ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Proposing Trust Count Based Validation Method to Lessen Internal Attacks in Mobile Adhoc Networks

D.SRINIVASA RAO
Department of Computer Science and Engineering
RSR Rungta College of Engineering & Technology
Bhilai, Chattisgarh, India
sridas712@gmail.com

MOHD. SHAJID ANSARI
Department of Computer Science and Engineering
GD Rungta College of Engineering & Technology
Bhilai, Chattisgarh, India
shajid_avis@yahoo.co.in

***Abstract*— Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. The wireless nature and inherent features of mobile ad hoc networks make them exposed to a wide variety of attacks. In an internal attack, the attacker gains the normal access to the network and takes part in the network activities, either by some malicious imitation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. In this paper, we develop a cluster based validation methods to lessen internal attacks. The entire network is divided into hierarchical group of clusters, each cluster having a fully trusted cluster head. Each node holds a certificate issued by an offline certificate authority (CA). The Trust Count (TC) for each of the nodes can be estimated periodically for every trust evaluation interval (TEI), based on their access policy (AP). The certificate of a node is renewed or rejected by the cluster head, based on its trust counter value. By simulation results, we show that our proposed technique provides better packet delivery ratio and resilience against node capture.**

Keywords- Node Capture Attacks, Clustering, Trust Count, Access Policy

I. INTRODUCTION

An autonomous system of mobile hosts connected by wireless links, often called *Mobile Ad hoc NETworks* (MANETs) . Mobile ad hoc network has been a challenging research area for the last few years because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc.. The eventual goal of designing a MANET network is to make available a self-protecting, "dynamic, self-forming, and self-healing network" for the dynamic and non-predictive topological network [1]. According to the positions and transmission range, every node in MANET acts as a router and tends to move arbitrary and dynamically connected to form network. The topology of the ad hoc network is mainly interdependent on two factors; the transmission power of the nodes and the Mobile Node location, which are never fixed along the time period. [2] Ad hoc networks excel from the traditional networks in many factors like; easy and swift installation and trouble free reconfiguration, which transform them into circumstances, where deployment of a network infrastructure is too expensive or too susceptible [5].

MANETs have applicability in several areas like in military applications where cadets relaying important data of situational awareness on the battleground, in corporate houses where employees or associates sharing information inside the company premises or in a meeting hall; attendees using wireless gadgets participating in an interactive conference, critical mission programmer for relief matters in any disaster events like large scale mishaps like war or terrorist attacks, natural disasters and all. They are also been used up in private area and home networking, "location based" services, sensor networks and many more adds up as services based on MANET [4]. The three major drawback related to the quality of service in MANET are bandwidth limitations, vibrant and non-predictive topology and the limited processing and minimum storage of mobile nodes [3] The wireless nature and inherent features of mobile ad hoc networks make them vulnerable to a wide variety

of attacks. The attacks on MANETs can be classified into various criteria as shown below [6, 7, and 8];

A. External Vs. Internal Attacks

External attacks are attacks launched by adversaries who are not initially authorized to participate in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers. More severe attacks in the ad hoc networks might come from the second source of attacks, which is the internal attack. Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in the ad hoc networks with the compromised internal nodes because communication keys used by these nodes might be stolen and passed to the other colluding attackers. On the other hand, nodes will be classified as misbehaving if they are authorized to access the system resources, but fail to use these resources in a way they should be. Internal nodes might misbehave to save their limited resources, such as the battery powers, the processing capabilities, and the communication bandwidth. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

B. Node Capture Attacks

Passive, active, and physical attacks combined together results in node capture attacks. The attacker will collect data
about the network by eavesdropping on message exchanges ,either restricted to individual attacker device or during the network with the aid of number of attacker devices deployed throughout the network ,in order to initialize or set up an attack.
The attacker can extract data about the network operation and state, along with successfully learning about the network structure and function, although the message payloads are encrypted. The attacker can capture a node from the network ultimately acquiring all the cryptographic material stored in it .Also the captured nodes can be reprogrammed by the Attacker and redeployed in the network in order to carry out malicious activities. Solution to node capture attacks has to meet the following requirements:

