ISSN:0975-9646

Identification of Misbehaviour Activities in Mobile Adhoc Networks

Indhumathi.J
Student,
M.E Computer Science and Engineering,
Sathyabama University,
Chennai, India.

Prem Jacob.T,
Assistant Professor,
Computer Science and Engineering,
Sathyabama University,
Chennai, India.

***Abstract*- Mobile Ad hoc Network is a collection of mobile nodes and it creates temporary network for the communication. Each node transferred the message to the other node by using wireless network. This network is not fully secured when it transfer the message. So that it needs to protect from an attacker. For identify the malicious node, already used TWOACK and Misbehavior Report Authentication (MRA) concept. This has time delay for detect the attacker. To avoid this issue, Fast random key is proposed in this paper, which reduce the time to identify the attacker in the network. The authentication is important for this process.**

Index Terms- Digital signature algorithm (DSA), Fast random key, Mobile Ad hoc Network (MANET).

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a group of mobile node use to communicate between source and destination. It allows for transmit the data like message, voice and video. MANET is a self configuring network. Ad hoc is a collection of wireless node that forms a temporary network. Each node should communicate with other node in its radio communication range. And there is no possible for transferring the message when the distance will increase from source to destination. For this, the intermediate node has been used. Based on this intermediate node we are using single hop and multi hop network. The multi hop is the group of single hop, which is mainly use to transfer the message. The single hop is a direct communication from the source to the destination.

The nodes are bidirectional method, which is performed by wireless transmitter and receiver. This is the moving network. So the nodes are able to configure and maintain for communication. The mobility and scalability is need, when the message is transfer to other node.

MANET is the open medium. So that there may be available for more attackers in the networks. These can be easily inserting the malicious node in the communication network. For detect these malicious node, TWOACK had been used. But it has time delay for identify the malicious node. And now fast random key is use to detect the malicious node.

The following paper includes: Section 2 related works, Section 3 Existing and Proposed system, Section 4 Experimental Design, and Section 5 Conclude the paper.

II. RELATED WORKS

Y.Hu, A.Perrig and D.Johnson [3] has presented the design and evaluation of Ariadne. This operation is based on DSR protocol. And this is highly efficient method. It prevent from many of denial of service attacks. The DSR route discovery and route maintenance are performed by using this protocol. The on-demand routing protocol provide the security when the sender need to send the message.

D.Johnson and D.Maltz [4] the sender specifies the route list in the packet's header. In some times routing algorithm occurred in the same way and this is not working in bidirection. Conventional routing protocol is used that route also maintained. The cache stores the route. If it is no longer, it will remove from cache. But it performs quickly when the node movement is frequent.

R.Rivest, A.Shamir and L.Adleman [6] use the encryption method for the security purpose. It builds the electronic mail that is enclosed with the signature. Finally it use private key and that key should not reveal to anyone. The trap-door one way method is not suit for other direction in the network, which is the problem of this method.

T.Anantvalee and J.Wu [1] need to prevent the network. The encryption and authentication is not sufficient when the network become complex. The IDS agent is responsible for detect the intrusion. It has local and global intrusion detection. M.Zapata and N.Asokan [7] use to reduce denial of service, distributed operation and loop free method. The cryptography system and use the routing protocol.

V.C.Gungor and G.P.Hancke [14] has the flexibility and rapid deployment. It use small sensor node with low cost. And it has an efficient protocol used for sensing method. L.Zhou and Z.Haas [8] need to use protocol for secure communication. To identify the misbehavior node, it uses cryptography method. Based on this, attacker is identified.

K.Liu, J.Deng, P.K.Varshney and K.Balakrishnan [5] mainly use cryptography method for authentication. This has the routing protocol to transfer the message. And that could send the acknowledgement after reach to the node. A.Singh, M.Maheshwari and N.Kumar [10] provide security for the communication. And it could be managed by a trusted one performed for all kind of works.

J.Parker, J.Undercoffer, J.Pinkston and A.Joshi [9], is use to find the intrusion in the network. So that it uses hierarchical intrusion method. If it detects the intrusion mean it gives the response to the sender of that message.

