Volume No:4, Issue No:10 (March-2019)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Trust Establishment for Transmitting the Data Securely Using Hash Key in MANETs

M.Chandu Jagan Sekhar
Department of Computer Science and Engineering
NS Raju Institute of Technology, Visakhapatnam, Andhra Pradesh-531173, India.

K.Neelima
Department of Computer Science and Engineering
NS Raju Institute of Technology, Visakhapatnam, Andhra Pradesh-531173, India.

N.Rajesh Varma
Department of Computer Science and Engineering
NS Raju Institute of Technology, Visakhapatnam, Andhra Pradesh-531173, India.

ABSTRACT

Mobile Ad-Hoc NET works also called as wireless Ad-hoc networks that usually have a routable networking environment. In MANET the mobile nodes should use remaining nodes and trust them in transmission of information. By the deficiency of central control the very next node may have a chance of dropping the packets due to malicious node. The one section that has to be more secured is MANET. MANET is very simple and adaptive so that, it is broadly used in emergencies, communications and mobile conferences. MANET consists of set of nodes in which all the nodes co-operate with each other for routing of packets. All the nodes which are configured are trusted. Nodes send or share the information with them using the data centre. During the transferring of information if any malicious node is detected, that node is eliminated. By removing the malicious node data is secured and kept confidential. Although misbehaviour of node is common here wireless Ad-hoc networks are used to misroute the sensor nodes that are in the malicious node cluster. HMAC is a message authentication code which involves cryptographic hash function and a secret key. It is used to check both authentication of message and data integrity. For calculation of HMAC we use algorithms like SHA-256 and SHA-3, which results in the MAC algorithm. The MAC algorithm is termed as HAMC-X, here X is hash function. So by using both hash key and SHA algorithms a trust is established between the nodes.

Key Words: ***MANET, NS2, Ad-hoc routing, HMAC, SHA.***

1. Introduction

Wireless ad-hoc networks are used to provide security for the information during data transmission.Manet is self ordered and infrastructure less network. In Manet architecture every node acts as a router and also as an end host.Manet also has dynamic topology architecture. Due to this architecture it promotes mobility. A mobile Ad-hoc network is autonomous systems of mobile nodes and it is a kind of wireless network dynamically create a specific network to interchange data without utilising any precedent network. [1] A wireless network consists of several nodes. In general, we have two types of nodes. They are:

- Genuine nodes
- Uncooperative nodes

Genuine nodes are those which have identity and there will be no harm generated to the data during transmission. Uncooperative nodes are those which have no identity and are unsecured nodes. They try to attack the secured nodes and may lead in transmitting false information [2]

MANETs has two types of uncooperative nodes. They are: malicious nodes and selfish nodes. The malicious

Cite this article as: M.Chandu Jagan Sekhar , K.Neelima & N.Rajesh Varma, "Trust Establishment for Transmitting the Data Securely Using Hash Key in MANETs", International Journal of Research in Advanced Computer Science Engineering, Volume 4 Issue 10, 2019, Page 52-57.

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

nodes cannot follow a protocol and therefore can be harmful nodes, and will try to harm and attack the system. The errors generated by the nodes need to be specified at different partitions. As an example, using a reputation system to identify the fault system, and later avoid those nodes. On other hand a selfish node is a logical node which is impartial to enlarge its welfare, where we can be explained as the advantage of the actions performed minus the total amount of its reactions. Since sending a message will suffer the amount, a fault node will have encouragement for doing. Existing trust ways for MANETs are generally divided into data-oriented, entity-oriented and hybrid trust models depending upon the calling target, which can be fault entities or fault messages or both of them attacks addressing availability, will be the most harmful as they affect safety- critical situations. And in this project we describe the various MANET security efforts and we then classify the existing threats.[3] Mobile Ad Hoc Network is a multi hop network formed by a group of wireless mobile nodes that transfers data packets from one to other for communication.

