Dynamic Security Scheme for MANET

A. Shajin Nargunam, N.I. College of Engineering, Thuckalay, Tamil Nadu, India; E-mail: ashajins@yahoo.com
M. P. Sebastian, Naitonal Institute of Technology Calicut, India; E-mail: sebasmp@nitc.ac.in

ABSTRACT

Secured communication in mobile ad hoc network is a crucial issue due to dynamic nature of the network topology. Due to lack of centralized control, issuing certificates from a centralized certification agent is not possible in ad hoc network. The major problem in providing security services in such infrastructure less networks is how to manage the cryptographic keys that are needed In MANET any node may compromise the packet routing functionality by disrupting the route discovery process.. These unique characteristics of mobile ad hoc networks causes a number of nontrivial challenges to security design such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic topology. These challenges make a cause for building multi-fence security solution that achieves both extensive protection and desirable network performance. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. We propose a novel cluster based security scheme to protect mobile ad hoc network link layer and network layer operations of delivering packet over the multihop wireless channel. The dynamic network topology can be managed efficiently by the proposed cluster based architecture. A well-behaving node becomes a cluster member after the initial trust verification process. The membership validity period of a node depends on how long it has stayed and behaved well. Non overlapping clusters are created using the dynamic cluster creation algorithm. The cluster construction is fully distributed so efficiency is not degraded by node mobility.

Keywords: Cluster, Denial of Service, MANET Security.

I. INTRODUCTION

In ad hoc network every node is self-organized and each node can communicate directly with other nodes in the network through broadcast radio transmissions, i.e., transmissions that reach all the terminals within the transmission power range. However, due to radio range limitations, physical broadcasting does not cover all nodes in the network. In multi-hop scenario, packets are relayed by intermediate nodes to reach the destination. Applications of mobile ad hoc networks can range from military field communications, where networks must be deployed immediately without the support of base stations and fixed network infrastructures, to inter-vehicle communications, designed for both traffic safety enhancement and entertainment purposes. The ultimate goal of the security solutions for mobile ad hoc network is to provide security services, such as authentication, confidentially, integrity, anonymity and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection. We seek to protect the network connectivity between mobile nodes over potentially multihop wireless channel, which is the basics to support any network security services. Security never comes for free. When more security features are introduced into the network, it increases the computation, communication and management overhead. In fact, both magnitude of security strength and network performance are equally important, and achieving a good trade-off between two extremes is the basic challenge in security design for mobile ad hoc network. Fully distributed cluster based security scheme provides secure peer to peer communication without compromising the network performance.

The rest of the paper is organized as follows. Section II discusses a review of related work. Section III describes the security issues in MANET. Section IV discusses the fully distributed cluster based security topology. Section V describes the dynamic clustering algorithm. Section VI discusses the performance issues. Section VIII concludes the paper.

II. RELATED WORK

The traditional key distribution protocols rely on infrastructure with online trusted third parties. When the users want to establish secure communication among them, each one of them has to obtain a new session key from the key distribution center. There is also number of schemes extending this approach to ad hoc network. [5] Present a hierarchical framework and key distribution algorithms for dynamic environment, with a focus on how keys and trust relationships are transferred when users move between so-called "areas" in the hierarchy. When distance vector routing protocols such as AODV [4] are used, the attacker may advertise a route with smaller distance metric than its actual distance to the destination or advertise a routing update with a larger sequence number and invalidate all the routing updates from other nodes.

Broadcast can be limited by adjusting the TTL value on each transmission is disused in [1]. The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. The first key pre-distribution scheme is given in [6].

Carmen et al. analyzed a wide variety of approaches for key distribution in sensor network [3]. Study of recent literature reveals that reliable mathematical modeling of ad-hoc networks is gaining increased attention [7]. In [2], they considered the case when each node is its own authority and tries to maximize the benefits it gets from the network. Attackers are mainly outsiders of any security system, and such attackers can be resisted through authentication protocol [9]. Routing protocol intrusion detection has also been studied as a mechanism for detecting misbehaving routers [10]. Mobile agent based mechanism is used in [8] to detect the intruders.

