# Authentication Based Scheme In MANET Using Cluster Based Routing Protocol

**Prof. Pranita M. Potey, Prof.Manish Potey, Prof. Nandini C. Nag**
(Department of Electronics & Telecommunication, Mumbai University, India)
(Department of Computer Engineering, Mumbai University, India)
(Department of Electronics & Telecommunication, Mumbai University, India)

.

## ABSTRACT

**Mobile and wireless technology is growing at a rapid rate. These advances have resulted in breakthroughs that have made feasible several prospects that were thought as impossible. Ad hoc networks are a consequence of the ceaseless research efforts in Mobile and Wireless networks. Ad hoc network is a class of wireless networks where there is no fixed infrastructure. Unlike traditional networks they do not have base stations to coordinate the activities of mobile hosts.**

**In this paper we proposed the authentication scheme using CBRP in MANETS. Here we have explored the concept of MANETS in location database management with proper authentication. For this purpose we have presented a distributed network consisting of two clusters along with their cluster heads.**

*Keywords-* **Authentication, CBRP, Cluster, MANET.**

## 1. INTRODUCTION

Mobile Adhoc wireless networks are basically the category of wireless networks that utilize multi–hop radio relaying and are capable of operating without the support of any fixed infrastructure. Hence they are also called infrastructures less networks.

Ad hoc wireless networks don’t need any infrastructure to work. In this each node can communicate with another node without any access point controlling medium access. Nodes in an ad hoc network can communicate only if they can physically reach each other i.e. if they are within each other’s radio range or if other nodes can forward the message. Nodes from two ad hoc networks can’t therefore communicate with each other if they are not within the same radio range. In ad hoc networks there might be only selected nodes which have the capability to forward data. In such a case most of the nodes have to connect to such a special node first in order to transmit data if the receiver is out of range.

In ad hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms which are the mechanisms to handle hidden or exposed terminal problems & priority mechanisms to provide certain quality of service. This type of networks provides greatest possible flexibility.

The absence of any central coordinator or base station makes the routing a complex one compared to cellular networks. In an ad hoc wireless network the routing and resource management are done in a distributed manner in which all the nodes coordinate to enable communication among them. This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes. Hence the mobile nodes in ad hoc wireless networks are more complex than their counterparts in cellular networks. The ad hoc routing protocol should minimize routing overhead, broken links or new routes should be detected as soon as possible, changes to the network topology should be detected and new routes must be created as soon as possible. It should also minimize memory or computation power at the hosts.

Wireless mesh networks and wireless sensor networks are specific examples of ad hoc wireless networks.These networks could be extremely useful in any scenario where geographical, terrestrial or time constraints make it impossible to have base stations. In battlefields or any other disaster situation where a network needs to be formed on an ad hoc basis without the support of any fixed infrastructure. In military applications it is also desirable to have a distributed system so that the risk of the entire network being compromised due to a single central authority is taken care of.

## 2. AUTHENTICATION IN MANETS

Basically there are two main approaches to solve the authentication problem in ad hoc networks. These two groups of cryptographic technique are defined using the basic classification used in cryptography which distinguishes between secret and public key methods.

The solution included in the first group are not many and they are recommended for sensor networks as the devices forming these networks are even more constrained in their resources.

The second approach methods based on Public Key Infrastructure (PKI) are the most studied so far. The main focus is on how to use public key cryptography and how to manage public key certificates in this restricted atmosphere.

Among the available possibilities to implement PKI in ad-hoc networks the easiest way is to employ a global trusted centralized certification authority (CA).Nevertheless this approximation should be discarded as it will hinder scalability. The main obstacle is that the access to this entity may provoke a bottleneck slowing down the communications among the member of the network since it is compulsory connecting with CA and verify each time the certificate. The most natural modification is to distribute the CA task among a set of nodes. In this sense the CA'S functions will be developed by a set of special servers included in the network. These servers will sign the public key of the nodes. In this way each time a component of the network B wishes to communicate with A of its peer should be in contact with the servers in advance in order to obtain A's public key signed with CA'S secret Key.