- To detect the node capture as early as possible.
- To have a low rate of false positives—nodes which are believed to be captured and thus subject to a revocation process, but which were not actually taken by the adversary.
- To introduce a small overhead.[10]

In our previous work [9], we have developed a combined solution for routing and MAC layer attacks. Our approach, make use of three techniques simultaneously which consists of a cumulative frequency based detection technique for detecting MAC layers attacks, data forwarding behavior based detection technique for detecting packet drops and MAC based authentication technique for packet modification.
Our combined solution presents a reputation value for detecting the malicious nodes and isolates them from further network participation till its revocation. In this approach, the technique to mitigate node capture attack is not taken into account. As an extension to the previous work, we develop a cluster based authentication technique to mitigate the internal attacks or node capture attacks. The authentication is performed by the cluster head by checking the trust count value of its members.

II. RELATED WORKS

Pushpita Chatterjee [10] proposed a new approach based on trust based self-organizing clustering algorithm. They have used the trust evaluation mechanism depending on the behavior of a node towards proper functionality of the network. The trust evaluation model gives a secure solution as well as stimulates the cooperation between the nodes of the network. The originality of their work consists of combining different metrics for quantifying trust and the use of DS theory in order to predict the trust of mobile node more accurately.

Wenbo He et al [11] proposed a SMOCK scheme, which adopts the combinatorial design of cryptographic keys to achieve lightweight key management. They further extend the idea of SMOCK to other applications, such as broadcast
authentication. Based on the SMOCK idea, they design a combinatorial hash-chain sharing scheme: A hash chain pool HC is constructed for the whole network and nodes store the commitment information for all of the hash chains in HC. All of the hash chains have the same releasing schedule, which is

guaranteed by loosely time synchronization. Message signing and verification use all the hash chains associated with the senders' identity.

Saju P John et al [12] proposed enhanced scalable method of cryptographic key management (SMOCK). They present a clustering based technique to reduce the two drawbacks; to over dependent on centralized server and increase in key-pair when node increases (proportionally less compared to traditional approach) which SMOCK posses. The clustering technique used select a CH, is an adaptive weight clustering method. The CH is stored with public keys of all its member nodes. The communication of nodes between two different clusters happens through their CH. Their method also discusses about the effects of node mobility between clusters.

Node ID	Node Status	
Neighbor ID	Neighbor Status	Link Status
…	…	…
Adjacent Cluster ID		

III. CLUSTERING

Division of the network into different virtual groups, based on rules in order to discriminate the nodes allocated to different sub-networks is called clustering. Each group has a group leader and cluster is headed by the cluster head. Specifically, one of the nodes in the clusters is head .A set of clusters form a group and each group is headed by a group leader. The nodes contained in a cluster are physical neighbors, and they use contributory key agreement, and they further contribute their shares in arriving at the group key. When there is change in membership, the neighbor node initiates the rekeying operation, thus reducing the burden on the cluster head .The group leader selects a random key to be utilized for encrypting messages exchanged connecting the cluster heads and the network head. It forwards the key to the group leader that is used for communication among the group leaders.

A. Classification

• **DS-based clustering**
– Route maintenance actions to the nodes from the dominating set
• **Mobility-aware clustering**
– Cluster based on the mobility behavior of the mobile nodes
• **Energy-efficient clustering**
– Consider the energy available at the nodes
• **Load-balancing clustering**
– Limit the number of nodes in a cluster in order to distribute the workload
• **Combined-metrics clustering**
– Considers multiple metrics
• **Low-maintenance clustering**
– Perform clustering for upper-layers and reduce the maintenance cost

B. Cluster Formation

Nodes periodically exchange HELLO packets to

- maintain a neighbor table
  neighbor status (C_HEAD, C_MEMBER, C_UNDECIDED)
  link status (uni-directional link, bi-directional link)
- maintain a 2-hop-topology link state table

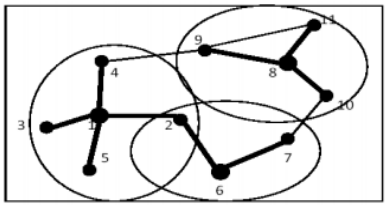

Figure 1: Cluster Structure

In figure 1 node 1 is cluster head for the cluster containing nodes 2, 3, 4 and 5, node 6 and 8 are cluster- heads for two other heads for two other clusters.

