SECURE AND RELIABLE KEY DISTRIBUTION TECHNIQUE FOR MOBILE AD-HOC NETWORK

[1]VISHAKHA SANGHAVI, [2]ASST.PROF. NAREN TADA

[1]PG Student, CE Dept., V.V.P. Engineering College, Rajkot, GTU
[2]Assistant Professor, CE Dept., V.V.P. Engineering College, Rajkot, GTU

vishakha.rkcet @gmail.com

***ABSTRACT*: In mobile ad hoc networks, due to unreliable wireless media, host mobility and lack of infrastructure, providing secure communications is a big challenge in this type of network environment. Key management is an important service for providing secure communications when the network size is large or the topology is undergoing frequent changes. In most existing key management schemes, a centralized key certification authority is used; however, it is not suitable for wireless environments due to the networks' scalability and the insufficient computation ability of mobile nodes. The key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. Here we suggest a scheme that uses a cluster-based topology and provides secure key distribution with light-weight transmission to provide reliable communication. We will use cryptographic technique like hash function and MAC(Message Authentication Code) for providing security and use network coding scheme for providing robustness which reduces the computational overhead. It will provide confidentiality and authentication of nodes against eavesdropping and impersonation attacks.**

Keywords— Security in MANET .Key Management in MANET, Cryptography, Network Coding.

I: INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Typically the network nodes are interconnected through wireless interfaces and unlike traditional networks lack specialized nodes, i.e. routers, that handle packet forwarding. Instead every node in the network functions as a router as well as an application node and forwards packets on behalf of other nodes. Ad hoc networks have the ability to form .on the fly. and dynamically handle the joining or leaving of nodes in the network.

The ad hoc networks generally presents the following characteristics [1]:

1) *Dynamic network topology:*

The network nodes are mobile and the topology of the network may change frequently. Nodes may move around within the network but the network can also be partitioned into multiple smaller networks or be merged with other networks.

2) *Limited bandwidth*:

The use of wireless communication currently used implies a lower bandwidth than traditional networks. This may limit the number and size of the messages sent during protocol execution.

3) *Energy constrained nodes*:

Nodes in ad hoc networks will most often rely on batteries as their power source. The use of complex algorithms, that consumes CPU time and energy there may not be possible.

MANETs consist of mobile nodes interconnected by multihop communications paths or radio links which are free to move at any speed in any direction and organize themselves randomly and can act as both routers and hosts. The nodes in the network function as routers, clients, and servers. These nodes are constrained in power consumption, bandwidth, and computational power. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. The security is an important issue for ad hoc networks; one of the major problems in providing security services in ad hoc networks is how to manage the cryptographic keys that are needed. In order to design practical and efficient key management systems it is necessary to understand the characteristics of ad hoc networks and why traditional key management systems cannot be used.

The paper is organized as follows: Section II describes the Key Management in MANET. Section III gives idea about the different key distribution techniques for providing Security. In section IV, we discuss the network coding approach. In section V, we mention the proposed algorithm to provide the security in key distribution in MANET.

II: KEY MANAGEMENT IN MANET

Many cryptosystems rely on the underlying secure, robust, and efficient key management subsystem. In fact, all cryptographic techniques will be ineffective if the key management is weak. Key management is a central part of the security of MANETs. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. Some asymmetric and symmetric key management schemes have been proposed to adapt to the environment of MANETs. Key management deals with key generation, key storage, distribution, updating, revocation, deleting, archiving, and using keying materials in accordance with security policies.

A keying relationship is the state wherein network nodes share keying material for use in cryptographic mechanisms. The keying material can include public/private key pairs, secret keys, initialization parameters and non-secret parameters supporting key management in various instances. Key management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties [2].

The fundamental function of key management schemes is the establishment of keying material. *Key establishment* can be subdivided into key agreement and key transport. *Key agreement* allows two or more parties to derive shared keying material as a function of information contributed by, or associated with, each of the protocol participants, such that no party can pre-determine the resulting value. In *key transport* protocols, one party creates or otherwise obtains keying material, and securely transfers it to the other party or parties. Both key agreement and key transport can be achieved using either symmetric or asymmetric techniques [3].