## 3. KEY MANAGMENT

Ad hoc wireless networks pose certain specific challenges in key management due to lack of infrastructure in such networks. Two types of infrastructure have been identified which are absent in the ad hoc was the network in wireless network. The first infrastructure, such as dedicated routers and stable links. This ensures communication with all nodes. The second missing infrastructure in ad hoc wireless networks is the administrative support of certifying authorities.

### 3.1 Password Based Group Systems

Several solutions for group keying in ad hoc wireless networks have been suggested in the example scenario for implementation is a meeting room, where different mobile devices want to start a secure session. The parties involved in the session are to be identifies based on location, that is, all devices in the room can be part of session. Hence, relative location can be used as the criterion for access control. If a TTP which knows the location of the participants exists, that it can implement location based access control. A prior shared secret key can be obtained by plugging on to a wired network first, before switching to the wireless mode. A password based system has been explored where, in the simplest case, a long string is given as a password for users for one session. However human beings tend to favor natural flavor, natural language phrases as password, over randomly generated strings. Such passwords if used as keys directly during a session, are really weak and open to attack because of high redundancy, and the possibility of reuse over different sessions. Hence protocols have been proposed to drive a strong key (not vulnerable to attacks) from the weak passwords given by the participants. This password based system could be two parties, with a separate exchange between any two participants, or it could be for whole group, with a leader being elected to preside over the sessions. Leader election is a special case of establishing an order among participants. The protocol used is as follows. Each participant generates a random number, and sends to all others. When every node has received a random number of every other node, a common presided function is applied on all the numbers to calculate a reference value. The nodes are ordered based on the difference between their random number and the reference value.

### 3.2 Threshold Cryptography

Public key infrastructure (PKI) enables the easy distribution of keys and a scalable method. Each node has a public/private key pair and a certifying authority (CA) can bind the keys to the particular node. But the CA has to be present all the time, which may not be feasible in ad hoc wireless network. It is also not advisable to simply duplicate the CA at different nodes. A scheme based on threshold cryptography has been proposed by which n servers exists in ad hoc wireless network, out of which any (t + 1) servers can jointly perform any arbitration or authorization successfully, but t servers cannot perform the same. Hence up to t compromised servers can be tolerated, this is called as (n, t+1) configuration, where n ≥3t+1.

To sign a certificate each server generates a partial signature using its private key and submits it to a combiner. The combiner can be any one of the servers, in order to ensure that the key is combined correctly, t+1 combiner can be used to account for at most t malicious servers, using t+1 partial signatures (obtained from itself and t other servers), the combiner computes a signature and verifies its validity using a public key. If the verification fails it means that any one of the t+1 key is not valid, so another subset of t+1 key is tried. If the combiner itself is malicious, it cannot get a valid key, because the partial signature of itself is always invalid.

The scheme can be applied to asynchronous networks, with no bound on message delivery or processing times. This is one of the strengths of the scheme, as the requirement of synchronization makes the system vulnerable to DOS attacks, an adversary can delay a node long enough to violate the synchrony assumption, thereby disrupting a system.

Sharing a secret in a secure manner alone does not completely fortify a system. Mobile adversaries can move from one server to another, attack them and get hold of their private keys. To counter this share refreshing has been proposed, by which servers create a new independent set of shares (the partial signatures which are used by the servers) periodically. Hence to break the system, an advisory has to attack and capture more than t servers within the period between two successive refreshes. Otherwise the earlier share information will no longer be valid. This improves protection against mobile adversaries.

### 3.3 Self Organized Public Key Management For Mobile Ad hoc Network

We have proposed a completely self-organized public key system for ad hoc wireless networks. This makes use of absolutely no infrastructure – TTP, CA, or server even during initial configuration. The users in the ad hoc wireless network issue certificates to each other based on personal acquaintance. A certificate is a binding between a node and its public key. These certificates are also stored and used by users themselves. Certificates are issued only for specific period of time and contain their time of expiry along with them. Before it expires, the certificate is updated by the user who had issued the certificate.