C. Algorithms for Node Registration

```
while(!myself_clustered){
        transmit(clus_find);
     waitforresponses();
        parse_responses();
        choose_suitable_cluster();
        if(suitable_cluster_exists) {
                send(clus_join_request);
                waitfor(clus_join_reply);
                if(clus_join_accept)
updatemyclus();
                else formownclus();
        }
    else formownclus();
}
```

IV. SYSTEM DESIGN

Every node within a cluster has an access policy (AP) which consists of the following access permission.

Read (R) ; Modify (M); Forward (F); Process (P) Depending on access policy nodes can be in three levels .It can be lower level (LL), Middle level (ML), and Higher level (HL). The LL node posses only F permission .The ML node posses both F and R permissions. The HL node posses all the permissions R, M, F and P. The existence of an offline certificate authority (CA) is assumed. Initially it issues a certificate signed by its public key to all the nodes which consists of the access policy AP for each node along with a certificate expiration time (CET). Each node involves in exchanging its AP with other nodes.

Before expiration, the certificate of a node must be renewed. After the cluster heads are selected, they broadcast a CH_CERT_REQ message to CA for a cluster head certificate request. On receiving the CH_CERT_REQ message from each cluster, the CA sends issues a cluster head certificate CH_CERT signed by its public key to all the cluster heads which consists of the cluster id and cluster head certificate expiration time (CHCET) such that CHCET > CET .We assume initial trust counter (TC) for all the nodes with a minimum threshold value (TC_{th}). The TC for all the nodes can be estimated periodically for every trust evaluation interval (TEI).

A. Certification

Keys are generated and exchanged through an existing relation between CA and each node. Each node must request a certificate from CA, before entering the ad hoc networks. Each node receives exactly one certificate, after securely authenticating their identity to CA. The node A receives certificate from C>A as follows, CA A: cert *A* = [IP *A* , K *Pu* , t, e, AP] K Pr The certificate authority contains the IP address of A the public key of A, a timestamp t of when the certificate was created, expiration time e and access policy AP. These variables are concatenated and signed by CA. All nodes must maintain fresh certificates, with CA. During the exchange of routing messages, nodes use these certificates to authenticate themselves to other nodes.

B. Hop-By-Hop Authentication

The method by which source verifies that intended destination was reached is by end to end authentication. Source node, A send data to particular destination that will be received by intermediate node.
A→Transmit: [DP, IP *x* , cert *A* , N *A* , t, AP] K Pr The DP includes a packet identifier ("DP"), the IP address of the destination (IP *x*), A's certificate (cert *A*), an once N *A* , the current time t and access policy(AP), all signed with A's private key. To allow for simplicity of nonce recycling, the nonce and timestamp are used in concurrence with each other. For the purpose of avoiding recycling within probable clock skew between receivers, it is made sufficiently large. Other nodes stores the nonce viewed by them lastly for a particular node along with its timestamp.

If nonce which has a later timestamp re-appears in valid packet, nonce is assumed to be wrapped around, and hence accepted. When a node receives DP message, its uses A's public key extracted from A's certificate, to authenticate the signature and to validate that A's certificate has not expired. The receiving node checks (N *A* , IP *A*), tuple to verify that processing of DP is not done previously. Nodes which have seen their tuple already don't forward messages. Else, the node proceeds by signing the contents of the messages, appends its own certificate, and sends the message to its next hop. Alterations of data or integrity attacks are prevented by signature. Let B be a neighbor that has received the DP from A, which it subsequently forward.
B→Transmit:[[DP, IP *x* ,cert *A* , N *A* ,t, AP] K Pr] K Pr *B* , Cert B Upon receiving the DP, B's neighbor C validates the signature with the given certificate C, and then removes B's certificate & signature, records B as its predecessor, signs the content of the message originally sent by A, appends its own certificate and forward the message. C then retransmits the DP.
C→Transmit:[[DP,IP *x* ,cert *A* ,N *A* ,t,AP]K Pr]K Pr*C* ,CertC. Each node along the path repeats these steps of validating the previous node's signature, removing the previous node's certificate and signature, recording the previous node's IP address, signing the original contents of the message, appending its own certificate and forwards the message. [K Pr - Private Key of node A ; K *Pu* - Public key of node A t - Time stamp ; e – Expiration time ; IP *x* -IP address of the node ; Cert *A* - Certificate belonging to node A]

