IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 06, Issue 09 (Sep 2016), ||V1|| PP 45-48

Enhancing Security of MANETs using Certificate Revocation

Khan Firdous Jahan Mohd Harun[1], Sunil B. Wankhade[2]
[1,2](Department of Computer Engineering, Rajiv Gandhi Institute of Technology/ Mumbai University, India)

Abstract: - MANET (Mobile Ad hoc Network) is an autonomous, robust and scalable system of mobile nodes that can communicate via wireless links with no rigid infrastructure. Owing to the independent and dynamic nature of mobile nodes, the topology of MANET changes frequently and is prone to various kinds of attacks. To eradicate the security threats, an efficient certificate revocation scheme has been adopted to attain a secure communication. Conventional schemes in MANETs aim to achieve greater security by electing a Cluster Head (CH) for each and every cluster which governs the entire network. In our paper, we propose a trust based system which nominates a CH based on the basis of higher trust value computation and Enhanced Certificate Revocation scheme (ECR) for discarding the authorization of the misbehaving nodes. This paper achieves greater reliability, avoids false accusation, quicker revocation time, efficient trust value computation, and also reduces the communication and computational costs compared to the existing mechanisms.

Keywords: - *Authorization, Certificate revocation, Cluster head, MANET, Trust value.*

I. INTRODUCTION

A MANET is an autonomous system of mobile nodes, a type of a wireless network in which the mobile nodes dynamically forms a network to exchange information without utilizing any pre-existing fixed network infrastructure. A MANET consist of a number of mobile nodes to carry out its basic functions like packet forwarding, service discovery and routing without the help of an established infrastructure. Each and every node of an ad hoc network depends on another node for forwarding a packet to its destination, because of the limited range of wireless transmission of each mobile node. MANETs are characterized by unreliable communications in which the topology of network changes dynamically. Also each node is limited by its computational power, bandwidth and battery. Due to lack of infrastructure and the self-configuring nature of networks, the nodes in the MANETs act both as a host and as a router. As MANETs are highly dynamic and self- developing, security is the major factor. There is a growing need to monitor the behavior of the connected node in all functional aspects. Trust metric is used to track every functional aspect of the misbehaving node and it is needed because, multiple attacks may be launched by the malicious nodes. The trust evidence collection mechanism collects plenty of information by which a neighboring node can be judged for its sincerity in participation of routing, data forwarding etc. To address routing problems in MANET, environment hierarchies among the nodes can be built, such that the network topology can be abstracted. This process is commonly referred to as clustering and the substructures that are collapsed in higher levels are called clusters [1]. Clustering is one of the promising approaches, since the network performance is degraded as the network size grows in MANET.

II. RELATED WORK

Certificate revocation is a method used to provide security to MANET, which isolate the attackers from participating in network activities further. These certificates are issued as well as revoked by the Certificate Authority (CA) which is a trusted third party. Certificate revocation means invalidating the attacker's certificate which is essential in maintaining the network secured. Sometimes malicious node will try to remove legitimate nodes from the network by falsely accusing them as attackers. Therefore, the issue of false accusation should be taken into account in designing certificate revocation mechanisms [2].

The existing approaches for certificate revocation are classified into two categories: Voting-based mechanism and Non-voting-based mechanism [3]. URSA [4] proposed by H. Luo et al. uses a voting based mechanism to evict nodes. The certificates of newly joined nodes are issued by their neighboring nodes. The certificate of an attacker node is revoked on the basis of votes from its neighbors. The scheme proposed by G.Arboit et al. [1] allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and thus each node monitors the behavior of its neighbors. The main difference from URSA is that nodes vote with variable weights. J. Clulow et al. [5] proposed a fully distributed "suicide for the common good" strategy, where certificate revocation can be quickly done by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. K. Park et al. [6] proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and

accused node in the warning list and black list, respectively. The certificate of the malicious attacker node can be revoked by any single neighboring node.

III. PROPOSED SYSTEM

3.1 Cluster Formation

The mobile nodes in MANET are collected in groups to form individual clusters. The cluster formation process is done using grid based approach [7] to form a single-hop cluster, in which each and every node exclusively belongs to a single cluster. According to the transmission range of each node, the network is partitioned into grids. The clusters are formed by calculating the relative distance of a node to each of its neighbors using equation (1):

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad \ldots\ldots (1)$$

Where D: Distance between a node and its neighbour
(x_1, y_1): Co-ordinates of the node
(x_2, y_2): Co-ordinates of its neighbour

3.2 Trust Calculation

Trust is an annotation of human behaviour. The definition of trust is differs with respect to different context. We take the definition made by T. Grandison in [8]: "Trust is the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context". Trustor (or "trustor node") refers to the node that implements the trust evaluation. Trustee (or "trustee node") refers to the node that is evaluated. Another term mentioned in the following text is "third node". Such third node is the node that a trustor expects who can provide honest recommendation on a specific trustee.