Initially each user has a local storage area consisting of certificate issued by him and the certificate issued by the other user to him hence, each certificate is stored twice by the issuer and the person for whom it has issued, periodically certificates from neighbors are requested and the repository is updated by adding any new certificates. If any of the certificates are conflicting (example, the same public key to different users, or the same user having different public keys), it is possible that a malicious note has issued a false certificate. A node than labels such certificates as conflicting and tries to resolve the conflict. Various method exist to compare the confidence in one certificate over another for instance another set of certificates obtained from another neighbor can be used to take a majority decision. This can be used to evaluate the trust in other users and protect malicious nodes. If the certificate issued by some node is found to be wrong, then that node may be assumed to be malicious.

## 4. KEY MANAGEMENT SERVICE

We employ cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. Use of such schemes usually requires a key management services. We adopt a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after nodes authenticate each other and establish a shared secret session key. In a public key infrastructure, each node has a public / private key pair, public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. There is a trusted entity called Certification Authority (CA) for key management .The CA has a public / private key pair, with its public key known to every node, and signs certificates binding public keys to nodes. The trusted CA has to stay on – line to reflect the current bindings, because the bindings could change over time: A public key should be revoked if the owner node is no longer trusted or is out of the network a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key.

It is problematic to establish a key management service using a single CA in ad hoc networks. The CA, responsible for the security of the entire network, is a vulnerable point of the network. If the CA is unavailable, nodes cannot get the current public keys of other nodes or to establish secure communication with others. If the CA is compromised and leaks its private key to an adversary, the adversary can then sign any erroneous certificate using this private key to impersonate any node or to revoke any certificate.

A standard approach to improve availability of a service is replication. But a replication of the CA makes the service more vulnerable. Compromise of any single replica, which possesses the service private key, could lead to collapse of the entire system. To solve this Problem, we distribute the trust to a set of nodes by letting these nodes share the key management.

## 5. AUTHENTICATION STRATEGY

The authentication strategy presented here is for a hierarchical architecture. A cluster based network has been used. The routing protocol that uses this is cluster based routing protocol, i.e., CBRP.

The cluster based architecture was devised to minimize the flooding of route discovery packets. The routing protocol that uses this is *Cluster Based Routing Protocol*, CBRP. This kind of architecture is most suitable for large networks with several nodes. The entire network is divided into a number of overlapping or disjoint 2-hop-diameter clusters as shown in figure below

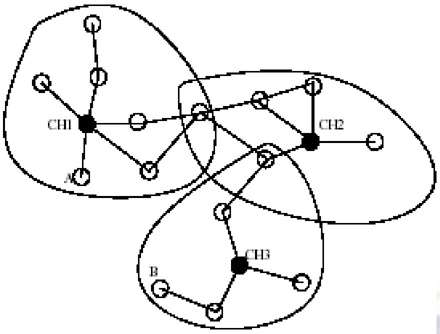


Fig 5.1. Cluster Formation

A cluster head is elected for each cluster to maintain the cluster membership information. A cluster is identified by its cluster Head ID. Each node in the network knows its Cluster Head(s) and therefore knows which cluster(s) it belongs to. A node regards itself as in cluster X if it has bi-directional link to the head of cluster X. In the current implementation of CBRP, the node with lower node ID is elected as cluster head. All the nodes broadcast HELLO messages periodically. The hello messages also contain tables carrying information about neighboring nodes and adjacent clusters.These HELLO messages are useful for maintaining upto date 2-hop topology.
The main focus is on authentication scheme that is most optimal for such hierarchical architectures.