C. Hop-By-Hop Authentication: Consider two nodes A and B. Each node will have time stamps TS *s* , (packet sending time), TS *r* (packet receiving time).

Case 1:
If A is in LL, the following two tests are conducted
Test 1: (For violation of confidentiality)
If (TSr - TSs)> TS *th* (where TS *th* is a threshold value)
Then TC = TC -1

Test 2: (For violation of integrity)

If (sign is not matching)
Then TC = TC – 1

Case 2:
If A is in ML, then the confidentiality test (Test-1) is conducted. The TC_i be the trust counter of node ni estimated by all the nodes in TE_{lk}. All the member nodes send TC_i to its cluster head CH.
If the CH detects that TC_i is less than TC_{th}, it puts the ni in his local CRL (Certificate Revocation List). The node ni sends its renewal request to its cluster head CH.
CH checks whether ni is in the CRL. If it is found, its request is rejected. Otherwise, it sends a certificate renewal reply to ni with its signature.

V. SIMULATION RESULTS

A. Simulation Model and Parameters

We use Network Simulator (NS2) to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We have kept the number of nodes as 100. The number of attackers is varied from 5 to 25. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1.

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet size	512
Speed	10m/s
Misbehaving Nodes	5,10,15,20,25

Table 1: Simulation Settings

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Resilience against Node Capture: It is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes.

Average End-to-End Delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.The simulation results are presented in the next section.

We compare our CBAT scheme with the trust based clustering and secure routing (TBCSR) scheme [13] in presence of malicious node environment.

C. Results

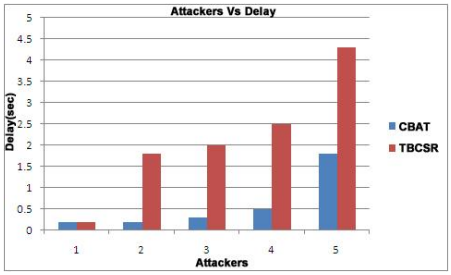

Figure 1: Attackers Vs Delay

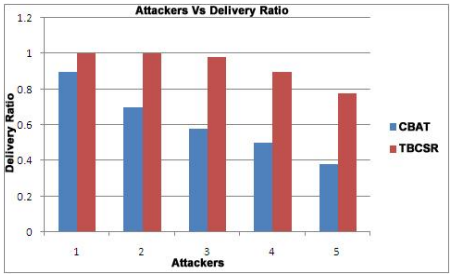

Figure 2: Attackers Vs Delivery Ratio

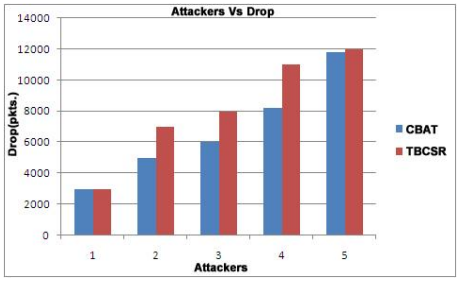

Figure 3: Attackers Vs Drop

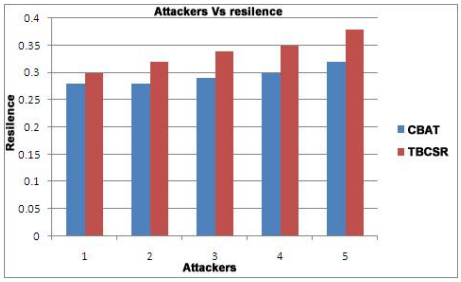

Figure 4: Attackers Vs Resilence

Figure 1 shows the results of average end-to-end delay for the misbehaving nodes for both the schemes. From the results, we can see that CBAT scheme has significantly lower delay than the TBCSR scheme, because of its hierarchical structure of authentication.