N.Kang, E.Shakshuki, and T.Sheltami [12] is detect the misbehavior node by using intrusion detection method. And it uses to identify the local and global intrusion node available in the network.

III. EXISTING SYSTEM AND PROPOSED SYSTEM

A .Existing System

In the existing system, the intrusion detection system called EAACK. If a source wants to send the data to the destination via intermediate node, each node send the acknowledging for every data packet when the packets are transmitted over the three consecutive nodes. If the packet is received by the destination, than we conclude that the data is safely reached to the destination. If not, the data will be retransmitted to destination via alternate path. Also Misbehavior Report Authentication (MRA) will be filed. Once receiving the data, the destination node check the data in its history, if the data is present then we conclude that the node which lied that they did not receive the data. Else we can conclude that the node have the data packet. For security purpose we can encrypt the data during the transmission. The main problem of this paper is, time delay for detecting the attacker.

MRA:

The Misbehavior Report Authentication is used, when the source did not get any acknowledgement from the node within a specified time period.

B.Proposed System

In this paper, fast random key algorithm is used and network is assigning TTL. The source will send the data to the destination, that network monitor all the node detail. So the network can update the key of each node for data transmission. Suppose anyone of the node does not send acknowledgement to previous node means network identify that misbehavior node based on primary key and intimate to source node. Here it takes less time for identifying misbehavior node. So delay is minimized. Here the acknowledgement is need, based on this only it will identify the malicious node. The techniques which is used in this paper will be explained shortly,

The techniques are,

1. Path selection
2. Acknowledgement
3. Buffer level

Path selection:

Each node in the network is assigned with key. The message is transfer to its neighbor node which is specified with the key. Through that only data transferred from source node to destination node.

Acknowledgement:

The acknowledgement is an end-to-end scheme. This is send to every node after receiving the data packet. Based on this only the sender known whether the destination get the packet message or not. So the acknowledgement is very important for message transferring method.

It uses the cryptography method for secured transmission and the node will get acknowledgement from its previous neighbor node, which is already transferred the data packet. For that it use digital signature algorithm.

Architecture of proposed system:

Architecture of proposed system includes fast random key algorithm. The whole process will be visible clearly in the architecture. The network has more nodes for transmit the message. Encryption is done, when the message transmission. Finally the malicious node identify based on the key, which is specified for each node and monitoring the network. Advantage of this proposed system is to minimize the time delay.

The acknowledgement has been verified by its previous node and server. Then it sends negative acknowledgement to the source node.

