Authenticating and Securing End-to-End Communications through Encrypted Key Model for Mobile Ad Hoc Network

M.B. Mukesh Krishnan
Research Scholar
Sathyabama University
Chennai – 600119, India

Dr. P. Sheik Abdul Khader
Professor and Head
Department of Computer Application.
B.S. Abdur Rahman University, Vandalur,
Chennai-600 048,India

ABSTRACT
Securing End to End Communication in mobile ad-hoc networks are difficult than the ones for fixed, while the security requirements are same namely availability, confidentiality, integrity, authentication and non repudiation. The difference occurs due to system constraints in mobile devices and frequent topology changes in the network. System constraints include low power architecture, small memory, limited bandwidth and limited battery power exhaustion. This paper is focus on the design and analysis a security solution for Mobile ad – hoc Network (MANET) through the authentication data encryption model. The model is analyzed under various attacks and the result shows that the proposed model is highly resistant to attack in end to end communication.

Keywords
Mobile Ad hoc Network , End to End Communication , Attacks

1. INTRODUCTION
A MANET (Mobile Ad Hoc Network) is a communication network characterized by the absence of any fixed infrastructure. In parallel to the deployment of ad hoc networks, the last decade saw the constant development of multicast services within the Internet. Multicast transmission is an efficient communication mechanism for group oriented applications, such as video conference, interactive multiparty games and software distribution. The combination of an ad hoc environment with multicast services, induces new challenges towards the security infrastructure to enable acceptance and wide deployment of multicast communication. Indeed, several sensitive applications based on multicast communications have to be secured within ad hoc environments. To prevent attacks and eavesdropping, services among which authentication, data integrity and data confidentiality need to be provided.

The main challenges that need to be addressed when designing security solutions for MANET are:

1. Lack of infrastructure
2. Resource-constrained nodes and communication links
3. Node mobility and network dynamics
4. Likely node compromise

The most suitable solution to overcome these challenges is through establishment through data encryption model. This model is responsible for the generation and the distribution of the encryption keys all group members. This key is used by the source to encrypt multicast data and by the receivers to decrypt it. Thus, only authenticated members are able to receive the multicast flow sent by the group source.

2. AUTHENTICATION OF ENCRYPTED KEY MODEL TO SECURING END TO END COMMUNICATION
Securing End to end communication is a fundamental issue with Mobile ad hoc networks and certainly security is an essential problem for all networks. With a strong infrastructure this problem could be diminished however, with mobile nodes and wireless links, it is not easy to provide such a secure communication. Since mobile ad hoc networking is generally on air communication, it is also open for eavesdropping or interference. A mobile ad hoc network should be secured from these kinds of attacks.

The paper proposes two scenario to achieve them

- Encrypted secured key exchange model
- Key distribution model for inside and inter group communication

Encrypted secured key exchange model work in end to end communication and key distribution model inside group achieves inside group and inter group key distribution model achieves inter group the whole model achieves entire communication.

2.1 Encrypted secure key exchange model
In this model when a new key is passed after encrypting with previously known key is decrypted at receiver side. The procedure for encryption and exchange of key is exactly the issue here. This model has an authentication center which collects the network information and malicious/misbehavior activity of the node by examining the node traffic and the frequency of transmission, it authenticates the not only the node belong to the group but also issues a certificate along with the session information and secret key to transmit between sender and receiver. The encrypted secure key exchange is achieve by encrypting the key and send it with a key exchange scenario same as regular key exchange model, but it is repeated with a secure code and the code is encrypted and send to