Trust calculation and its management is a tough task in MANETs due to the unpredictable nature of nodes and computational complexity constraints in the network. In our trust model, we analyse two types of trust between a trustor node and a trustee node and they are: direct trust and recommendation trust (indirect trust). Trust value computation is performed for every interval and also Trust value is updated. To build a trusted environment, a node with larger Trust value is declared as the CH for each cluster. Unless the trust calculation is complete, there is no cluster head. Direct trust is a kind of credential obtained by a trustor node through its direct experience upon the trustee node. Recommendation trust is the credential obtained by a trustor node from a third node or nodes' recommendation on the trustee node.

3.2.1 Direct Trust Calculation

Let us calculate direct trust of node B by the node A as shown in figure 3.2.1. First node A sends some number of packets to the node B. After getting all the messages from node A, node B sends the acknowledgement to the node A. Now we will calculate direct trust using following algorithm:

Trust Parameters
f = Number of packets that are forwarded
d = Number of packets that are dropped
m = Number of packets that are misrouted
Step 1: Collect data for f, d, m.
Step 2: Calculate total number of packets which are dropped and misrouted. i.e. (d+m)
Step 3: Calculate total number of packets which are successfully reached to node B. i.e. {f - (d+m)}
Step 4: Calculate the Direct Trust by using the formula
Direct Trust (T_D) = {f - (d+m)}/f

3.2.2 Indirect (Recommendation) Trust Calculation

In case when a trustor node does not have enough direct experience on a trustee node, the trustor node may query a third node for recommendation. Let us suppose the third node has some trust value V_i on the trustee node based on its own evaluation. The recommendation trust T_R value for the trustor node is calculated using equation (2) as:

$$T_R = T_D * V_i \quad \ldots\ldots (2)$$

T_D is the direct trust value that the trustor node has on the third node. Multiplication of the values expresses that the recommendation value is affected by the value how much the trustor node trusts the third node. To ensure that the recommendation is more reasonable, a trustor node may query several other third nodes for recommendation. In such cases, the recommendation trust value is calculated using equation (3) as:

$$T_R = \frac{1}{n} \sum_{i=1}^{n} (T_D * V_i) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

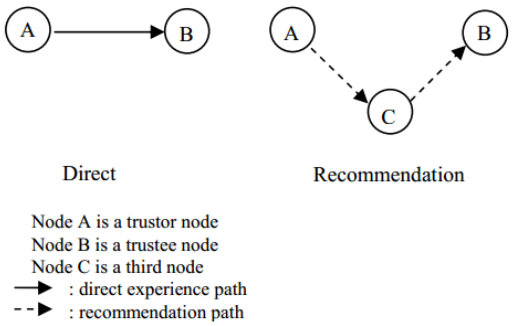
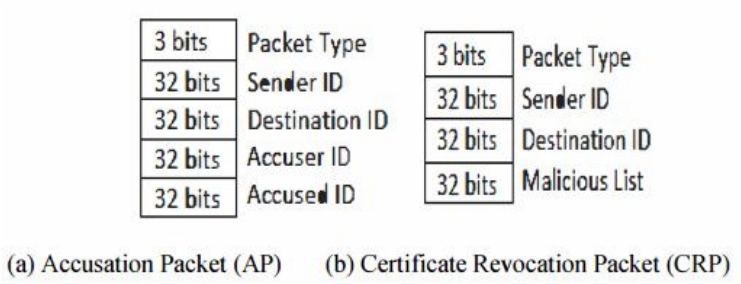


Fig. 3.2.1: Direct and Indirect Trust Calculation

3.3 Enhanced Certificate Revocation scheme (ECR)

The prime responsibility of CA [9] is to authenticate the nodes which enter the network and revoke the certificate of the malicious nodes. CA uses Public Key Encryption algorithm to distribute the certificates to the nodes.



(a) Accusation Packet (AP) (b) Certificate Revocation Packet (CRP)

Fig.3.3.1: Control packets

In our scheme, the CH manages the Warn List (WL) and Black List (BL). Every node knows the behaviour of their 1-hop neighbours. An accuser claims that the node is malicious if it fails in relaying the packet to the destination and it sends Accusation Packet (AP) to the CH. AP as shown in Figure 3.3.1(a), encompasses Accuser (AC) ID and Accused (ACD) ID. Now, CH analyzes the reported nodes. If the accuser's Trust value is greater, then CH checks for the accused in the WL. The accused node which is in the WL indicates the second accusation and finally, CH removes it from the WL and adds it into the BL. At the same time, if the accused node is not in the WL called as first accusation, CH inserts into the BL. If the accuser's Trust value is smaller, then both the nodes are pushed into the WL. After a period of time, CH evaluates the above process again, updates the lists and transfers Certificate Revocation Packet (CRP) to the CA for revocation. The CRP as depicted in Figure 3.3.1 (b) consists of the malicious nodes in the cluster.