III: DIFFERENT KEY DISTRIBUTION TECHNIQUES FROM PREVIOUS WORK

The operations like packet forwarding and routing, distributing keys or any secret information can be easily jeopardized if counter-measures are not taken on these operations at early stages. Key management is central to MANET security. Key management involves key generation, key distribution, key updation. The difficult task is how to distribute a key and update a key to ensure secure communication between two authenticated nodes. Because any node can enter or leave the network in dynamic topology, key updation must be done securely. If a new node wants a key to communicate with other node, any key must be kept secret should be distributed in a way that authenticity, confidentiality and integrity is not violated and there should be less message passing for provide authenticity and confidentiality between communicating nodes. There have been several research work proposed on key distribution schemes in recent literatures.

In N. Suganthi, R. S. Mohana Priya and V. Sumathy's scheme [4], they have suggested to divide the network into clusters. Cluster head will maintain the group key, it will also update the group key whenever there is a change in the membership. Here the re-keying process will be performed only if there is any movement of nodes within the clusters. So the computation and communication cost will be reduced. They provided authentication between communicating nodes both in inter and intra cluster communication. And also the network life time will be extended with the help of monitoring node. The performance results prove the effectiveness of that key management scheme. Without clusters, the computation time, time delay and packets transferred from central node are more. With the formation of cluster, the computation time and other parameters are greatly reduced. Due to distributed behavior ,the performance has been increased.

Another scheme for security [5] is provided by D. Suganya Devi and G.Padmavathi. It illustrates an algorithm which is an enhancement of Optimized Multicast Cluster Tree (EOMCT) with Destination Sequenced Distance Vector (DSDV) routing protocol. It provides efficient multicast key distribution. The main idea of EOMCT is to use DSDV routing protocol to elect the local controllers of the created clusters as shown in figure 7. The principle of this clustering scheme is to start with the group source Group Controller (GC), to collect its 1-hop neighbors by DSDV, and to elect LCs which are group members have child nodes at the next level. The LC belongs to the unicast path between the source and the child group members. At this step, the elected LCs covers the group members having 2-hops neighbors of the group source. This scheme iterates until LCs cover all the group members. This method is performance efficient and more suitable for secure multicast key distribution dedicated to operate in MANETs. The future work deals with reliability of key distribution, which is an important issue in adhoc network due to the high packet loss during secure multicast key distribution.

Cluster-based composite key management scheme [6] is suggested by R.PushpaLakshmi, Dr.A.Vincent Antony Kumar. In this scheme, authors have presented a new composite key management scheme based on a combination of techniques such as hierarchical clustering, partially distributed key management, offline certification authority and mobile agent. Initially, clusterhead is elected using dominator election algorithm. It computes trust value of each node based on node's neighbors opinion.The resultant node with maximum trust ability is marked as dominator. Next, the public key of ClusterHead (CH) changes with respect to its trust value. The public key is evaluated based on its previous public key and its trust value. At last, when new node joins the cluster, Offline dealer assigns unique id for the new node. The new node register its public key information in CH. CH records the information about new member in its member table with fields: mem_id, public key. When a node leaves a cluster, the CH removes the node information from it's member list.

Message Relaying Scheme [7] is proposed by Hisham Dahshan and James Irvine. They present an analysis of a message-relaying based key distribution scheme for mobile ad hoc networks that was previously proposed by van der Merwe et al. Considering the message overhead occurring at the MAC layer in addition to the message overhead occurring at the network layer is an important issue in order to get a comprehensive study of the impact of the scheme on both layers. The scalability of the scheme is evaluated by investigating its performance on a network as large as 100 nodes. Message relaying scheme provides an efficient way to distribute keying material. The key distribution scheme is scalable since the one-hop certificate delivery ratio varied between 97% and 84% in the first scenario and between 99% and 81% in the second scenario.

R. Murugan and A. Shanmugam have suggested the scheme [8] for mminimum prior trust relationship between the nodes. It provides approach for a distributed key management and authentication approach by deploying the recently developed concepts of identity based cryptography and threshold secret sharing. The identity-based cryptography mechanism provided not only to provide end-to-end authenticity and confidentiality, but also saves network bandwidth and computational power of wireless nodes. which guarantees the ability for an arbitrary pair of devices to exchange a key in a secure fashion. This process is achieved without the prior knowledge of the maximum MANET size. The ad hoc wireless network can grow incrementally and also reduce if the mobile node participated in one ad hoc is detached due to the node movement from one zone to another.

