Secure Routing in Multicast Routing Protocol for Manet's

Amandeep chhabra
Department of Computer Science and Engineering,GIMT Kanipla.

Geeta Arora
Department of Electronics and Communication,GIMT Kanipla

Abstract - A Mobile Ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense. So, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints i.e. limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. Another term is Multicasting which is an efficient means to support key applications of mobile ad hoc networks (MANET) such as tele-conferencing . In Multicasting the message is transmitted from one node to multiple nodes.These applications require both high secure protections and efficiency guarantees even in the presence of mobility, random link error. The issue of security is important in routing protocols and the efficient key distribution should be implemented effectively. To implement Security in various routing protocols there are four key management approaches naming key Predistribution, Key transport, key arbitration and Key agreement. The Objective of the paper is to implement security to Multicast routing protocol using Group Diffie hellman(GDH) algorithm which generates keys for 1 to N nodes in same group and for more than one groups and then transmits the message securely by using that keys.

I.INTRODUCTION

A MANET[1] is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance,QoS/multimedia,andstandards/products. Currently, the routing, power management, bandwidth management, radio interface, and security are latest topics in MANET research.Our work is related to security.

II.SECURITY GOALS IN AD HOC NETWORKS

The security of communication in ad hoc wireless networks is important especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANET's[6] more vulnerable to digital/cyber attacks than wired networks.

The key attributes required to secure ad hoc network are:

1. *Confidentiality* ensures payload data and header information is never disclosed to unauthorized nodes.
2. *Integrity* ensures that message is never corrupted.
3. *Availability* ensures that services offered by the node will be available to its users when expected, i.e. survivability of network services despite denial of service attacks.
4. *Authentication* enables a node to ensure the identity of peer mode it is communicating with.
5. *Non-repudiation* ensures that origin of a message cannot deny having sent the message.

III.SECURITY CHALLENGES

Achieving securing performances in wireless ad hoc environment is a challenging task. Unlike the wire-line networks the unique characteristics of ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer architecture, insecure operational environment and shared broadcast radio channel, stringent resource constraints, roaming of nodes, highly dynamic network topology combined with lack of central authority and association, scalability and physical vulnerability[6].

Roaming nodes with relatively poor physical protection can be exposed to malicious attacks by compromised nodes. To reduce the vulnerability, which may be caused by compromised centralized entity, and to achieve high survivability, ad hoc network should have distributed architecture.

Dynamic topology and changeable nodes membership may disturb the trust relationship among the nodes. The trust may also be disturbed if some nodes are detected as compromised. Nodes in wireless ad hoc networks may be dynamically affiliated to different administrative domains. This dynamism could be better protected with distributed and adaptive security mechanisms.

Scalability is an important issue concerning security. Security mechanisms should be capable of handling a large network as well as small ones.

Resource availability (band-width, battery and computational power) in ad hoc networking is a scarce feature. Providing secure communication in such changing and dynamic environment, as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad hoc environments also allow implementation of self-organized security mechanisms.

IV.MULTICASTING

A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers. These applications include bulk data transfer (for example, the transfer of a software upgrade from the software developer to users needing the upgrade), streaming continuous media (for example, the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants), shared data applications (for example, a whiteboard or teleconferencing application that is shared among many distributed participants), data feeds (for example, stock quotes), Web cache updating, and interactive gaming (for example, distributed interactive virtual environments or multiplayer games such as Quake). For each of these applications, an extremely useful abstraction is the notion of a multicast: the sending of a packet from one sender to multiple receivers with a single send operation. Multicast[2] communication is an efficient means to support key applications of mobile ad hoc networks (MANET) such as tele-conferencing .These applications require both high secure protections and efficiency guarantees even in the presence of mobility, random link error. Characteristics of MANET, for example limited resources, dynamic topology, vulnerability to network congestion, challenge a secure multicast protocol that is suitable in MANET environment. Multicasting plays an important role in typical applications of ad hoc wireless networks, namely, emergency search and rescue operations and military communication [4].Multicast routing protocols can be classified as: Tree based multicast routing protocols: In tree based multicast protocols[4],there is only one path between a source –receiver pair . This tree-based concept is borrowed from the multicasting protocols in wired networks. Since efficiency can be achieved and robustness is not a critical issue in the stable wired network, most multicast methods are tree-based, either source- or shared-tree-based[9].The main drawback of these protocols is that they are not robust enough to operate in highly mobile environments. Tree based protocols can be classified into two types: source – tree based and shared – tree based protocols[4].In source tree based a tree is created by each source and has as many number of tress as source and in shared tree based there is single multicast tree for all sources. Mesh based multicast routing protocols: Multicasting routing protocols which provide multiple paths between a source-receiver pair are classified as mesh based protocols [4].