In [10] fully distributed cluster based packet routing architecture is given. The feasible path to a destination is calculated using the QoS information available with each cluster members.

III. SECURITY IN MANET

In contrast to fixed networks a centralized certification authority is not feasible in ad hoc networks. Distributing the functionality of certification authority over number of nodes is a possible solution. This can be achieved creating n shares for a secret key and distributing them to n different node. Key can be generated by combining s shares using threshold cryptography technique.

Current ad-hoc routing protocols are completely insecure. Moreover, existing secure routing mechanisms are either too expensive or have unrealistic requirements. In ad hoc network, security solution should isolate the attackers and compromised nodes in the network. Proactively isolating the attackers ensures that they cannot continue to attack and waste the network resources in future. A security solution should have decreasing overhead over time when the network is in good condition without any attacks. By adopting the cluster based security scheme it cause less overhead as the network is in operation and proactively isolate the attacker as non cluster member.

IV. CLUSTER-BASED TOPOLOGY

We assume that self organized mobile networks are formed by a group of nodes having a valid identity (for example communication between the military officials or disaster recovery team). In our design each node is granted temporary admission into the network using an identity verification process. Each node generates a secret using the equation (1) and forwards it to the neighboring nodes. To verify the secret, neighboring nodes generates the covert using its identification number and compute the difference between the received value and the calcu-

lated covert. If the difference is less than the threshold value Sth, it accepts the sender as a valid member and add the sender node ID to set S. (S is the set of all valid neighbors and dynamic clustering algorithm uses set S to create non-overlapping clusters)

$$y = f(id, cur - time) \quad (1)$$

After initial verification all nodes are continuously monitored by the neighboring nodes and credits are calculated based on the behavior of the neighbors. Watch-dog mechanism is used to monitor the neighboring nodes. A node accumulates its credits as it stays and behaves well in the network. The period of validity is propositional to its credits. Miss-behaving nodes credits are decremented; it will be denied network access when it reaches the minimum threshold level.

A. Probabilistic Clustering Model

It is possible to characterize this type of phenomena to which the poisson distribution is possible. T1, T2, T3 … Tn are the non-overlapping intervals, then the number of nodes entering into the cluster boundary in the interval is independent. There exists a constant q such that the probability of one event (exactly one node enters into the cluster boundary or leaves the cluster boundary) occurs in the interval of length dt is approximated to q*dt. The probability of two or more events will occur during an interval is approximately zero. So the experiment can be called as poisson experiment. For such experiment, if X counts the number of events occurs during any given interval, then it can be shown that X posses a poisson distribution. If the three poisson condition do hold and is X counts the number of events occurs during some specific time interval duration t, the X is poisson distributed with $\lambda = qt$.

$$P(X = x) = p(x;\lambda) = e^{-\lambda} \lambda^{x} / x! \quad (2)$$

The probability distribution function is

$$P(X \le x) = \sum_{k=0}^{x} p(x;\lambda) = \sum_{k=0}^{x} e^{-\lambda} \lambda^{k} / k! \quad (3)$$

E(x) is a parameter that carries information regarding the central tendency of the random phenomenon modeled by X. E(x) is often sufficient to give a partial description in terms of moments of the random variable. A moment generating function of a distribution can be employed to find the moments of the random phenomenon. Function of the variable t is defined as the moment of the random phenomenon X with respect to time t. The cluster topology changes can be represented using the random experiment X. The probability of nodes entering into the cluster boundary and nodes leaving a particular boundary can be calculated from the moment generating function.

