Smart Key Managment Using Incremental Grouping key Management Algorithm

Ms.Rashmi C.Deshmukh*, Prof.Bhushan N.Mahajan**
*(Department of (Wireless Communication & Computing), G.H.R.C.E (Autonomous), India)
** (Department of Computer Science & Engineering , G.H.R.C.E (Autonomous), India)

ABSTRACT

Wireless networks that utilize multi-hop radio relaying and are capable of operating without any support of fixed infrastructure. Ad hoc wireless networks are defined, as the nodes communicate directly between one another over wireless channels.

As mobile ad hoc networks edge closer toward wide-spread deployment, security issues have became a central concern and are increasingly important.To transfer the data from source to destination trust is very important.

Key management is an essential cryptographic primitive upon which other security primitives are built. In this,technique key management issue of mobile ad-hoc network is discuss. In which the original data are encrypted multiple times and hence this technique provide multiple encrypted data which gives more security. Decryption of multiple encrypted data is done only at destination node.

Keywords **–** Cluster, Cluster Head, Encryption, Key Management, MANET, Security.

1. INTRODUCTION

1.1 Mobile Ad hoc networks

Mobile Ad-hoc Network (MANET) with its unique and special characteristics is prone to a host of Security threats from within and outside the network. In an ad hoc wireless network, the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among them as a group [12]. A mobile ad hoc network is a self – organizing system of mobile nodes that communicate with each other via wireless links with no infrastructure or centralized administration such as base stations or access points. A node in a MANET operates both as hosts as well as routers to forward packets to each other. MANETS are suitable for applications such as military, emergency rescue and mining operations. Among all the research issues, security is an essential requirement in ad hoc networks. Compared to wired networks, MANETS are more vulnerable to security attacks due to the lack of a trusted centralized authority, easy eaves dropping because of shared wireless medium, dynamic network topology, low bandwidth, battery power and memory constraints of the mobile devices. The security issue of MANETS in group communication is even more challenging because of multiple senders and multiple receivers. Factors affecting security are group type, group size, member (node) characteristics (power, storage, availability), membership dynamics, membership control, number and type of senders, volume and type of traffic and routing algorithm used [5].

Ad hoc wireless networks are defined as the category of wireless networks that are capable of operating without the support of any fixed infrastructure and nodes communicate directly between one another over wireless channels[12].

1.2 Benefits of Ad-hoc Network

1.2.1**.** Fully self-organized MANETs can be informally visualized as a group of strangers, people who have never met before, Coming together for a common purpose. These people have no prior relationships and share no common keying material on their nodes. Users therefore have to establish security associations between themselves, after network formation [11].

1.2.2. Mobile ad-hoc network provide wireless devices that can move freely in the network and cooperate to send packets on one another [1].

1.2.3. MANET provides the security on key Management in which the key management for group communication is to solve the most critical security technology of MANET security.

1.2.4. Wireless network has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, flexibility, mobility, reduced cost-of-ownership, and scalability. Wireless network have some security threats, in which anyone who use it or intend to use it should be aware.

1.3. Issue in Mobile Ad Hoc Networks

Security is a fundamental issue that needs resolution before ad hoc networks will experience large scale deployment. Vehicular ad hoc networking is a good example of a MANET application with some serious security implications failure of the security mechanisms may result in the loss of human life.[11].

The various security issues are:

- How to create secure key in key management**.**

After key creation some keys must be omitted from key pool to achieve a group of trustworthy keys. Length, randomness, creation method, and lifetime of generated keys are main important items in key issuance (or generation) process [6].

- How to initialize key distribution which is second step of key management

Second difficulty rises from key distribution which is second step of key management. Key distribution is process of spreading generated key among all nodes going to use the key to make secure session for safe data transferring. First-time key distribution is second issue of key management process. Some methods today exist for secure first time key distribution over insecure communication facilities and the most common way is establishing secure channel between key generators [7].

- How to inform all nodes that issued key is not valid afterward for session use.

Last process of key management is informing all nodes that issued key is not valid afterward for session use. It again requires consuming time and resources to inform all nodes that last key no more is valid. Also after nodes became aware about revoked key, generating and distributing a new key is required again [4].