V.MULTICAST SECURITY

Multicast sessions may be described in terms of their membership. In general, a session is defined as either public or private. Both types are defined by the level of session access control required to receive or transmit data within the multicast group . Public sessions are typically encountered on the Internet Multicast Backbone (MBONE)[10] and are supported by the dynamic nature of multicast communications (i.e., knowledge of the multicast address is often encryption. In order to create a private session, access to the required session cryptographic key material should be restricted through a registration and authentication process. Only authorized users should be able to gain access to group key material and subsequently participate in the session. A secure multicast session is a private session with encryption of data content.

VI.ISSUES

Over the years, multicast has been the topic of many research, engineering, and deployment efforts. These efforts have continued to transform multicast into a technology that can be relied on by many applications.Previously Work has been done in reliability, manageability, scalability, quality of service, and ease of deployment. As these areas become more mature, there is increased potential for multicast[11] to be used as the underlying distribution mechanism for content distribution applications. Therefore, security in multicast content distribution is a concern. The maturity of multicast security solutions have the potential to enable the use of multicast for confidential and high-value content, and help spark the use of multicast by new applications. The lack of security obstructs a large deployment of this efficient communication model. This limitation motivated a host of research works that have addressed the many issues relating to securing the multicast, such as confidentiality, authentication, non-repudiation, integrity, and access control. Many applications, such as broadcasting stock quotes and video-conferencing, require data origin authentication of the received traffic. Hence, data origin authentication[12] is an important component in the multicast security architecture. Multicast data origin authentication must take into consideration the scalability and the efficiency of the underlying cryptographic schemes and mechanisms, because multicast groups can be very large and the exchanged data is likely to be heavy in volume (streaming). Besides, multicast data origin authentication must be robust enough against packet loss because most multicast multimedia applications do not use reliable packet delivery. Therefore, multicast data origin authentication is subject to many concurrent and competitive challenges, when considering these miscellaneous application-level requirements and features. In this article we review and classify recent works dealing with the data origin authentication problem in group communication, and we discuss and compare them with respect to some relevant performance criteria. The fundamental aspects of secure multicast secrecy, authentication, Encryption, and Data integrity are very important factors for evaluating a secure multicast scheme. We summarize those factors as following:

- Secrecy of routing information is very important for both of the payload data and the routing message headers. The transmission messages are encrypted and only member of multicast group can read the content of datagram.
- Authentication verify the identities of group member so that they may be authorized to create, send data to, or receive data from a group and guarantees all of the routing information and payload data that can be verified the sender who claims to be.
- Encryption ensures that eavesdroppers cannot read data on the network.
- Data integrity ensure that datagram has not been altered in transmit. A message could be altered because of the malicious attacks during the transmission time. Encrypting datagram with cryptographic key in transmit is one important way implementing multicast secrecy. Key mechanism ensure only group members can read datagram. Key also be used for authentication because only group member can generate encrypted multicast datagram. The most important issue in key management is how to generate key and distribute it.