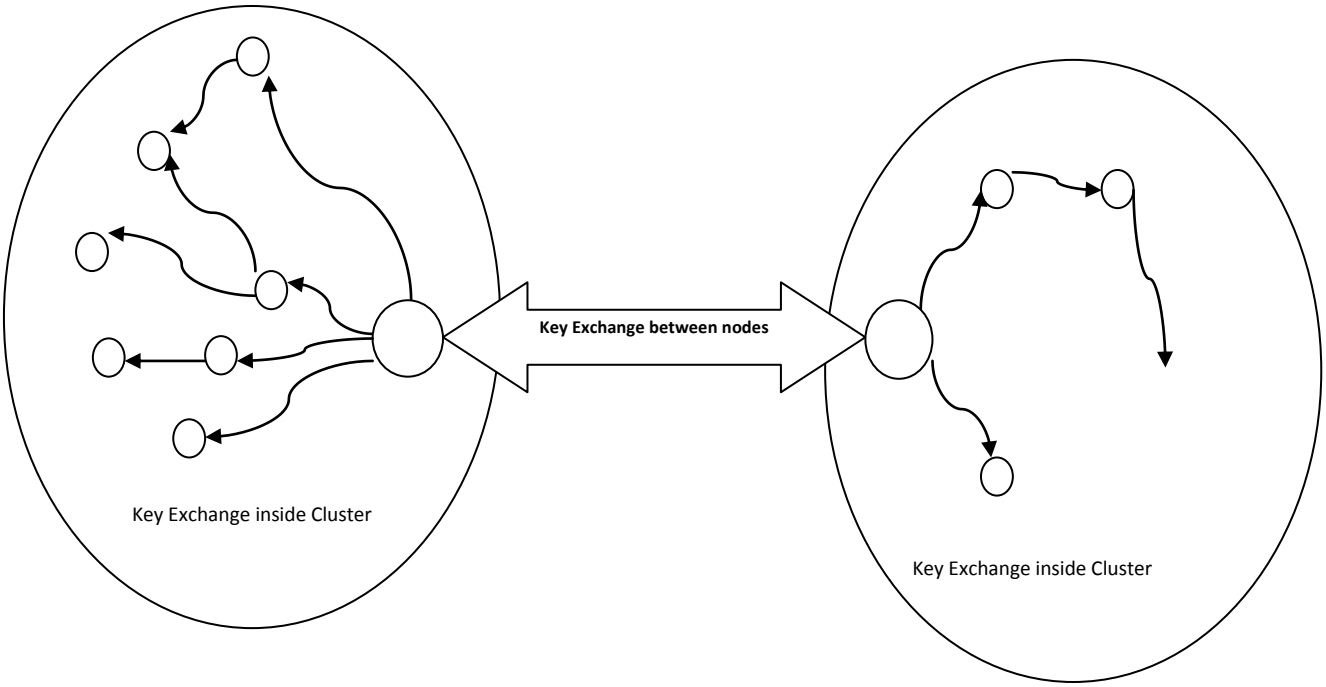

Fig. 1 Key distribution model for inside and inter group communication

the receiver end along with the data. The receiver decrypt the data using the key and secure code is obtained along with the receiver key and secures code, the receiver should use certificate of authentication issued by authentication center in the network to decrypt the data.

2.2 Key distribution model for inside and inter group communication

Key distribution is taken place in various steps as follows
Step 1: Group formation of nodes
Step 2: Distribution of public key inside group
Step 3: Registration of node with cluster/group head
Step 4: Registration of node with authentication center
Step 5: Generating trust hold for communication between authentication center and node
Step 6: Repeat step 1 to step 5 when new node enter the group.
In the key distribution model we have two scenarios.

Scenario 1 – Key distribution between the nodes present inside the same group
Scenario 2 – Key distribution between the nodes present in two different groups.

In scenario 1 the node cluster are communicated between each other and there is no need to have any extra process than the encrypted secure key exchange model because authentication center present inside the group via the cluster head and the authentication center the key distribution will take place.
In scenario 2 the cluster heads of adjacent cluster will communicate between each other and communicates the authentication key, the cluster head also act as a authentication center and accelerates the communication to other communication clusters. The figure 1 shows how the cluster head act as authentication center and distributes the certificates inside and the between two groups. The success of the scenario is based on the threshold level of the authentication center.

3. COMMUNICATION MODEL

Following steps describe the communication flow between various nodes

1) New member registers and get authentication certification id for communication from authentication center
2) Sender broadcast the request to communication request
3) Receiver sends back acknowledgement.
4) If the receiver present in other group, group head sends back acknowledgement
5) Authentication center gives its authentication to the new member securely.
6) All above procedures are repeated when communication is requested

In each step from 2 to 5, our model defines "time out" value (e.g. 5 seconds) in order that new member cancels the communication; because it may happen that the node leaves from the network within the communication. When new member cancels the communication, it restarts communication with another key just after the time out.

4. IMPLEMENTATION

The proposed security measures were implemented using NS/2 as the simulator. The implementation part consists of following steps

- Creation of Node
- Setting Node Mobility
- Setting Security Pattern
- Creating malicious nodes
- Traffic creation

5. CREATION OF MALICIOUS NODES

Out of N nodes in the network 20% of the nodes were made malicious. In the network the malicious nodes are the nodes, which generate more of Route Requests than the normal value . These nodes were selected randomly. Normally the nodes generate route requests when data is present in their buffer and a proper route to the destination is not known. The randomly selected nodes were made to generate more number of route requests irrespective of their buffer and route discovery status. Each malicious node in the network generates a variable number of route requests to another randomly. The above said security measures operations are done cooperatively by a group of nodes when the confidence percentage level is very low. When the confidence level is very high the alleged node is directly purged from the network increasing the efficiency of the model and thereby decreasing the time taken for the detection and response modules incorporated. Thus the mal nodes are identified through the proposed security model.

6. EXPERIMENTAL SETUP

NS/2 version 2.34 software is used for the model implementation. The simulations were based on 500 by 500 flat space scattered with 50 wireless nodes. The nodes move from a random starting point to a destination with a speed ranging from 0-20 m/sec as the destination is reached another destination be targeted after a pause time. The MAC layer used for simulations is IEEE 802.11. The Intrusion detection and intrusion response model are incorporated. Traffic sources used are Constant Bit Rate (CBR) with each data packet 512 bytes long. 10 nodes in the network were made the sources and the destinations were spread randomly across the network. The mobility model used is random waypoint in rectangular field. Duration of the simulations is 500 seconds. Separate simulations were performed for the malicious node created in the network and after the implementation of the end to end environment based response model.