## 6. ASSUMPTIONS

The proposed scheme is based on the following assumptions:
1. All the nodes of the network mutually trust one another. This can be safely assumed because the formation of the network itself is after the approval.
2. Each network node has sufficient computational power to execute the encryption algorithms and key generation algorithms.
3. Each node has sufficient memory to store the keys.
4. The transport protocol used is TCP.

Prior to the explaining the approach, we define the different key types that are used and the method adopted for the distribution of these keys.

When a node joins the network, it is given a *system public key* and *system private key*. This pair of keys is shared by all the nodes of the network. Besides the system key, each node also needs a *cluster key*. This *cluster key* is unique to every cluster and a single cluster key is shared by all the nodes belonging to a cluster. This key is generated by the cluster head and distributed to all the cluster members. This key is encrypted with the *system public key* and broadcast by the head. Each cluster head also has a unique pair of public/private key called *headkey*.

This private key is known only to the head that generates it. The corresponding public key is known to all the network nodes. This is done by means of a network wide broadcast that is initiated by each head immediately after it gets elected as the leader. Thus each member node needs to maintain a pair of *system keys*, a *cluster key* and a table consisting of *cluster ids* and the corresponding head's *public key*. The cluster head has an additional responsibility of storing securely its private key.

## 7. ALGORITHM

Nodes A, B and their respective cluster heads, CH1 and CH2, are marked. The cluster head acts as the certification authority for all its members. If A wishes to communicate with B, the following steps are to be performed for data authentication and integrity.

The two communicating parties, A and B, exchange a session key that is only valid for one TCP session. This is exchanged after mutual authentication for which their corresponding heads act as CAs. The head's keys are used for secretly exchanging session keys. The Cluster Heads then decrypt and transmit the session key to their corresponding members who are involved in the session.

When a node wants to establish a session with another node, it also sends this request to the head.

The head generates a set of k random prime numbers, (R1, R2, Rk), that are fairly large. The value of k could be as small as 16 or 32.The k numbers are encrypted first with the *head's private key* and then with the *cluster key*. Along with each number a time-stamp is encrypted so that they could be used for a limited amount of time. Therefore, each cluster head has a table containing Eck (Epv(R1; tv)); to Eck(Epv(Rk; tv)) where Eck is encryption using cluster key, Epv is encryption using the head's private key and tv is the corresponding timestamp.

The head then broadcasts the k encrypted values, Eck(Epv(R1; tv)); toEck(Epv(Rk; tv)). All other cluster members could also receive this and buffer the values since these *k* values could serve as *authentication tags* for any of the members. The tags are decrypted with the cluster key before they are buffered. They can be used as authentication tags because they have been encrypted with the head's private key. They are also encrypted with the session key to protect them from malicious listeners.

If the sender already has unexpired *tags* that it acquired by listening to earlier broadcasts from head, then it would use the same and not send any request to the head.

When a window of *w* packets is to be sent, the k encrypted tags are used to obtain a permutation of size w. Each of these tags is appended to one packet.

When the receiver receives the packets with tags appended, it should be able to verify the origin and authenticity of the tags. A function called *check* is used for this purpose. The tags are input to the function, and the output of the function is a value that is unique for each set of input. Since the tags are prime numbers the check function could be as simple as the product of the decrypted tags. It would be unique.

The sender applies the check function to the tags, considering ‘m’ at a time (the number ‘m’ can be decided according to the application). This function is computed as check(R0;R2…..R(m - 1)) , check(R(m+1) , R - (m + 2)…….R(2m - 1)), and so on.

The output of the function is encrypted. The highest sequence number among these ‘m’ packets is also encrypted along with the value obtained from the check function. The session key is used for this encryption.

When the receiver receives the packets, it also computes the check function of the received tags. The computed value is compared with that sent by the sender. If they match the sender accepts, else the sender could identify that some tags are invalid.

Since the check function is computed for every ‘m’ packets the receiver could even narrow down the search for unauthentic packets to a range of ‘m’. The checksum field of the TCP header is also encrypted with session key so that any tampering of data during transit would be detected by computing checksum.