VII.KEY MANAGEMENT ISSUES

The key management[13] for multicast requires quite a lot more traffic compared to the key management for unicast. First, the common group key should be distributed to each group member and all the senders. If the traffic should also be authenticated, each sender has to distribute their authentication key to all of the group members. Some multicast routing systems don't require that there is a group owner or a group originator (core router), so the key management scheme presented above won't work. A simple solution is to use a semi-permanent group key, which is used to generate temporary group keys used to encrypt traffic or authenticate messages. There are various kinds of attacks possible on adhoc networks as discuss in[6].Cryptography is one of the most common and reliable means to ensure security. It can be applied to any communication network[4].In cryptography the original information to be sent from one person to another is called plain text. This plain text can be converted into cipher text by the process of encryption. An authentic receiver can decrypt/decode the cipher text back into plain text by the process of decryption. The processes of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the key is to be kept secret to ensure the security of the system, it is called secret key. The secure administration of cryptographic keys is called key management[4].The four main goals of cryptography are confidentiality, integrity, authentication and non-repudation. There are two main cryptographic algorithms : symmetric key algorithms ,which use the same key for encryption and decryption and asymmetric key algorithms, which uses two different keys for encryption and decryption[4].Next comes is key management approaches which is to share a secret information among a specified set of participants. The main approaches to key management are[4] :

1. Key Predistribution:

As the name suggests key pre distribution involves distributing keys to all interested parties before the start of communication. once deployed, there is no mechanism to include new members in the group or to change the key.

2.Key transport:

In key transport system ,one of the communicating entities generates keys and transports them to the other members. It assumes that a shared key is already exists among the participating members. This prior shared key is used to encrypt a new key and is transmitted to all corresponding nodes. Only those nodes which have the prior shared key can decrypt it. This is called Key encrypting method (KEK)[4].

3.Key Arbitration:

Key arbitration schemes use a central arbitrator to create and distribute keys among all participants. Hence, they are a class of key transport schemes. There is a difference in distribution of public keys which belong to a public knowledge, and private (secret) keys which are shared by multiple entities. Private keys can be distributed through a pre-established secure channel or an open channel. Public keys are usually distributed through certificates. A certificate binds a public key with an entity.

4.Key agreement:

Most of key agreement schemes are based on asymmetric key algorithms. Key agreement is used when it is necessary for several parties to agree upon a secret key and its exchanges, used in later communications. In case of group key agreement, each participant contributes a part to the secret key. This involves high computational complexity. The most popular key agreement scheme is Diffie-Hellman exchange.

VIII.RELATED WORK

A lot of research has been done in the field of providing security to Multicast ad hoc networks[3][8][7][15] but all these research done does not fully fulfill the essential security in Manets.

Many Group diffie hellman protocols aim to distribute a session key among the multicast group members for a scenario in which the membership is static and known in advance. However these protocols are not well-suited for a scenario in which members join and leave the multicast group at a relatively high rate. As described by[3] formalization of group diffie hellman key exchange and the adversary capabilities is done. In the formalization, the players do not deviate from the protocol, the adversary is not a player and the adversary capabilities are modeled by various queries. These queries provide the adversary a capability to initialize a multicast group via set-up queries, add players to multicast group via join-queries and remove players from multicast group via remove-queries.

Another simple and efficient region based group key management scheme is proposed, simply called SERGK[8], for MANETs. The basic idea of SERGK is that a physical multicast tree is formed in MANETs for efficiency. Group members take turns acting as group coordinator to compute and distribute intermediate key materials to group members. The keying materials are delivered through the tree links. The coordinator is also responsible for maintaining the connection of the multicast group. All group members can calculate the group key locally in a distributed manner.

The 2-party Diffie-Hellman exchange was first proposed in 1976, there have been efforts to extend its simplicity and elegance to a group setting. The Authors of [14] discuss a useful DH-based multi-party key-generating technique for large static groups, called Group-DH. The principal of this protocol is simple: the two involved nodes, *M*1 and *M*2, send one another a partial key to be used for the common key computation. *M*1 generates a random number $r1$ $(1 £ r1 £$ *p*), and sends a*r*1 to *M*2, such that a and *p* are constants known by each node. On the other hand, *M*2 generates a random number *r*2, and sends a*r*2 to *M*1. Thereby, each node could compute the common key, which is $ar1 \times r2$ This solution is based on discrete logarithmic arithmetic, and also relies on the agreement on the parameters a and *p* between the two nodes. Although it is simple and limited to two nodes' common key establishment, this protocol was used to design more sophisticated protocols.