Compared to the existing mechanisms, our proposed ECR yields a competent misbehaving node detection scheme which achieves the following:

i) It scrutinizes the exact malicious node without any fake accusation in the cluster with the two levels of accusation process.

ii) Our Scheme requires AP and MP transferred across the accuser, CH and CA, which is sufficient to detect the improper nodes and thus, it reduces the communication and computational complexity.

iii) It minimizes the period of revocation.

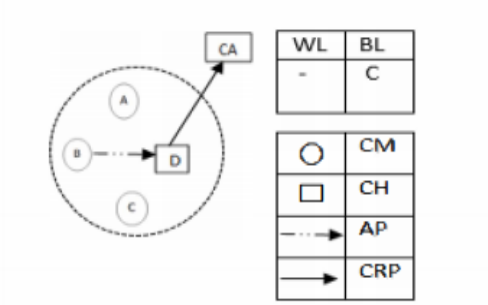


Fig.3.3.2: Revoking a node's certificate (First accusation)

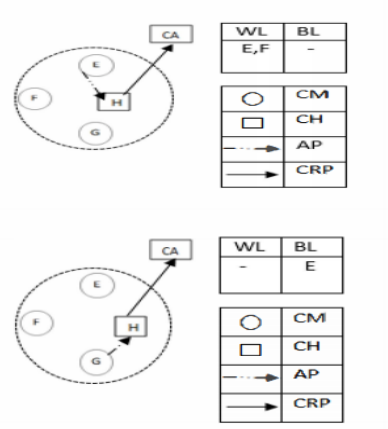


Fig.3.3.3: Dealing with second accusation

Applying the proposed ECR algorithm in MANET for detecting the malicious nodes as depicted below. Here, we consider nodes A, B, C and D. Node B accuses C and sends AP to the D (CH). Now CH identifies it as fist accusation, so the node C is added into the BL as shown in Figure 3.3.2. The accuser E notifies that F is malicious, but E holds a lesser Trust value. So, CH pushes nodes E and F into the warning list and waits for the second accusation as represented in Figure 3.3.3.

IV. CONCLUSION

In MANETs, security is the paramount importance due to the dynamic, infrastructure less and unpredictable nature of the nodes in the network. Our proposed system aims to identify the malicious node with the trust value and revoke the authorization using ECR. This proposed scheme will achieve efficient detection of misbehaving nodes which will lead to minimized revocation time and will solve the false accusation problem without affecting the freedom of the accuser. Our simulation results will be indicating that our novel mechanism provides a greater outcome compared to the traditional ones.

We simulate the ETBCRM (Enhanced Trust based Certificate Revocation of Malicious nodes in MANETs) using Network Simulator-2 (NS-2).The comparative results will show the performance analysis using direct trust, indirect trust method and their combination. We will use AODV routing protocol. Performance metrics that can be used are delay, throughput, packet delivery ratio (PDR), and revocation time.

REFERENCES

[1] 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.

[2] E.K Neena, C. Balakrishnan "Efficient in Revoking Certificates of Malicious Nodes in MANET", *International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-1, Issue-9,* Nov 2013.

[3] M.Kannan, E.Dinesh, Improving QOS in Cluster Based Certificate Revocation for Mobile Ad Hoc Network, *International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.*

[4] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks", *IEEE/ ACMTrans. Networking, vol. 12, no. 6,* pp.1049-1063, Oct. 2004.

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

[6] K. Park, H. Nishiyama, N. Ansari, and N. Kato, *"*Certificate revocation to cope with false accusations in mobile ad hoc networks", in *Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring,* Taipei, Taiwan, May 16-19, 2010.

[7] Ferdous, Raihana, Vallipuram Muthukkumarasamy, and Elankayer Sithirasenan. "Trust-Based Cluster Head Selection Algorithm for Mobile AdHoc Networks." *(TrustCom), 2011 IEEE.*

[8] Grandison, T.W.A., *"Trust Management for Internet Applications"*, in Department of Computing. 2003, University of London: London, British. p. 252.

[9] Y. Dong, Ai-Fen Sui, S.M. Yiu, Victor O.K. Li, Lucas C.K. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks", *computer communications* 30.11 (2007): 2442-2452.