Figure 1. Security architecture protocol stack

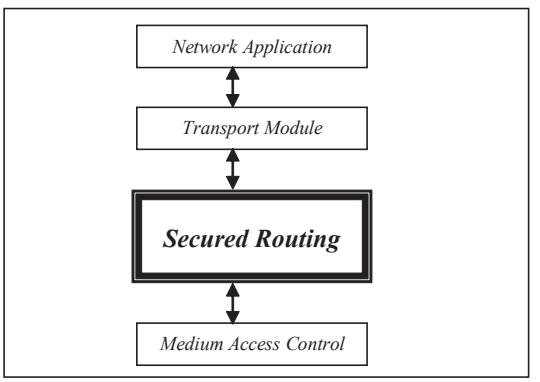


Figure 2. Framework of the network layer security

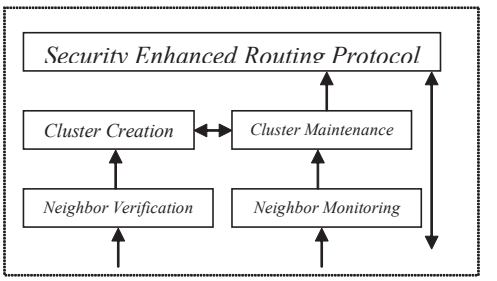


Figure 1 illustrates the protocol stack architecture of our security system. Figure 2 illustrates the composition of our security solution, which consists of five inter-related components.

B. Cluster Gateway Node Selection Process

MANETs can be modeled as an undirected graph with weight, G, G= [V, E] V, is the set of the mobile nodes and the E the set of the bidirectional wireless link. G and V are both dynamic set. An edge dominating set is a split edge dominating set if removal of D splits the graphs G1 and G2 into two sub graphs. The split domination number Dn is the cardinality of the dominating set.

Theorem 1

Let D be a split edge dominating set of G then

$$|E - D| \le \sum_{x \in D} \deg(x) \quad (4)$$

The equality holds if and only if the following conditions (a) and (b) hold.

a. D is independent
b. For each $x \in E - D$ there exits only one edge $y \in D$, such that $N^{I}[x] \cap D = \{y\}$, where $N^{I}[x]$ is the set of edges having exactly one vertex in common with x.

Proof:

Since each edge in $E - D$ is adjacent to at least one edge in D, it contributes at least one to the sum of degrees of the edge of D.

Hence $|E - D| \le \sum_{x \in D} \deg(x)$

Now let $|E - D| = \sum_{x \in D} \deg(x)$

Suppose D is not independent. Let x1 and x2 be any two edges of D having a common vertex. Then x1 is counted twice; once in deg(x1) and once in deg(x2). Then the sum of the degree of edges in D exceeds $|E - D|$ by at least two, a contradiction to the equality (6). Hence, D must be independent.

Now let $|E - D| = \sum_{x \in D} \deg(x)$ and (b) does not hold. Then $N^{I}[z] \cap D = \phi$ or $|N^{I}[z] \cap D| \ge 2$ for some $z \in E - D$. Since D is split dominating set the former case does not arise.

Let *x1* and *x2* belong to $N^{I}[z] \cap D$. Then $\sum_{x \in D} \deg(x)$ exceeds $|E - D|$ by at least one, since z is counted twice; once in deg(x1) and once in deg(x2), a contradiction. Hence if (a) and (b) are true then $|E - D| \le \sum_{x \in D} \deg(x)$.

If D is independent then D represent the set of gateway nodes that interlinks two clusters. So set of gateway nodes connecting two different clusters can be identified using equation (4).

Cluster creation module forms the non-overlapping clusters based on the valid neighbor set data. Gateway nodes are identified by the cluster maintenance module and all members maintain the list of gateway nodes. In dynamic network environment asymmetric keys can be used to encrypt/decrypt the data.

C. Cluster Maintenance

Cluster maintenance module proactively maintains the route information of all cluster members. There are three topology changes that requires cluster updation

Route discovery packets are forwarded only to the gateway nodes if the destination node is not in the same cluster. Our security system can operate in two modes. In normal mode route discovery packets are forwarded in plain text. Source announces its public key. Destination node can encrypts its data using source public key. For further data transfer symmetric keys can be used. In normal mode a passive attacker can view the path information during a data transfer. In fully secured mode in addition to data encryption the network layer packet header is also encrypted using the public key of gateway node along the path. In a shared wireless channel all neighbors hear the signal. But only the corresponding node can decode the coded signal using its private key. So information is never disclosed to unauthorized nodes.