IV: NETWORK CODING APPROACH

Network coding offers an excellent solution for maximizing throughput in various networks. Because of its simplicity and high efficiency, the idea of network coding can also be used for designing a lightweight key distribution schemes for wireless ad hoc network. It can resist a series of attacks suffered in wireless ad hoc network and has better performance.

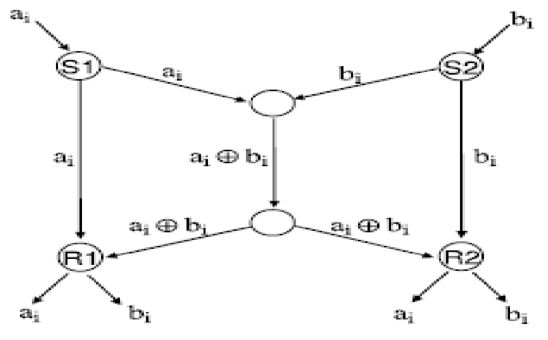

Fig. 1 Simple Scenario of Network Coding [9]

Consider a communication network in which certain source nodes multicast information to other nodes on the network in the multihop fashion where every node can pass on any of its received data to others. We are interested in how fast each node can receive the complete information, or equivalently, what the information rate arriving at each node is. Allowing a node to encode its received data before passing it on, the question involves optimization of the multicast mechanisms at the nodes. Among the simplest coding schemes is linear coding, which regards a block of data as a vector over a certain base field and allows a node to apply a linear transformation to a vector before passing it on**.**

The idea underlying network coding is usually illustrated using the famous butterfly example.

Consider the network in Fig. 1, where source *S*1 wants to deliver the stream of messages *ai* to both *R*1 and *R*2, and source *S*2 wants to send the stream of messages *bi* to the same two receivers. Assume all links have a capacity of one message per unit of time. If routers only forward the messages they receive, the middle link will be a bottleneck, which for every time unit, can either deliver *ai* to *R*1 or *bi* to *R*2. In contrast, if the router feeding the middle link XORs the two messages and sends *ai* ⊕ *bi* (or any linear combination of *ai* and *bi*), as shown in the figure, both receivers obtain two messages in every time unit. Thus, network coding, i.e., allowing the routers to mix the bits in forwarded messages, can increase network throughput.

V: PROPOSED METHOD TO PROVIDE SECURITY IN KEY DISTRIBTION

We consider a cluster-based ad hoc hierarchical network topology. A subset of the network nodes is selected to serve as the network backbone over which essential network control functions are supported. The approach to topology control is often called clustering, and consists of selecting a set of c1usterheads in a way that every node is associated with a c1usterhead, and c1usterheads are connected with one another directly or by means of gateways, so that the union of gateways and c1usterheads constitute a connected backbone. Once elected, the c1usterheads and the gateways help reduce the complexity of maintaining topology information, and can simplify such essential functions as routing, bandwidth allocation, channel access, power control or virtual-circuit support.

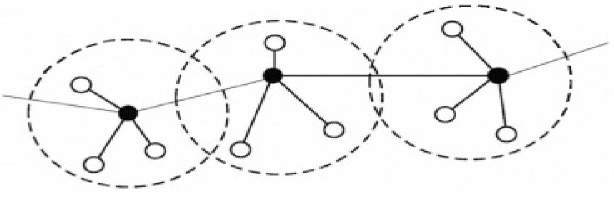

Fig. 2 Network Topology

- **<u>Step 1:</u>**

In first step, we are combining some nodes to make one cluster. After defining all clusters, select a set of c1usterheads in a way that every node is associated with a c1usterhead, and c1usterheads are connected with one another directly or by means of gateways.

Dominator election algorithm selects a node having maximum trust ability and maximum probability of future contact as dominator. The algorithm computes trust value of each node based on node's neighbors opinion. For node i in the network the algorithm compares node's trust value with trust value of its neighbors. The resultant node with maximum trust ability is marked as dominator.