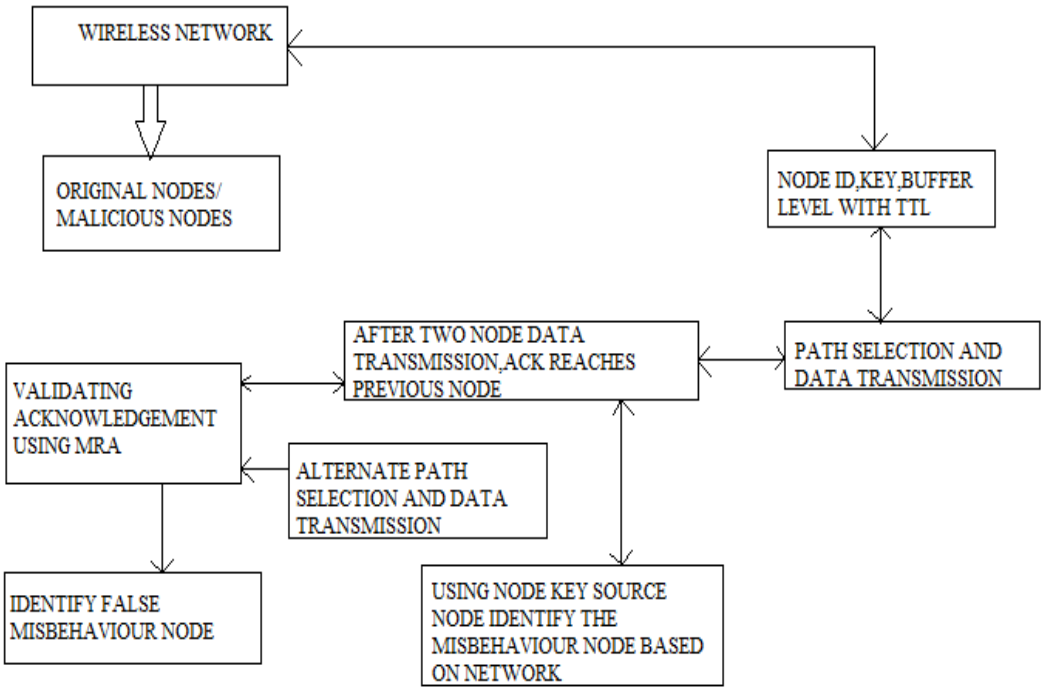

FIG: 1 Architecture Diagram

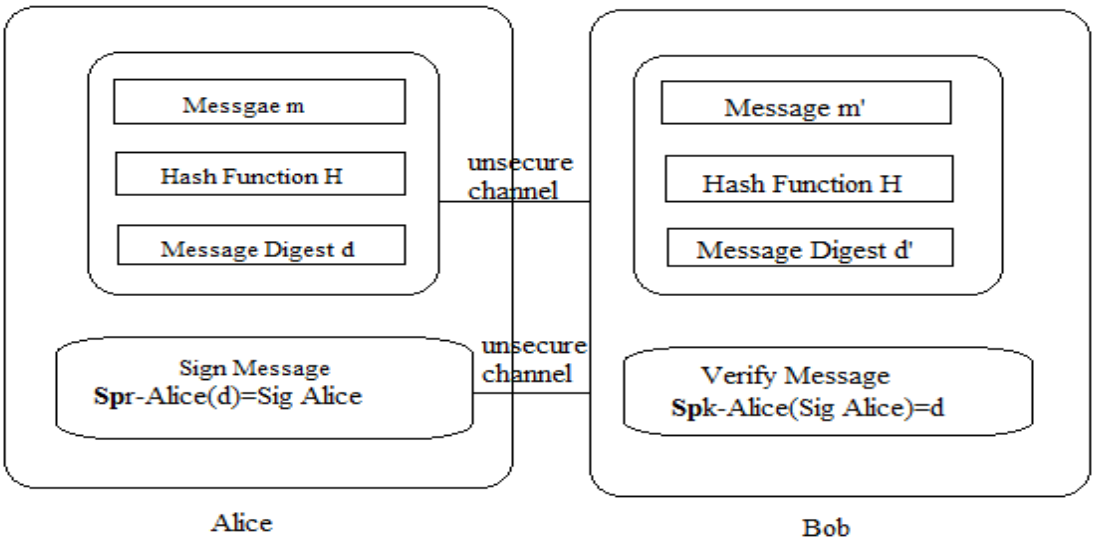

FIG: 2 Communications with Digital Signature

Digital Signature:

For security purpose, the data will be encrypted by using cryptography method. The Digital Signature algorithm is used. This algorithm has two categories. First one is, the original message is encrypted and it attached with private signature for authentication that is DSA. And the second is, transfer message should be verified by the destination. So the malicious node can't read the message. Finally it could decrypt the message after verification.

Process of the hash function H and message m compute the message digest

H (m) =d.

Message digest (d) is mainly send to the next process for key generation.

Alice specifies the sender and the bob is receiver.

Alice will need to apply the private key which is $P_{r\text{-}Alice}$ message digest d. It shows the results as in the form of signature Sig_{Alice} with private key and message m.

$$Sp_{r\text{-}Alice}(d) = Sig_{Alice.}$$

The private key should not reveal to anyone in the network. Alice will send the message along with Sig_{Alice}. Bob will get the message like m' that compute message digest.

$$H(m') = d'.$$

Finally Bob verify the signature by using Alice's public key,

$$Sp_{k\text{-}Alice}(Sig_{Alice}) = d.$$

If d =d' then the message is reached correctly. So the destination will get the message without the packet loss.

By using this method, the node identified whether it got the correct message from the source node.