V. IMPLEMENTATION

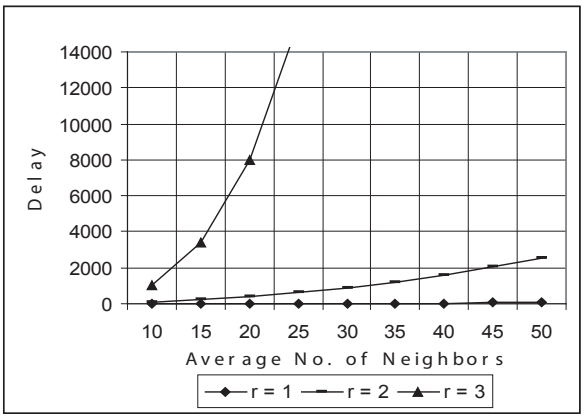
In order to provide scalability and to enhance the availability (by providing the service locally), the network is partitioned into a number of non-overlapping groups called clusters. In the conventional approach, each cluster has exactly one distinguished node, designated as cluster head, which is responsible for organizing and establishing the cluster. Cluster-head election algorithms are used to elect these cluster heads. The main bottleneck in this approach is the single point of failure (if the cluster head crashes, the entire QoS parameter table information will be lost), which forces the above procedure to be repeated for the construction of the QoS parameter table and subsequent election of the cluster head. To overcome the above problems, a fully distributed architecture is proposed. Clusters are created using a cluster creation algorithm and each cluster member maintains a QoS parameter table (about its cluster members) and a gateway table. Gateway nodes manage the communication with adjacent clusters. Routing is typically divided into two types: routing within the cluster (intra-cluster routing) and routing between different clusters (inter-cluster routing).

In this section, we present our algorithm and protocols that implement the localized security services and the self initialization of the mobile ad hoc networks. For the proposed clustering technique each node needs one or more hop connectivity information to execute cluster creation and maintenance algorithm. The cluster boundary or radius is adjusted based on the congestion factor of ad hoc network. The degree of the node is used as the congestion factor cf. If the congestion factor cf is grater than maximum threshold tmax (cf > tmax), it implies ad hoc population is very high consequently the hop count is set to one. If the congestion factor is between tmax and minimum threshold tmin (tmin <= cf <= tmax) it denotes the node is in a medium populated area consequently the hop count is set to two to create a strong connectivity. If the congestion factor cf is less than tmin (cf < tmin) it implies the node is in a sparsely populated area consequently the hop count set to three to maintain the strong connectivity.

Dynamic Clustering Algorithm

1. S: set of ID's of neighbors according to the hop count including the current node ID.
2. if (cur_id == msi(S))
   cluster_id = cur-id;
   forward to all nodes in set S (cur_id, cluster_id, location)
   S = S – {cur_id}
3. while (S != empty)
   on receiving neighbors(id, cid, loc)
   if (id == cid) and (cluster_id == UNKNOWN or cluster_id > cid) and (md == NOTSET or md > diff(cur_loc – loc)
   cluster_id = cid
   md = diff(cur_loc – loc)
   S = S – {id}
   if (cur_id == min(S))
   if (cluster_id == UNKNOWN) cluster_id = cur_id

Figure 3. Delay versus average no. of neighbors



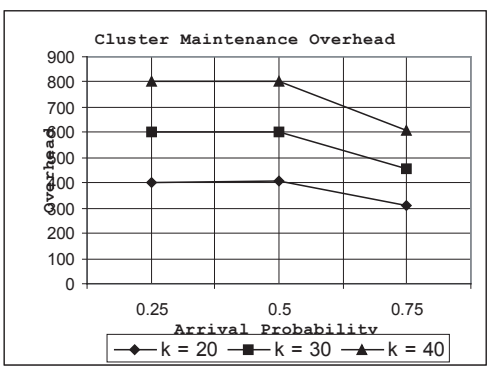
forward to all nodes in set S (cur_id, cluster_id, location)
S=S-{cur_id}