For establishing routes between any two nodes which are farther than one hopped special protocols are designed. So in the same way we use mainly three types of Ad Hoc protocols like:

- Pro Active protocols-DSDV, CGSR, OLSR.
- Reactive protocols-DSR, AODV, CBRP.
- Hybrid protocols-ZRP.

There are also two types of attacks in MANETs like active and passive attacks. In the same way there are also two types of hash functions like keyed and UN keyed hash functions. The characteristics of these hash functions include high possibility of collision resistance and also security. And also hash functions like MAD and SHA-1 are used in software industries for verification of many files and security. These has functions are designed based on the logical operations. Structural topologies of the algorithms are little bit difficult which leads to complicated processing. Coming to AODV protocol, it is a distance vector routing protocol. It is reactive protocol. AODV uses numbers to delete the problem of loops. When a node need to transfer information with the other node whose route is not known, it uses RREQ packets. Each packet has an ID, both start and end node addresses and also sequence numbers.

- The ID is used to identify the RREQ packet.
- Sequence numbers give the information about control packet.
- Hop count is used to maintain the number of nodes between the source and destination.

AODV is used to secure the route discovery using integrity and authentication. To secure the AODV messages we use:

Digital signatures for authentication

These are used to protect the integrity of data in RRQE/RREP messages. When request is received from destination it will reply with RREP only if it satisfies the AODV requirements. When a node receives the RREP it checks the signature

Hash chains for hop count data

It are formed by one way hash function. Every time when a node is sends a message it performs various operations. In the same way always when a node receives a message it also performs various operations.

2. Experimental Study

In this project the feasibility is analyzed with a general plan and some cost estimates. This study is used to protect that the proposed system is not a problem for project. To do the experimental study some analysis of the requirements is important. We mainly consider three keys in this analysis. They are:

- ECONOMIC
- TECHNICAL
- SOCIAL

2.1 ECONOMIC:

It is done to check the economic impact on system. The amount of fund is limited which can be invested in research and development of system. The funds are

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

justified. The system was well developed within the given funds because most of technologies are freely available.

2.2 TECHNICAL:

This study is totally based on the practical requirements of the system. The developed system should not have heavy demand over technical resources and must have finest requirements like minimal changes are required to implement.

2.3 SOCIAL:

It is to check how the user accepts the system. This study is used to train the user so that he can work on the system efficiently. The user must understand the necessity of the system rather than afraid of it.

2.4 ARCHITECTURE

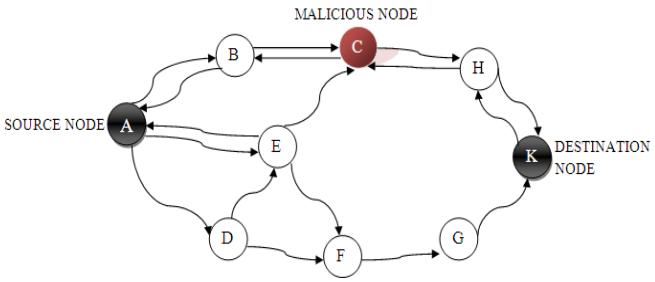

Fig1: Node Representation

3. Description

Here we have three main sections. They are:

- Sensor node
- Aggregate node
- Data centre

SENSOR NODE:

It is used in selection of nodes and aggregators. It also views the aggregated groups (i.e., clusters). Then it updates the complete file and transmits the data file.

AGGREGATOR NODE:

It consists of group of sensor nodes and shows the data that is collected.

DATA CENTER:

It is used to receive the files and show the complete details of the files. Downloading of files is also done using data centre.

4. Implementation

In this project Network simulator 2 is used. NS is chosen as the simulator because of the range of features it provides and partly because it has a freely available code that can be modified and extended. There are different versions of NS2 tool. The latest version is ns-2.1b9a and while ns-2.1b10 is under development. NS2 is an Event driven simulator. Goal of NS2 is to support networking, research and education. NS2 is used for designing new protocols, comparing different protocols and traffic evaluations. It is also freely distributed and open source.

