds the accused nodes. In the case of true accusation IL holds attacker nodes and for false accusation it keeps legitimate nodes.

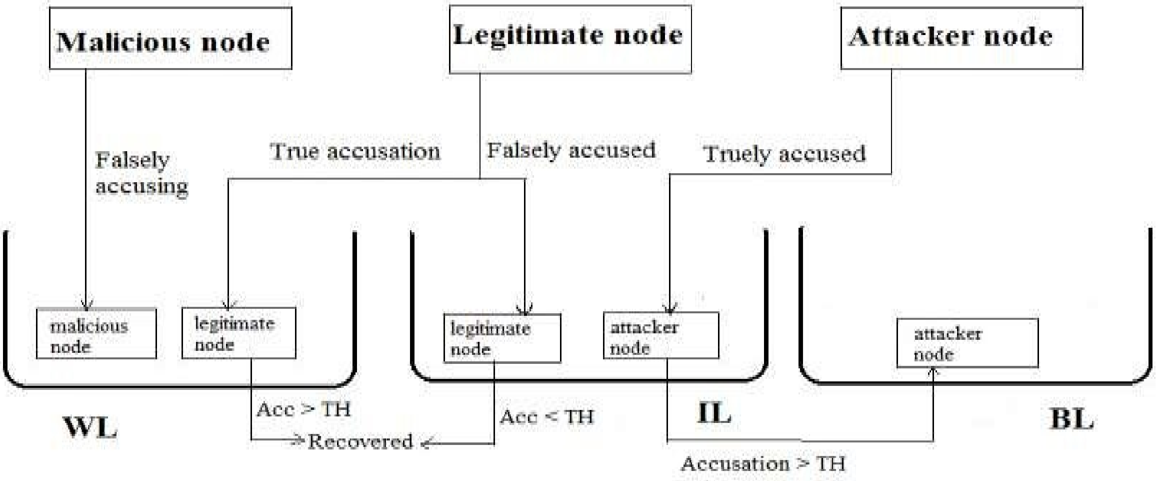

Fig. 2. System Architecture of Reduced Overhead based Approach

IV. Solution Methodology

The immediate solution for the problems in existing system is the threshold based approach. In threshold based approach certificate revocation process is based on a threshold value (TH). A predefined threshold value is set in the CA. Each node can make accusation against another node only once. Once the accusation is made the accusing node is kept in the WL and accused node is kept in the BL. CA continues to receive accusations against the accused node for some time period. Then compare the number of received accusation with the threshold (TH) for each accused node. We consider the accused node as a real attacker if and only if the number of accusation reaches TH. Once the accused node is deemed as an attacker, CA will revoke the certificate of this attacker node and evicted from the network. Then CA will broadcast the list of attacker nodes to all other nodes in the network. So we can finally say that the corresponding accusing node as legitimate node and release it from the WL as well as restore its function as the normal node. Otherwise if the number of accusation fails to reach the TH, which means the case of false accusation. Then the corresponding accusing node, malicious node is detained in the WL itself and the accused node, legitimate node is recovered from the BL to continue its function as normal node for secure communication.

The reduced overhead based approach is an enhanced scheme of threshold based approach which solve the drawbacks of it. In threshold based approach some sort of overhead exist even though the performance is better. Since the certification revocation process and the node releasing process are based on the threshold value and a time period, the accusing and the accused node will not take part in communication process for that time period. In such a situation when a node try to make a communication with its neighbouring node which is already an accusing or accused node, the node cannot complete its communication due to unavailability of nodes and go for another node and so on. Each time when the node check for availability of node for communication, overhead may arise. Thus we enhances this scheme by introducing the reduced overhead based approach.

The main enhancement is made on the list maintained by the CA. Intermediate list (IL) is the new list in CA to keep the accused node, either the accusation is true or false. So the IL contains both attacker node and legitimate node. The accusing node is kept in the WL itself. The CA will send the IL to other nodes and update the list each time when the accusation is made. A threshold is set in the CA and the number of accusation is compared with the TH just like the earlier approach. When a node try to make a communication there is an unavailability of nodes in the threshold based approach, results in overhead. But in this case if the node cannot make a proper route then it will try with the nodes in the IL to make the route. Eventhough IL contains both attacker and legitimate node, overhead for checking the availability of nodes will reduce. At the same time if the nodes in the IL is found to be an attacker, it will moved on to the BL and removed from the network by revoking the certificate by the CA. By keeping the accused node in the IL and allowing them to participate in communication process, the proposed system handles the false accusation also and proves that it is better than existing one.

V. Conclusion And Future Work

MANET allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Ensuring secure communication between nodes is the significance of this paper. For this we propose two approaches, where one enhances the other. The proposed one solves the drawbacks of existing system. Threshold based approach, based on a threshold value for certificate revocation can be considered as an immediate solution for the existing system [1].Guaranteeing better performance and delivery probability is the main feature of this scheme, but some sort of overhead exist. For making the communication secure with reduced overhead and high delivery probability we enhances the threshold based approach and introduces reduced overhead based approach. This approach maintains an additional list called intermediate list (IL) in the certification authority.Due to the importance of wireless communication, researchers explore the field of MANET. By applying new approaches the proposed system can be improved.

References

[1] Wei Liu, Hiroki Nishiyama, Nirwan Ansari, Jie Yang, and Nei Kato, "Cluster-BasedCertificate Revocation with Vindication Capability for Mobile Ad Hoc Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, Feb. 2013.

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

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

[4] 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.

[5] 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.

[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] 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.

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

[9] 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.

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

[11] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks," IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489, Dec. 2007.