Using the above algorithm the non-overlapping clusters are formed based on the location of mobile nodes. The nodes, which are very close to each other, are grouped together. Each node maintains a route table with the QoS values and public key of all trusted cluster members. The algorithm is self-terminating and it leaves only the far-off isolated nodes as non-cluster members.

Neighbor monitoring is a lightweight process. It does not affect the normal functioning of a mobile node. For calculating the credit it simply listens to the packet forwarded by the nearby nodes. Using the message authentication code it checks whether the packets are relayed correctly by the neighboring nodes. Active attackers can be isolated using this mechanism. But another issue is in the shared wireless channel any node with in the transmission range of another node can receive the signals. So passive attackers can read all transmitted plain text data. To defend such types of attacks we propose a lightweight public key encryption method. The encryption and decryption process is done in the network layer. If network layer receives an encrypted packet, it decrypts the packet using its private key. If current node is the destination node, the data part is given to the upper layer. Otherwise according to the route table information find out the next node along the path to destination. Encrypt the packet using the intermediate node public key and send it. By this way we can protect the data from passive attackers also.

For cluster maintenance idle nodes periodically send a small alive signal to all trusted cluster members. If the update timer expires the corresponding node entry status in the route table is changed to down and it starts a wipe out timer. If the wipe out timer expires the corresponding entry is removed from the routable. If an alive signal or a data packet is received form that node before the timer expires then the status the node is revoked to up state and it restarts the update timer.

Figure 4. Cluster maintenance overhead



VI. PERFORMANCE EVALUATION

As the network topology changes dynamically, we considered a random topology for the analysis.

Let k denotes the average number of neighbors of a node. n is the number of mobile nodes in the network. c is the average number of members per cluster. Total number of messages replicated by a single cluster init message is

$$S_r = 1 + \sum_{i=0}^{r-1} k^i(k-1) \quad (5)$$

Where r denotes the radius of the cluster in number of hops. Rr nodes receive and process the cluster init message.

$$R_r = \sum_{i=0}^{r-1} k^i(k-1) \quad (6)$$

Figure 3 shows that as number of neighbors increases the processing overhead increases which in turn increases the packet transmission delay. Value of Rr is directly proportional to r and k. In ad hoc network topology changes dynamically. So k varies dynamically and it is not possible to control the topology change in ad hoc network. To have strong connectivity the cluster radius has to be increased. If r increases then the transmission delay increases exponentially. So without losing the connectivity we have to reduce the radius r. if number of neighbors' increases then r can be reduced without affecting the connectivity. If r decreases then transmission delay decreases. The cluster radius can be adjusted according to the value of k to maintain the connectivity and to reduce the transmission delay. If k is grater than the maximum threshold (tmax) then r can be set to one. If k is less than the minimum threshold (tmin) then r can be set to three. The maximum and minimum threshold values can set according to the other external parameters. If value of x is between tmax and tmin then rcan be set to two. The cluster initialization overhead can be maintained at an optimum level without losing the connectivity by adjusting the values of k and r.