7. MOBILITY

For different ranges of mobility the graph is plotted. The system performance has been observed in the presence of malicious nodes and measured. The performance enhancement is due to the implemented model. In the simulation misbehaving node generates false route requests. So the corresponding packet delivery decreases for it.

8. EVALUATIONS

We evaluated the model by average group formation time, authentication key distribution which includes the public key, secure key and authentication issued by the authentication center. All tests have been done with the following set of parameters:

- 1024 bits key
- Number of pauses between transmission : 5, 10 and 20
- Bit strings length for communicationl: 20
- Public key length: 1024 bits

According to this experiment, while many rounds in the communication procedure may slightly take longer response, the average exchange time minimize its performance impact. In fact, based on our analysis, the exchange procedure takes less than 10% of the total response time, yet data transmission over wireless link possesses the highest ratio. Now measuring the message size of the key exchange is additional important criteria. The experiment shows the total message size transmitted in the secret key acquisition procedure. We could then estimate the data communication cost of our communication. Actually the key exchange for approximately 90% of the total message size, and it would be proportionally increased to the threshold value. Reducing rounds of communication will clearly reduce the total time, but trade-off exists between the communication robustness and performance.

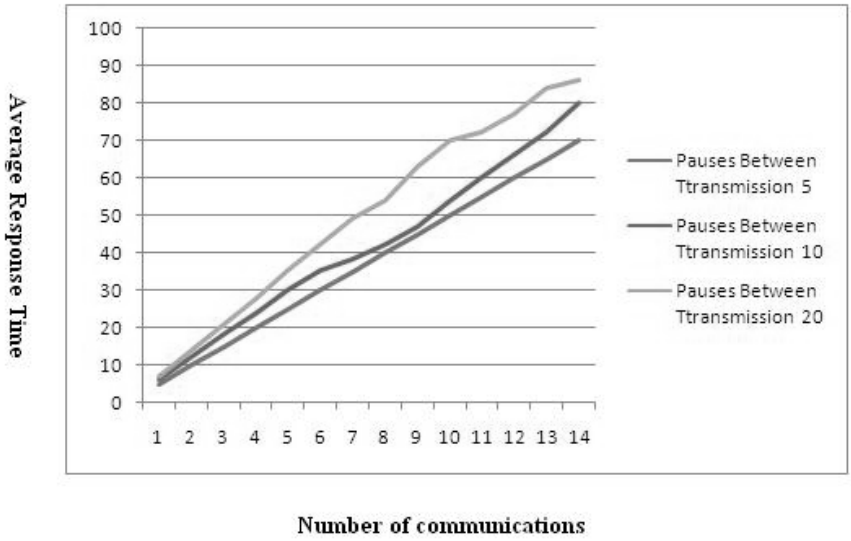

Fig. 2 Average Response time for communication

9. CONCLUSION

The End to End Communication in mobile ad-hoc networks are analyzed a security solution through the authentication data encryption model. The model is analyzed under Masquerade attacks , man in the middle attacks , Rollback attack attacks and Replay attacks and the result shows that the proposed model is highly resistant to attack in end to end communication.

10. REFERENCES

[1] Tseng, Y. Min., A heterogeneous-network aided public-key management scheme for MANETS. Published in Wiley InterScience, Int. J. Net. Mgmt v.17: pp.3–15 2006

[2] Pirzada, A., Mc Donald, C.: Kerberos Assisted Authentication in Mobile Ad-hoc Networks, the 27th Australasian computer science conference 2004

[3] Varadharajan, V., Shankaran, R., Hitchens, M.: Security for cluster based ad hoc networks. Computer Communications; 27(5): 488–501. 2004

[4] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N.: A Survey of Routing Attacks in Mobile Ad Hoc Networks. IEEE Wireless Communications, 85–91 October 2007

[5] Panaousis, E.A., Nazaryan, L., Politis, C.: Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications. In: ICST Mobimedia 2009, London, UK, September 7-9,(2009

[6] Mahajan, V., Natu, M., Sethi, A.S.: Analysis of Wormhole Intrusion Attack in MANETs. In: Proc. IEEE Military Communication Conference,2008.

[7] Advanced Encryption Standard: J¨org J. Buchholz http://buchholz.hs-bremen.de December 19, 2001

[8] vocal Technologies, Ltd. http://www.vocal.com

[9] SEC 1: Elliptic Curve Cryptography: Certicom Research Contact: secg- talk@lists.certicom.com September 20, 2000 Version 1.0

[10] Kristin Lauter: The Advantages of Elliptic Curve Cryptography for wireless Security, Microsoft corporation, IEEE Wireless Communications • February 2004

[11] Elisabeth Oswald: Introduction to Elliptic Curve Cryptography, Institute for Applied Information Processing and Communication A-8010 Inffeldgasse 16a, Graz, Austria, July 29, 2005.

[12] RFC 3588. Diameter Base Protocol, P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, September 2003.

[13] RFC 3748. Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Lefkowetz, June 2004.

[14] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems Based on Pairins, The 2000 Symposium on Cryptography and Information Security, 2000.

[15] A.O. Salako. Authentication in Ad hoc Networking, In Proceedings of London Communications Symposium 2002 .

[16] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks, International Conferenc on Network Protocols (ICNP), 2002.