IX.PROPOSED ALGORITHM

There are various kinds of attacks possible on adhoc networks as discuss in[6].Cryptography is one of the most common and reliable means to ensure security. It can be applied to any communication network[4].In cryptography the original information to be sent from one person to another is called plain text. This plain text can be converted into cipher text by the process of encryption. An authentic receiver can decrypt/decode the cipher text back into plain text by the process of decryption. The processes of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the key is to be kept secret to ensure the security of the system, it is called secret key. The secure administration of cryptographic keys is called key management[4].The four main goals of cryptography are confidentiality, integrity, authentication and non-repudation. There are two main cryptographic algorithms : symmetric key algorithms ,which use the same key for encryption and decryption and asymmetric key algorithms, which uses two different keys for encryption and decryption[4].The aim is to implement Key Agreement approach using Diffie hellman Algorithm for Multicasting protocol in which all the nodes in the network agree on the same key as said by the key agreement approach. For two nodes the algorithm has been implemented in[14].Our work has been extended to n-party communication in which n parties or nodes can participate in communication.

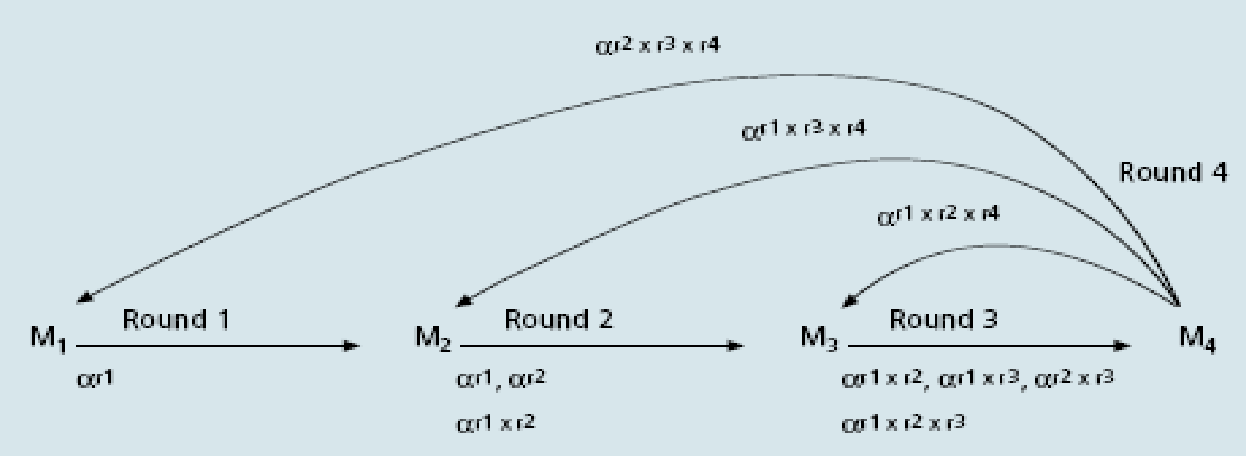
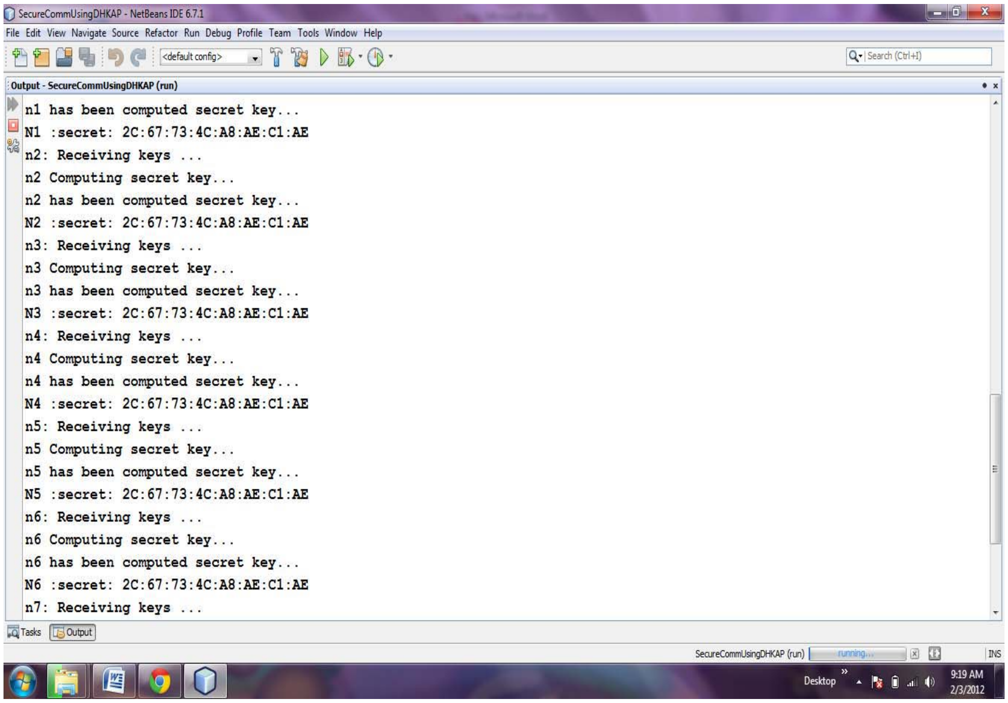