For cluster maintenance each cluster member needs to forward the new information to all other cluster members. If a cluster member leaves the network, the trusted cluster member who identifies the change must inform this to all other members. A misbehaving node can also send a similar message to all other cluster members. But to prove the identity of the sender the trusted cluster member can encode the data using its private key. All other member maintenance the public keys of other trusted members and the data could be decoded using the corresponding public key. If a new node enters into the cluster boundary, it calculates the congestion factor. Based on the congestion factor it calculates the hop count and it executes the dynamic clustering algorithm. The cluster maintenance traffic overhead varies based on the arrival of new cluster member and departure of existing cluster members. Let Pnew is the new cluster member arrival probability. Let t is the traffic overhead per link. The overhead created by the arrival of new nodes is N.

$$N = Pnew\ [t(1 + 2\ r\ k)\ ] \quad (7)$$

Normally the probability of arrival of new cluster members increases as the node congestion increases. In our approach to maintain the connectivity, the cluster radius r is adjusted according to the congestion factor. So value of r decreased as Pnew increases. Figure 4 show that cluster maintenance overhead due to arrival of new cluster members does not increases as the new cluster member arrival probability increases.

$$c = r\ k \quad (8)$$

The control message traffic overhead for cluster maintenance is in o(c2). Even though the number of nodes in the network increases c remains almost constant because the cluster radius is adjusted according to number of nodes. c dose not increases as n increases. The control message traffic overhead does not increase as the number of nodes in the network increases. So this approach is scalable.

VII. CONCLUSION

Most of the proposed routing solutions are, as yet, incomplete when it comes to security issues. We can trust a routing mechanism only when it guarantees that all transmission will be protected. In this paper we proposed a novel security based routing protocol in which the packets are routed only through the trusted members. The trust factor of a mobile node is verified and monitored by neighbor verification and neighbor monitoring modules. Based on the calculated credits other cluster members maintain their routing table. In fully secured mode all transmissions are protected by encoding the network layer packet header in addition to data encoding. In the sheared wireless channel all neighbors hear the signal but only the corresponding router can decode the packet using its private key. Analysis shows that the secured cluster creation and maintenance overhead does not increase as the network size increases. This scheme is more efficient in terms of the resultant routes establishement, resource reservations, and computational complexity. If multiple malicious nodes collaborate, they in turn will be restricted and isolated by their neighbors, because they monitor and exercise control over forwarding RREQs by nodes. Hence, the scheme successfully prevents Distributed DoS (DDoS) attacks. Future works includes the implementation and testing of the algorithm in real environments.

REFERENCES

[1] E.M Belding-Royer, "Hierarchical routing in ad hoc mobile networks" Wireless Communication & Mobile Computing, vol. 2, no. 5, pp. 512 – 532, August 2002.

[2] L. Buttyan and J.P Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, pp. 579 – 592, Oct 2003.

[3] D.W Carman, P.S. Kruns and B.J Matt "Constraints and Approach for Distributed Sensor Security", NAI Labs Technical Reports, Sep 2000.

[4] Charles E. Perkins, Elizabeth M. Belding-Royer and Ian D. Chakeres. "Ad Hoc On-Demand Distance Vector Routing" Mobile Ad Hoc Networking Working Group, Internet Draft, Oct 2003.

[5] B. DeCleene, L. Dondeti, S.Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, s. Vasudevan and C. Zhang. "Secure Group Communication for Wireless Networks", in proc. IEEE MILCOM01, Oct 2001.

[6] Y. Desmedt and S. Jajodia, "Redistributing secret shares to new access structures and its applications," George Mason Univ., Tech. Rep., 1997.

[7] I. Glauche, W. Krause, R. Sollacher, and M. Greiner, "Continuum percolation of wireless ad-hoc communication networks," cond-mat/0304579, April 2003.

[8 C. Krugel and T. Toth, "Flexible, Mobile Agent Based Intrusion Detection for Dynamic Networks" Euro. Wireless, Italy 2002.

[9] K. Sanzgiri, B. Dahill, B.N Levine, C.Shields and E. Belding-Royer, "A secure routing protocol for ad hoc networks", in proc. 10th Int. Conf. Network Protocols (ICNP'02) 2002, pp 78-89.

[10] Nargunam A.S and Sebastian M.P "Fully distributed cluster based routing architecture for mobile ad hoc networks" In Proceedings of the first IEEE International Conference on Wireless and Mobile Computing, Networking and Communication (WiMob'2005) pages 383 – 389.