## 8. RESULTS

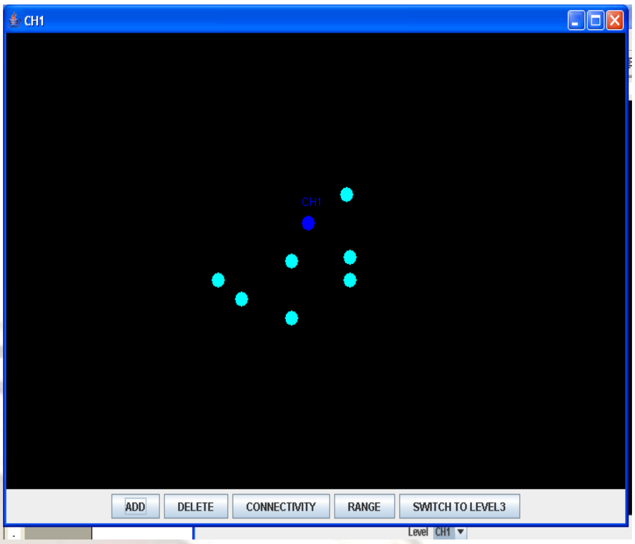


Fig 8.1. Cluster1 and the various nodes are created

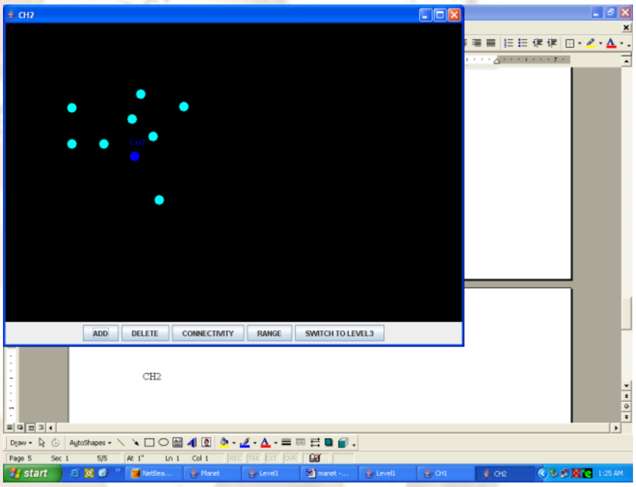


Fig 8.2. Cluster2 and the various nodes are created

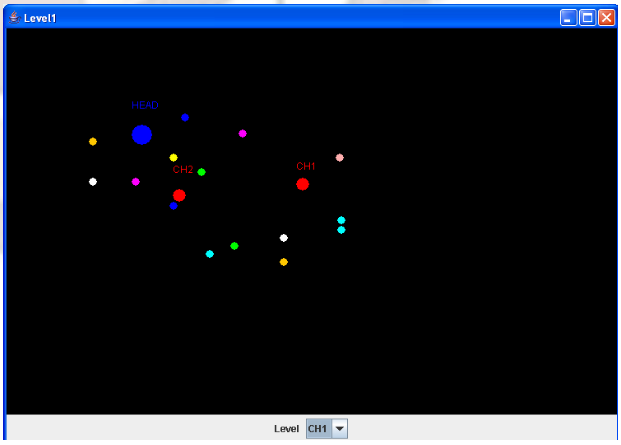
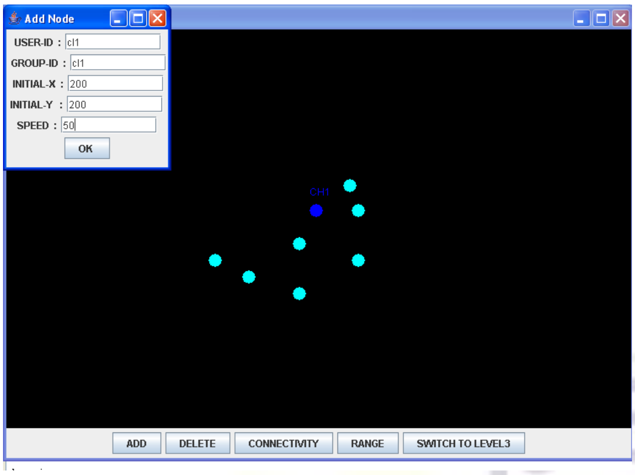