Fig Diffie Hellman Algorithm for 4-party Communication

The new protocol consists of *n* rounds, allowing *n* nodes to establish a common key. In the first *n* – 1 rounds contributions are collected from each node. In the first round, *M*1 generates *r*1 and computes $ar1$, which it sends to *M*2. In the second step *M*2 generates *r*2, computes $ar2$ and sends it to *M*3, along with a*r*1 and $ar1 \times r2$. This latter sends to *M*4 (after making the required computations) the third-round partial factors, i.e., $ar1 \times r2$, $ar1 \times r3$, $ar2 \times r3$, as well as the third-round partial key $ar1 \times r2 \times r3$. This process continues for each *Mi* (*i* < *n*). Upon the (*n* – 1)th round, the collector node *Mn* receives the (*n* – 1)th round partial factors, and the (*n* – 1)th round partial key, then it generates its random number and computes the final key *K*.4 in the last round.

The Algorithm and the method used to generate the keys for 4-party communication is used for n-party communication as we can see below in the figure.Four groups each having two nodes have been made statically and after the simulation of the network all the eight nodes will generate the same secret key as said by the key agreement approach which is implemented by Diffie hellman algorithm and then the network will ask for the group index to whom which we want to send our data or information.


SecureCommUsingDHKAP - NetBeans IDE 6.7.1
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
<default config>
Search (Ctrl+I)
Output - SecureCommUsingDHKAP (run)
Tasks
Output
SecureCommUsingDHKAP (run)
running...
INS
Desktop
9:19 AM
2/3/2012

```
n1 has been computed secret key...
N1 :secret: 2C:67:73:4C:A8:AE:C1:AE
n2: Receiving keys ...
n2 Computing secret key...
n2 has been computed secret key...
N2 :secret: 2C:67:73:4C:A8:AE:C1:AE
n3: Receiving keys ...
n3 Computing secret key...
n3 has been computed secret key...
N3 :secret: 2C:67:73:4C:A8:AE:C1:AE
n4: Receiving keys ...
n4 Computing secret key...
n4 has been computed secret key...
N4 :secret: 2C:67:73:4C:A8:AE:C1:AE
n5: Receiving keys ...
n5 Computing secret key...
n5 has been computed secret key...
N5 :secret: 2C:67:73:4C:A8:AE:C1:AE
n6: Receiving keys ...
n6 Computing secret key...
n6 has been computed secret key...
N6 :secret: 2C:67:73:4C:A8:AE:C1:AE
n7: Receiving keys ...
```

The snapshot shows the generation of keys for all the nodes in the network and all the nodes agree on the same secret key as stated by Diffie Hellman Algorithm and Key agreement approach.