1.4. Key Management

A keying relationship is the state where in 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. In summary, key management integrates techniques and procedures to establish a service supporting.

1. Initialization of system users within network.

2.Generation, distribution and installation of keying material.

3. Control over the use of keying material [11].

2. Proposed Work

Our aim is to develop a system that deals with the key management so that security are increase when data are transfer from source node to destination node through various intermediate node in the network so we are using the IGKM (Incremental Grouping Key management) algorithm .In proposed work the source node and some intermediate node will encrypt the message and only destination node is responsible for decrypting the message multiple time to get original message.

2.1 Architecture and Flow of Key Management

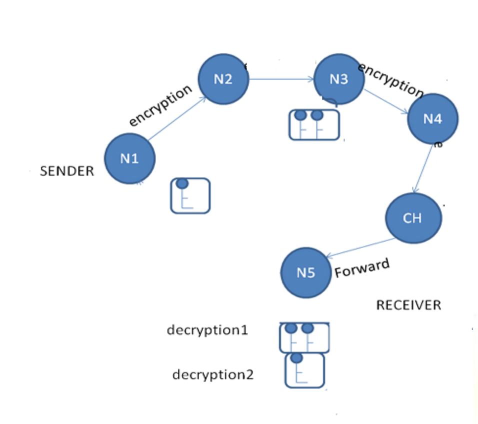


Fig 1. System Architecture of Key Management

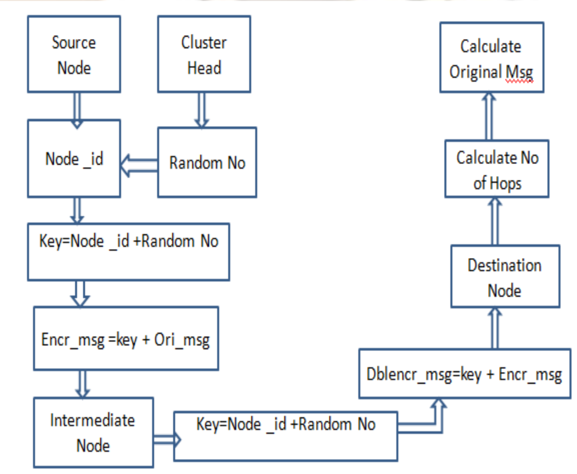


Fig 2. Flow of Key Management

System Architecture of Key Management includes the following processing:

1. Node 1 wants to send the message to Node 5 ,so N1 generate the key using the code and its id (key= node_code+ node_id).

2. Key add with the plaintext (encry_msg = key+ plaintext) and forward to the next node which is not the destination node.

3. Node 2 only forwards the encrypted message because every node is not responsible for encrypting or decrypting the message.

4. Again Node 3 generate its key using code and its own id then again adds it with the encrypted message which is coming from Node2. This process is repeated until the message is not reach at the destination.

5. The destination node counts the number of hops and count how many number of message is encrypted and according to that destination node will decrypt the message.

6. The Cluster Head is responsible for broadcasting the random number to all nodes in the network

2.2 Incremental Grouping Key Management (IGKM)

The Sender node wants some random number for that Sender node request to the Cluster Head and Incremental Grouping Key Management (IGKM) algorithm works in two phase first is Encryption phase and second is Decryption phase which work as follows:

2.2.1 Encryption Phase:

1. Cluster Head broadcast the random number.

2. Every node has unique identification number (node_id).

3. Now to generate the key the secret code is added with the node_id and key is generated.

4. Now to send message at the destination message will pass through number of intermediate nodes. So the message must in encrypted form.

5. To encrypt the message the key is added with message and send to next node.

6. At next node from step 3 to step 5 same procedure follows and message will encrypted multiple times .

2.2.2Decryption Phase:

1. Destination node have a random number. Then it calculate the number of hops

2. Then using this random number and hops destination node calculate the original message from multiple encrypted message.