Figures 2 and 4 show the results of average packet delivery ratio and resilience against node capture, respectively, for the increasing misbehaving nodes. Clearly the CBAT scheme outperforms the TBCSR scheme by achieving more delivery ratio and resilience, since it has more security features for node compromise attacks.

Figure 3 shows the results of packets drop for the schemes when the number of attackers is increased. From the results, we can see that CBAT scheme has

significantly less packet drops than the TBCSR scheme, since the attackers are immediately isolated.

VI. CONCLUSION

In this paper, we have developed a cluster based validation methods to lessen internal attacks in MANET. In this technique, the entire network is divided into hierarchical group of clusters, each cluster having a fully trusted cluster head. Each node holds a certificate issued by an offline certificate authority (CA). Initially CA issues a certificate signed by its public key to all the nodes which consists of the access policy (AP) for each node along with a certificate expiration time (CET). Before expiration, the certificate of a node must be renewed. The Trust Count (TC) for each of the nodes can be estimated periodically for every trust evaluation interval (TEI), based on their access policy (AP). When a node send renewal request to its cluster head (CH), CH verifies whether the node is in its CRL, if so, the request is rejected. Otherwise it sends a certificate renewal reply to nodes with its signature. By simulation results, we have shown that our proposed technique provides better packet delivery ratio and resilience against node capture.

REFERENCES

[1] Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine, "An Ontological Approach to Secure MANET Management", In Proceedings of the 2008 Third International Conference on Availability, Reliability and Security, pp. 787-794 , 2008.

[2] Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain, "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol", European Journal of Scientific Research, .32(4), pp. 444-454, 2009.

[3] M.Uma and Dr.G.Padmavathi, "A Comparative Study And Performance Evaluation Of Reactive Quality Of Service Routing Protocols In Mobile Adhoc Networks", Journal of Theoretical and Applied Information Technology, 6(2), pp. 223-239, 2009.

[4] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.), Springer, 2006.

[5] Yu Huang, Beihong Jin, Jiannong Cao, Guangzhong Sun and Yulin Feng, "A Selective Push Algorithm for Cooperative Cache Consistency Maintenance over MANETs", EUC, pp. 650-660, 2007.

[6] N.Shanthi, L.Ganeshen and K.Ramar," Study Of Different Attacks On Multicast Mobile Adhoc Network", Journal of Theoretical and Applied Information Technology, 9(2), pp. 45-51, 2009.

[7] Yang Xiao, Xuemin Shen and Dingzhu Du, "Wireless Network Security", Springer, ISBN-10 0- 387-28040-5, 2007.

[8] S. A. Razak, S. M. Furnell and P. J. Brooke, "Attacks Against Mobile Ad Hoc Networks Routing Protocols.", In Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET '04)

June 28-29, World Scientific and Engineering Academy and Society (WSEAS), USA., pp. 147-152, 2004.

[9] R. Murugan and A. Shanmugam, "A Combined solution for Routing and Medium Access Control Layer Attacks in Mobile Ad Hoc Networks", Journal of Computer Science, 6(12), pp.1416-1423, 2010.

[10] Pushpita Chatterjee, "Trust Based Clustering And Secure Routing Scheme For Mobile Ad Hoc Networks", International Journal of Computer Networks and Communication, 1(2), pp. 84-97, 2009.

[11] Wenbo He, Ying Huang, Ravishankar Sathyam, Klara Nahrstedt, and Whay C. Lee, "SMOCK: A Scalable Method of Cryptographic Key Management for Mission-Critical Wireless Ad-Hoc Networks", IEEE Transactions on Information Forensics and Security, 4(1), pp. 140- 150, March 2009.

[12] Saju P John and Philip Samuel, "A Distributed Hierarchical Key Management Scheme for Mobile Ad hoc Networks", International Conference on Information, Networking and Automation, Oct. 2010