Initially network is built .A cluster of nodes with an aggregator are generated and each cluster consists of a group of nodes with a colour code. Data centre is present in the centre of all clusters for transmission data from data centre to the aggregators. From each aggregator data is again send to the nodes. Now while transmission of the data, if any malicious node is detected that node is deleted and the remaining nodes in the cluster are joined to the nearest cluster. By removing the malicious node data is secured and kept confidential. Data is transferred from data centre to aggregators. Each aggregator consists of cluster of nodes. Using hash key if there is any unauthenticated or malicious node, it is detected and that node is removed from the particular cluster. All the aggregators send the beacon messages to all the sensor nodes. Aggregator sends the authentication message to cluster members i.e., nodes. After verifying all the aggregators, if there is an unauthenticated one, that aggregator is removed. So the nodes in the unauthenticated aggregator will join to the nearest cluster. Then all the aggregators send the sensor node report to the data centre. After the data is received, the data centre sends the acknowledgement message to the authenticated aggregators. Then all the aggregators collect the data from the sensor node. Data centre

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

verifies the aggregated data with the ID based signature. Aggregator sends the collected data to the data centre. Based on the above process a graph is generated based on the delivery of the packet. The delivery of packet explains about the packet delivery code. And also the process tells about how much energy is consumed based on the information transferred from the nodes. By the above output driven approach we came to know that how much efficiently security can be given to the nodes while transferring the information.

5. Results and Discursions

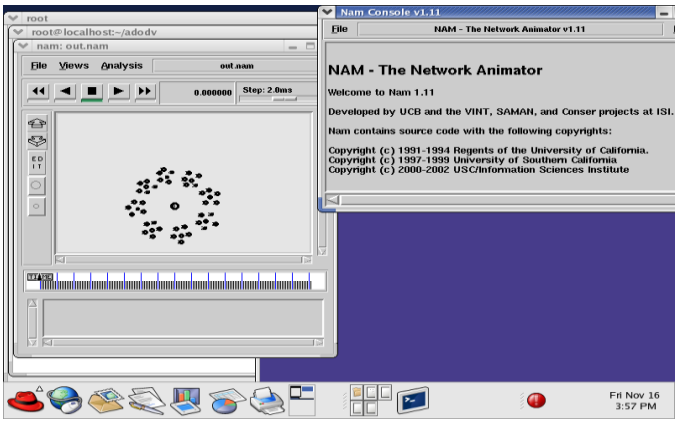

Fig 2:Building The Network

Initially network is built using the network animator. Here a cluster of nodes with an aggregator are placed. These entire clusters are built around a data centre. The data centre is responsible for the passing of data or information to all the aggregators. Then from those aggregators data is sent to the particular nodes of a cluster.

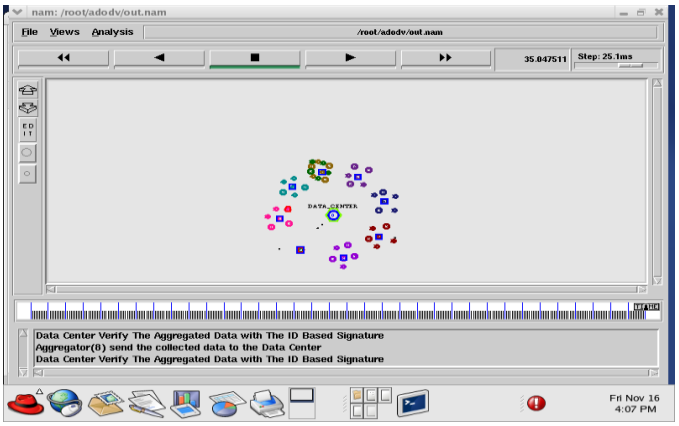

Fig 3:Sensing The Route

Here each cluster is given a colour for recognition. Then from the data centre the sensing of route is done using a particular sensor. In the process of sensing if any malicious node is detected then that nodes is eliminated and the nodes that group are joined to the nearest cluster.