3. SIMULATION RESULT

The node is constructed using NS2 simulator. NS simulator is based on two languages an object oriented simulator, written in C++, and OTcl (an object oriented extension of Tcl) interpreter, used to execute user's command scripts. A simulation script generally begins by creating an instance of this class and calling various methods to create nodes, topologies, and configure other aspects of the simulation.

As the nodes are organized in this security scheme, the nodes exchange keys and data only with its authenticated neighbors. This avoids expensive global rekeying operations when the membership in the network changes or when the network is partitioned. Figure 2. is a simulation output of wireless nodes when they are created and Figure 3. is a simulation output of wireless nodes when they transfer the packet between nodes that are plotted on NAM Figure 4 represents the simulation output of the throughput of the packets.

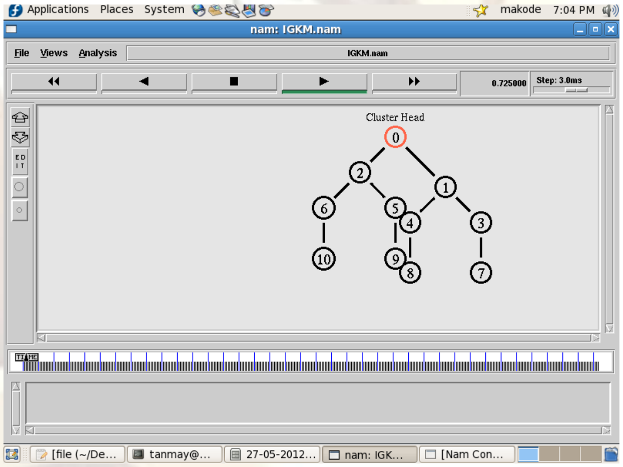
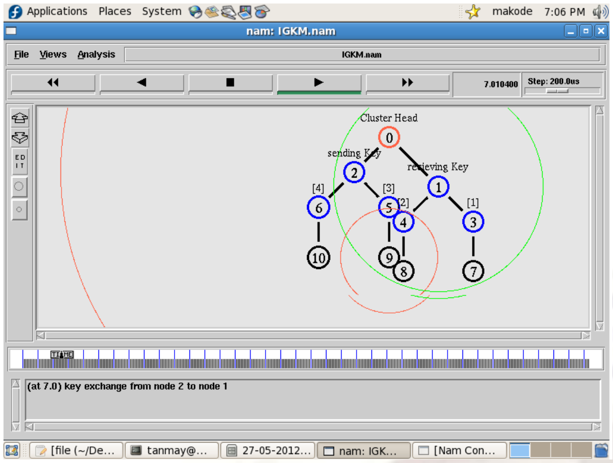
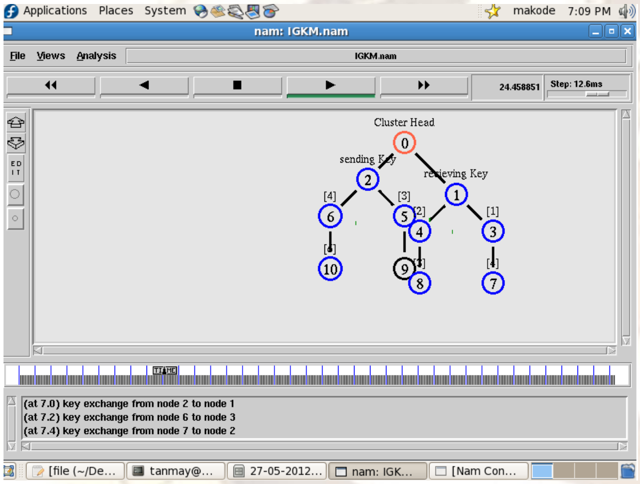


Fig.3 Cluster Based Scenario



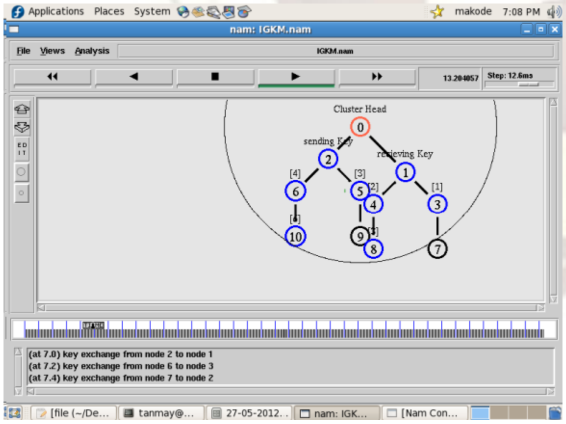
```
(at 7.0) key exchange from node 2 to node 1
```