As shown in figure below four groups each containing two nodes in each have formed and data will communicate through intermediate nodes.If we enter group index 0 then the message will transmit to only group i.e node N2 only.And,if we enter group index 1 the message will transmit to group 2 i.e nodes N3 and N4.The efficient distribution of keys between the nodes ensure secure communication between the nodes in the network.

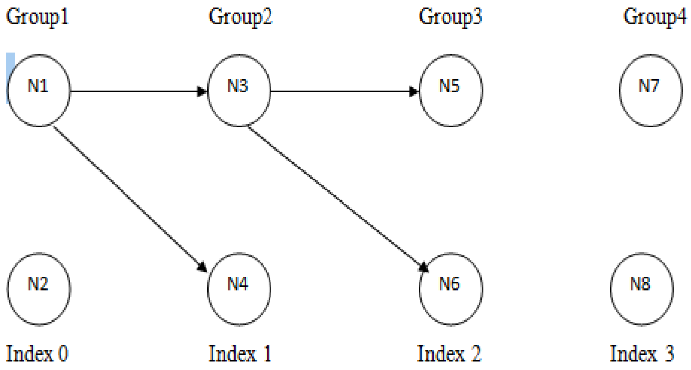
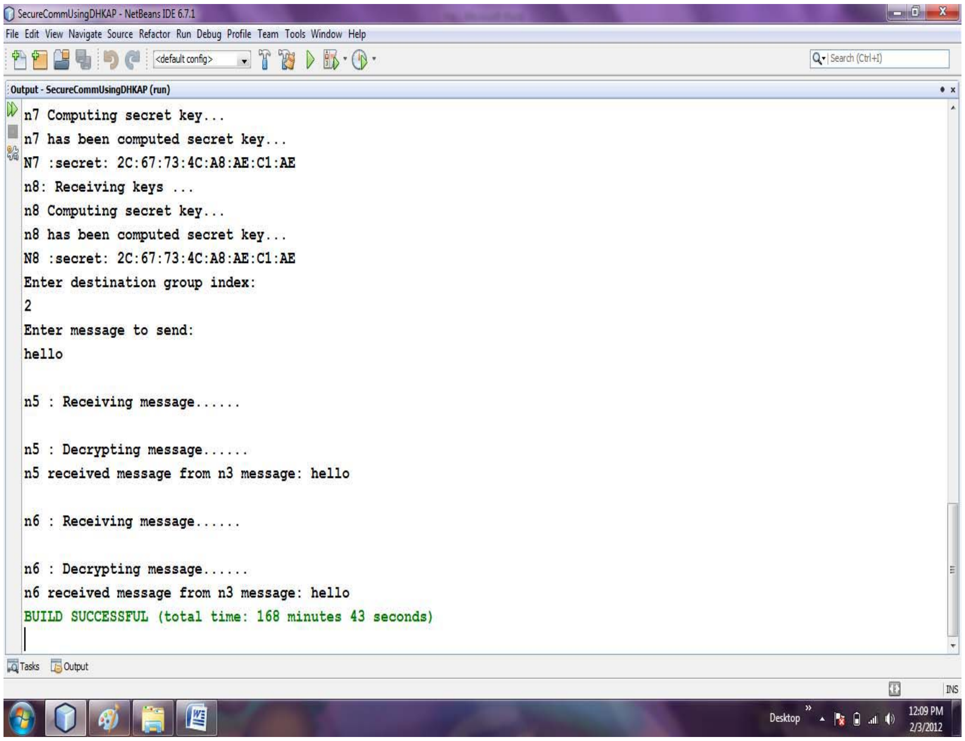


Fig Network of 4 groups transmitting message from N1 to N6.

In the above figure if we enter group index 2 then the message will transmit to N3 and N4, then to N5 and N6 through N3.The same is in the case if we want to communicate to N8 then the message will transfer through N3 to N5 and N6,then N7 and N8.The snapshot below shows the transmission of message “hello” to node N6. The same procedure is in the case of n-nodes. So, The model we propose transmits message to a group of nodes which is property of multicasting in a secured way by using Group Diffie Hellman algorithm.