Fig 8.3.Cluster Head and Cluster1 and Cluster2 are formed



USER-ID : cl1
GROUP-ID : cl1
INITIAL-X : 200
INITIAL-Y : 200
SPEED : 50
OK

Fig 8.4. Adding node to cluster 1

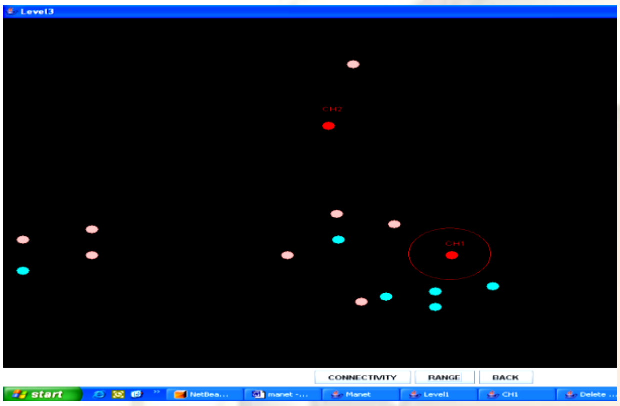


Fig 8.5 .Indicating range of node

## REFERENCES

[1] Ben-Jye Chang; Szu-Liang Kuo, "Markov Chain Trust Model for Trust-Value Analysis and Key Management in Distributed Multicast MANETs", *Vehicular Technology, IEEE Transactions* Volume: 58 , Issue: 4 , 2009 , Page(s): 1846 - 1863IEEE JOURNALS

[2] Denko, M.K., Jun Tian , Nkwe, T. ,Obaidat, M.S. Dept. of Comput. "Cluster-Based Cross-Layer Design for Cooperative Caching in Mobile Ad Hoc Networks", *Canada,Systems Journal*, IEEE Volume: 3 , Issue: 4 , 2009.

[3] Jane Y. Yu and Peter H.J. Chong, "A Survey of Clustering Schemes For Mobile Ad Hoc Networks" *IEEE Commun. Survey & Tutorial*, First quarter 2005, Vol 7 No.1.

[4] Shengrong Bu; Yu, F.R.; Liu, X.P.; Mason, P.; Tang, "Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks". *Vehicular Technology, IEEE Transactions* , 2011 , IEEE JOURNAL

[5] Jean-Pierre Hubaux, Srdjan Capkun, Student Member "Self-Organized Public-Key Management for Mobile AdHoc Networks", *IEEE transaction on mobile computing*, volume 2, No.1 ,march-January2003

[6] Kitada, Y., Watanabe, A., Sasase, I., Takemori, K., "On demand distributed public key management for wireless ad hoc networks", 2005 *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, IEEE, Aug. 2005, pp.454-457

[7] Capkun, S., Buttyan, L., Hubaux, J.-P., "Self-organized public-key management for mobile ad hoc networks", *IEEE Transactions on Mobile Computing, IEEE Educational Activities Department*, Volume 2, Issue 1, Jan.-Mar. 2003, pp.52-64

[8] Gutmann, P., *"Simplifying public key management", Computer, IEEE Computer Society, Volume 37, Issue 2, Feb*. 2004, pp.101-103.

[9] Ruidong Li, Jie Li, Kameda, H., Peng Liu, *"Localized public-key management for mobile ad hoc networks"*, Proceedings of the IEEE 2004 Global Communications Conference, IEEE, Volume 2, 29 Nov.-3 Dec. 2004, pp.1284-1289