This algorithm has both encryption and decryption method. First the sender encrypts the message that could be transmitting through the intermediate node. And second the destination decrypts the same data by using sender's public key.

Buffer level and TTL:

When the source will send the message to destination, the Time To Live (TTL) is assign. Within the specified time period, each node should get the acknowledgement after reach to the destination. If it not getting any acknowledgement then it known by the monitor. It sends the report to the source. Based on the monitor, the malicious node is identified.

If the packet is dropped because of the inadequate space, then it not consider as a malicious node. For that again source will send the message to the destination. This will send to another path in the network. When the source is ready to send the message, it will consider these two methods.

The sender and receiver have the private and public key. The senders encrypt the data and use its private key with the signature. And it sends to the receiver's public key.

And the receivers use its private key for the decryption. Here each node sends the acknowledgement to its previous node after getting the data packet. These are the common method when the message is transferred by using cryptography method in the network.

This is an algorithm which gives excellent results when detect and verify node in network on based fast random key. And it is much faster, so the network assigns key value for every node based this algorithm that means it randomly provide a key for each node in network.

IV. EXPERIMENTAL DESIGN

Experimental design is include the entire data flow of our system. Here it shows the normal data transmission in the network. Each node in the network is specified with the key. And that could be monitor. If any node did not sending the packet or the acknowledgement to its neighbor node in a proper way that is consider as a misbehaving node. FIG 3 shows that each node send data packet and get the acknowledgement.

The entire network had more nodes that mainly used for transaction process between source and the destination by using the intermediate node. That message transaction is given by following figure 3, which is a formal packet sending and it receives the acknowledgement from the node after got the packet.

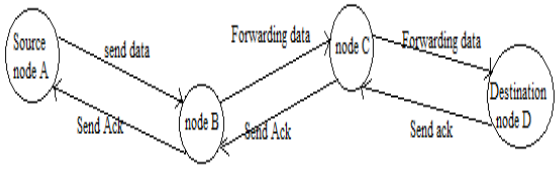

FIG: 3 Experimental Diagram

Data transmission from the source to the destination based on the key.

V. CONCLUSION

In this paper, fast random key algorithm is implemented. It allocate key for each node in the network. Digital Signature algorithm is used, when the sender ready to send the message and it keeps buffer level, TTL, which network monitor all the node details. By using this method, it could identify the malicious node. And it reduced the time delay. In future work, we will implement hybrid cryptography method for security and use real time network for testing the performance.

REFERENCE

[1] T.Anantvalee and J.Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in wireless/mobile security.2008

[2] Y.Hu, A.Perrig and D.Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," 2002, pp.12-23

[3] A.Patwardhan, J.Parker, A.joshi, M.Iorga and T.Karygiannis, "Secure routing and intrusion detection in ad hoc networks,"2005, pp.191-199.

[4] D.Johnson and D.Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing.1996

[5]K.Liu, J.Deng, P.K.Varshney and K.Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs,"IEEE Trans. Mobile Comput., vol.6, no.5, pp.536-550, May 2007.

[6] R.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"vol.21, no.2, 1983.

[7] M.Zapata and N.Asokan, "Securing ad hoc routing protocols," in proc.ACM workshop wireless secur. 2002, pp 1-10.

[8] L.Zhou and Z.Haas, "Securing ad-hoc networks," IEEE Netw., vol.13, no.6, pp.24-30. 1999.

[9] J.Parker, J.Undercoffer, J.Pinkston, and A.Joshi, "on intrusion detection and response for mobile ad hoc networks,"2004.

[10]A.Singh, M.Maheshwari, and N.Kumar, "Security and trust management in MANET," 2011, pp.384-387.

[11] R.Akbani, T.Korkmaz, and G.V.S.Raju, "Mobile Ad hoc Network Security", 2012.

[12] N.Kang, E.Shakshuki, and T.Sheltami, "Detecting misbehaving nodes in MANETs", 2010, pp.216-222.

[13] N.Nasser and Y.Chen, "Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network", 2007.

[14] V.C.Gungor and G.P.Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach", 2009.

[15] G.Jayakumar and G.Gopinath, "ad hoc mobile wireless networks routing protocol-A review", 2007.