Fig 4. Key Sending



```
(at 7.0) key exchange from node 2 to node 1
(at 7.2) key exchange from node 6 to node 3
(at 7.4) key exchange from node 7 to node 2
```

Fig 5. Packet transfer between nodes



```
(at 7.0) key exchange from node 2 to node 1
(at 7.2) key exchange from node 6 to node 3
(at 7.4) key exchange from node 7 to node 2
```

Fig 6. Broadcasting

4.CONCLUSION & FUTURE ENHANCEMENT

As the applications of mobile ad-hoc networks gain more ground, security issues becomes a hot research topic. This discussed the new Incremental Grouping Key management (IGKM) algorithm which is suitable for the key management.

proposed technique addresses the network security Issues. Besides, the technique uses a key system, and consists that define how keys are distributed, added, and updated during the life time of the network.

In real time application that relies on wireless communication has a big issue that is network security and authentication. Therefore, providing security and authentication is important as much as providing network connection to the user. This is the major concern for most of the network service providers today and hence data encryption and proper key management techniques are very critical in enhancing the security .Future work may concentrate on cluster head that takes more some of responsibility to send secure message at the destination.

References

[1] K.Gomathi, B.Parvathavarthini," An Efficient Cluster based Key Management Scheme for MANET with Authentication" 2010 IEEE.

[2] WEI Chu Yuan," A Hybrid Group Key Management Architecture for Heterogeneous MANET" ,2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing.

[3] Mu Haibing, Liu Yun, Zhang Changlun," A Compossite Muticast Meanagement Scheme for MANET", 2006 6th Intertional Conference on ITS Telecommunications Proceedings.

[4] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor," Group Key Management in MANETs", International Journal of Network Security, Vol.6, No.1, PP.67–79, Jan. 2008.

[5] Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei," Random Key Assignment for Secure Wireless Sensor Networks", October 31, 2003,

[6] N. Vimala, Dr. R. Balasubramaniam," Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey ", IEEE April 2010.

[7] S.Vijayalakshmi, S.Albert Rabara, " Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP3 and NAWA",

International Journal of Computer Applications (0975 – 8887)Volume 16– No.7, February 2011.

[8 HaowenChan, AdrianPerrig, DawnSong,"Random Key Predistribution Schemes for Sensor Networks" .

[9] N. Suganthi, R. S. Mohana Priya, V. Sumathy," An Efficient and Dynamic Key Management Scheme for Mobile Ad hoc Networks" European Journal of Scientific Resear.

[10] D. V. Naga Raju, Dr. V. Valli Kumari and Dr. K. V.S.V.N. Raju," Efficient Distribution of Conference Key for Dynamic Groups" , International Journal of Computer Theory and Engineering,Vol.2,No.4,August,2011793-82.

[11] Johann van der Merwe," Key Management in Mobile Ad Hoc Networks", November 17, 2005.

[12] S. Sumathy, B.Upendra Kumar,"Secure Key Exchange and Encryption Mechanism for Group Communication in Wireless Ad-hoc Networks", Inter National journal on application of graph theory in wireless ad-hoc networks and sensor networks (Graph-hoc), Vol.2, No.1, march 2010.

[13] S.Sumathy and B.Upendra Kumar,"Secure key exchange and encryption mechanism for group communication in wireless adhoc network" International journal on application of graph theory in wireless ad-hoc network and sensor network(graph ad-hoc) ,vol.2, no.1,March 2010

[14] AldarC-F.Chan," Distributed Symmetric Key Management for Mobile Ad hoc Networks", IEEE INFOCOM 2004

[15], Yenumula B. Reddy,Rastko Selmic" Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach", ICN 2011 : The Tenth International Conference on Networks.