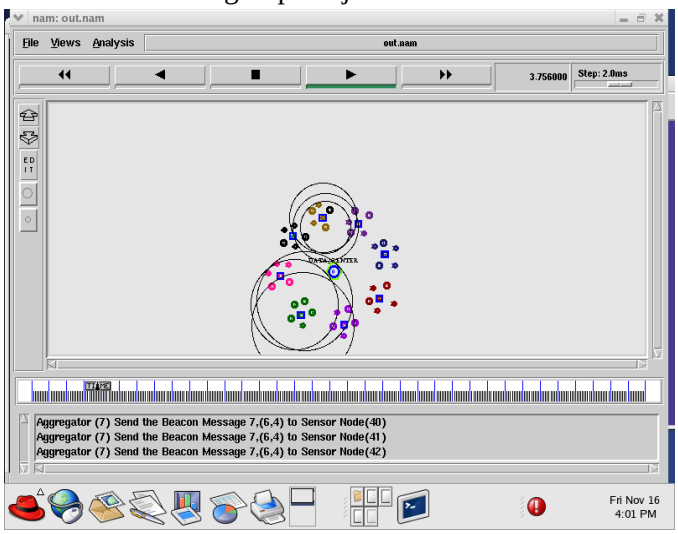

Fig 4: Applying Secure Routing Protocol For Routing Formation

For all the nodes now we apply a secure routing protocol for route formation. Based on this protocol sensing of nodes is then using a particular sensing protocol. Data is transferred from data centre to all the aggregators and then nodes.

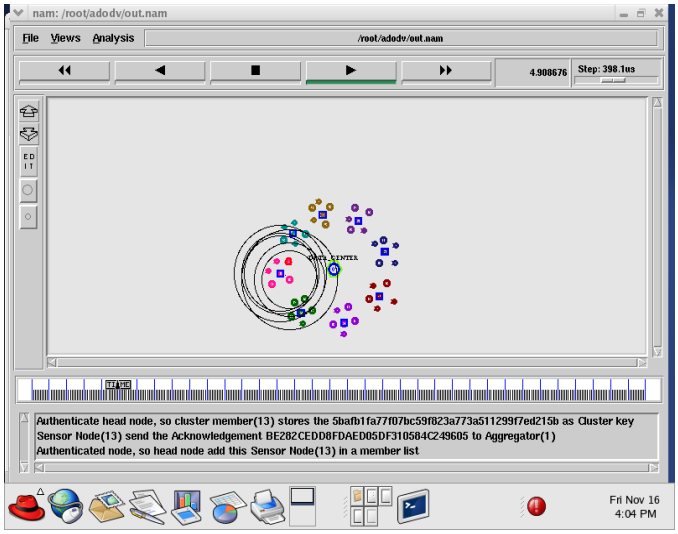

Fig 5: Applying Route Maintainance And Generating Id Based Route

Volume No:4, Issue No:10 (March-2019) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Now for each node we generate an ID for routing. Based on that ID sensing of the nodes is done using a particular sensing protocol. Then for each node hash key is generated.

6. Graphs

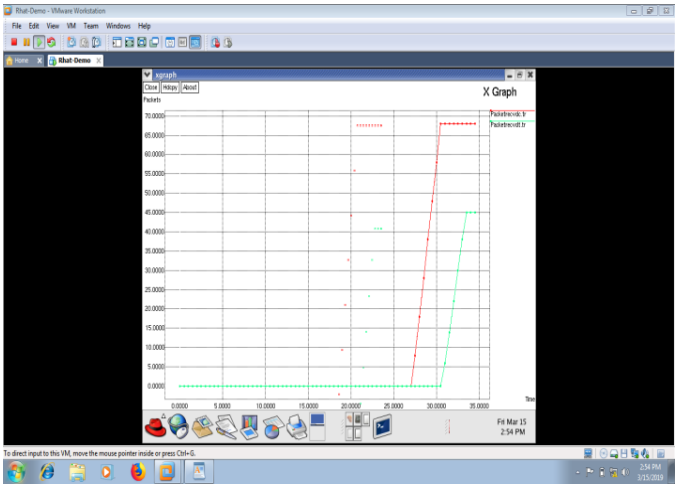

Fig 6:Packet Delivery Ratio

In the above fig: 6 the packets are generated up to 68,000 packets at the time of 27000 minutes of execution which is represented with red colour line. Those packets are generated in the process of sending nodes from unauthenticated node cluster to the nearest cluster. And after eliminating the fault node we again start the process of checking every node again. Then we generate packets of about 45000 at the time interval of 31.000 min