SecureCommUsingDHKAP - NetBeans IDE 6.7.1
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
<default config>
Search (Ctrl+I)
Output - SecureCommUsingDHKAP (run)
Tasks
Output
INS
Desktop
12:09 PM
2/3/2012

```
n7 Computing secret key...
n7 has been computed secret key...
N7 :secret: 2C:67:73:4C:A8:AE:C1:AE
n8: Receiving keys ...
n8 Computing secret key...
n8 has been computed secret key...
N8 :secret: 2C:67:73:4C:A8:AE:C1:AE
Enter destination group index:
2
Enter message to send:
hello

n5 : Receiving message......

n5 : Decrypting message......
n5 received message from n3 message: hello

n6 : Receiving message......

n6 : Decrypting message......
n6 received message from n3 message: hello
BUILD SUCCESSFUL (total time: 168 minutes 43 seconds)
```

X.CONCLUSION

In the paper various issues related to Manet's and Multicasting are studied. The various problem areas in relation with Multicasting are explained .Various Key Management issues have been explained. Group Diffie Hellman(GDH) Algorithm is implemented statically with 3 groups and 2 nodes in each and can be increased upto n-nodes. The Message communicating between the nodes is communicating securely as all the nodes uses secret key to encrypt and decrypt message.

XI.FUTURE SCOPE

The Future Scope for Security in Multicast Routing is very large. The Implementation of the Algorithm can be done on a particular routing protocol. The Implementation can be done on any Simulator and implemented on a particular Multicasting protocol like MAODV.The number of nodes in the network are predefined that can be extended to dynamic environment in which number of nodes can be changed.

REFERENCES

[1] Rashid Hafeez Khokhar, Md Asri Ngadi , Satria Mandala ," A Review of Current Routing Attacks in Mobile Ad Hoc Networks".

[2] Jiejun Kong, Yeng - zhong Lee, Mario Gerla ," Distributed Multicast Group Security Architecture for Mobile Ad Hoc Networks", Department of Computer Science University of California Los Angeles, CA 90095.

[3] Emmanuel Bresson, Olivier Chevassut & David Pointcheval ," Provably Authenticated group diffie hellman key exchange – the dynamic case".

[4] C.Siva ram murthy , B.S.Manoj ," Adhoc wireless networks architecture and protocols".

[5] N. Vimala, B. Jayaram, Dr. R. Balasubramanian , " Efficient group key management protocol for region based Manets".

[6] Ajay Jangra, Nitin Goel, Priyanka& Komal Bhatia," Security Aspects in Mobile Ad Hoc Networks".

[7] Xiang-yang li,Yu wang,ophir Frieder ," Efficient hybrid key agreement protocol for wireless adhoc networks".

[8] Elizabeth M.Royer , Charles E Perkins," Multicast operation of the adhoc on demand distance vector routing protocol".

[9] Shuhui Yang , Jie Wu," New Technologies of Multicasting in Manet ".

[10] Shuhui Yang , Jie Wu," New Technologies of Multicasting in Manet ".

[11] Paul Judge and Mostafa Ammar , Georgia Institute of Technology , " Security Issues and Solutions in Multicast Content Distribution: A Survey".

[12] Yacine Challal , Hstem Bettahar , and Abdel madjid Bouabdallah, Compiegne University of technology," A Taxanomy of multicast data origin authentication: issues and solutions in proceedings of ieee communications third quarter 2004,volume 6,no 3.

[13] M .V.Vijaya Saradhi , BH.Ravi krishna," A group key management approach for multicast cryptosystems " in Journal of Theoretical and Applied Information Technology.

[14] Vankamamidi S. Naresh , Nistala V.E.S. Murthy," Diffie-Hellman Technique Extended to Efficient and Simpler Group Key Distribution Protocol " in International journal of computer Applications august 2010.

[15] Wenjing Lou, Wei Liu , Yuguang Fang," SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks" in ieee infocom 2004.