If there exists nodes with equal trust ability, the algorithm compares the probability of future contact of nodes with neighbors. It select a node with maximum probability as dominator. A node is selected as dominator only if it is not in dominating set and N(i) not in dominating set. The selection mechanism is performed when any of the following happens: Cluster Head(CH) goes down due to low battery, CH moves outside the cluster, periodically for certain time interval. The procedure for dominator election is described as follows.

```
For each node i in the network
    Compute Ti = compute_trust(i, N(i))
End for

For each node i in the network
    For each node j in N(i)
        Find node k with max(Ti,Tj)
            If Ti = Tj
        Calculate Pcontact for i and j
          Find node k with max(Pcontact )
            End if
        Add k to DS if k є DS and N(k) є
      DS
    End for
End for
```

- **Step 2:**

In Second step, we initialize the keys by RSA algorithm, we assume here that there is one TTP (Trusted Third Party) in the network to initialize the scenario. It generates a random number, a secret key and the corresponding identifiers for each Ad hoc node. TTP stores Key; and a list of an encrypted version of the other node's keys.

```
For each node i in the network
    Initialize key
    Where key includes a random number, Secret
    key and identification number
End for
```

- **Step 3:**

In third step, we distribute the keys based on whether the sending and receiving nodes are in same clusterhead or in different cluster. If there are in same cluster then sending and receiving nodes will request and reply through its clusterhead and after authenticate nodes by checking MAC address of both are same or not, clusterhead do network coding of their request and reply so that communication time can be less and generate a secret key and send it to both nodes so they can share the secret information.

If there are in different cluster then sending and receiving nodes will request and reply through their clusterhead and after authenticate nodes by checking MAC address of both are same or not, both clusterhead will be checked for authentication and then they do network coding of their request and reply so that communication time can be less and generate a secret key and send it to both nodes so they can share the secret information.

```
Begin
    Check sender and receiver nodes are ion
same cluster or not.
    If they are in same cluster
        CH generates MAC address and do
    network coding and send it to both nodes.
        Sender and Receiver node
        computes the MAC address and
        compare them for authentication
        and confidentiality.
    Endif
    If they are not in same cluster
        Both clusterhead s generate the
        MAC address and do network
        coding on keys. Both clusterhead
        also computes the MAC address
        and compare them for authenticity
        of clusterheads.
    Endif
     CH generates the secret keys for sender
       and reciver node. On receiving the keys,
       both nodes can distribute the data
       securely.
End
```

- **Step 4:**

In step 4, we update the keys, If any node will leave or any new node want to join the network, then key should be generated for new node and key should be discarded for leaving node and information about changes in the keys should be passed to all other nodes in the network.

Two random number are included in secret share key which are changed with every new protocol execution, it will guarantee that it will be fresh for every protocol. When a node wants to update key, only execution of the new protocol should be initiated.

VI: CONCLUSION

Although security issues in mobile ad hoc networks have been a major focus in the recent years, the development of fully secure schemes for these networks has not been entirely achieved till now. MANETs have a unique characteristics and constraints that make traditional approaches to security inadequate. The lack of an infrastructure exacerbates the situation of using shared secret keys or authentication among members. In this paper, we propose a scheme which uses network coding approach and cryptographic method to secure the key distribution in MANET. This method will provide less communication overhead for distributing the keys and provides authentication and confidentiality between nodes.

REFRENCES

[1] J.Macker and S. Corson, RFC 2501, Mobile Adhoc Networking(MANET):Routing Protocol Performance Issues and Evaluation Consideration, IETF 1999.

[2] Johann van der Merwe, "Key Management in Mobile Ad-hoc Network", M.Sc. Thesis, Nov. 2005.

[3] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook in Applied Cryptography*. CRC Press, 1996.

[4] N. Suganthi, R. S. Mohana Priya, V. Sumathy, "An Efficient and Dynamic Key Management Scheme for Mobile Ad-hoc Nework", European Journal of Scientific Research, ISSN 1450-216X, Vol.55, No.4 (2011), pp.no. 538-548.

[5] D. Suganya Devi and G.Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Ad hoc Networks", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp. 934-938, Oct. 2009.

[6] R.PushpaLakshmi, Dr.A.Vincent Antony Kumar," Cluster Based Composite Key Management in Mobile Ad Hoc Networks", International Journal of Computer Applications**,** Vol. 4, No.7, pp. No. 30-35, July 2010.

[7] H. Dahshan and J. Irvine, "Analysis of Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying", IEEE International Conference on Wireless and Mobile Computing (WIMOB), pp. 538-542, Oct. 2008.

[8] R. Murugan and A. Shanmugam, "Key Distribution System for MANET with Minimum Prior Trust Relationship", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, pp. no. 75-79, May 2009.

[9] S. Katti, H. Rahul, W. Hu, D. Katabi, M. M´edard, J. Crowcroft, "XORs in The Air: Practical Wireless Network Coding", SIGCOMM'06, 11–15 Sep. 2006, Pisa, Italy.