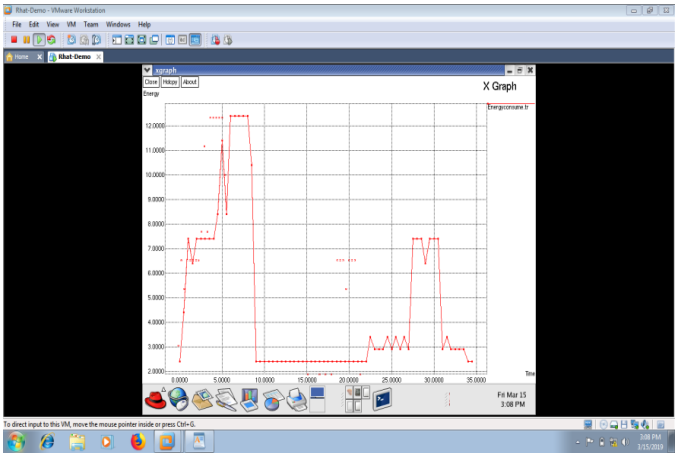

Fig 7:Total Energy Consumed

In the above fig: 7 we consumed energy in each different time intervals. When we have unauthenticated node, we consume more energy and when that node is eliminated less energy is consumed. While collecting the data we have consumed some energy i.e. 12,500. After eliminating the node again we perform same process and collect the data. Then we get the maximum energy as 7500.

7. Conclusion

In this paper we present an Id-based aggregate signature (IBAS) scheme for MANETs which can be compressed with many signatures created by Sensor nodes into a small one. Therefore the storage and communication can be reduced. And moreover, we can prove that IBAS scheme is secured through Oracle model which is based upon Computational Diffie Hellman (CDH) assumption, and also we can show that this aggregate signature can resist the collision of attacks.

8. References

[1]. Aurobindo Sundaram, An Introduction to Intrusion Detection, http://www.acm.org/crossroads/xrds2-4/intrus.html, last accessed on March 9, 2004

[2]. K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, ”An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”, IEEE Transaction on Mobile Computing, Vol.6, No.5, 2007, pp.536-550.

[3]. J. Gomez, D. Dasgupta, ”Evolving Fuzzy Classifiers for Intrusion Detection”, in Proc. of the 3rd Annual IEEE Information Assurance Workshop, 2002.

[4]. J. M. Mendel, ”Computing with Words and Its Relationships with Fuzzistics”, Information Sciences, 2007

[5]. L. M. Feeney and M. Nilsson, .Investigating the energy consumption of a wireless network interface in

an ad hoc networking environment,. in IEEE INFOCOM, 2001.

[6]. S. Marti, T. Giuli, K. Lai, and M. Baker, .Mitigating routing misbehavior in mobile ad hoc networks,. in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), August 2000.

[7]. L. Buttyan and J-P. Hubaux, .Enforcing service availability in mobile ad-hoc WANs,. in Proc. of First IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, August 2000.

[8]. J-P. Hubaux, T. Gross, J-Y. Le Boudec, and M. Vetterli, .Toward self-organized mobile ad hoc networks: The terminodes project,. in IEEE Communications Magazine, January 2001.

[9]. Junhai Luo, Xue Liu, Mingyu Fan, ”A trust model based on fuzzy recommendation for mobile ad-hoc networks”, ELSEVIER Computer Networks 53, pp.2396-2407, 2009.

[10]. Zhiwei Qin, Zhiping Jia, Xihui Chen, ”Fuzzy Dynamic Programming based Trusted Routing Decision in Mobile Ad Hoc Networks”, Fifth IEEE International Symposium on Embedded Computing 2008, pp.180-185, 2008.