Hybrid Security Using Encryption Algorithm in Wireless Adhoc Network

Sukhvir Kaur[1], Kulwinder Singh[2]
[1]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*
[2]*Department of Electronics and Communication Engineering, Punjabi University, Patiala, India*
[1]sukhvirkaur022@gmail.com
[2]ksmalhi@rediffmail.com

Abstract: Wireless mobile adhoc networks are used in short distance communication where each operating terminal has their own range of operation. We present a scheme which provides privacy in an adhoc network. This RSA encryption algorithm based on asymmetric encryption algorithm which works on public key for encrypting a message or private key for decrypting a message. This proposed scheme preserves privacy of nodes and reduces attacks in adhoc networks. We show how packets are transmitting from source node to destination node through neighboring nodes. We also show the improvement in throughput of network in the presence of attackers.

Keywords: RSA, ADOV, MANET, HLA, SHA-I

I. INTRODUCTION

Wireless adhoc networks are build-up with wireless nodes which interact precisely above prevailing wireless channels. These nodes are rigged with the wireless transceivers. Every node does not alone perform the performance of an end system and it also pretends as a router which transmits packet to covet nodes. And the adhoc network is anticipated to do appointment tasks that the infrastructure network can't perform [12]. An adhoc network is generally used by rescue mission teams, in military, taxi drivers and used by many more. Here, in the adhoc network a node can disseminate only with present nodes which are in its area and such node can interact or communicate with another node, but the routing algorithm is imperative. Wireless network also known as spontaneous network in computer network branch.

There are two means by which packet loss can occur [2, 3, 6, 8] that is by link error and malicious packet dropping attack. It is paramount for detect and encounters whether the link errors only, or is by combination of both link error loss and malicious packet drop loss reasons of packet drop in network. Here, the absolute interest is in the insider incursion case where such malicious nodes abandon and decline packets selectively to deteriorate the network performance. The packets are transmitted from source to destination and a bitmap is obtained for each node. By using the bitmap, correlation can be obtained between the lost packets and from this correlation, malicious node can be identified. For correlation of lost [12, 10] packets HLA (homomorphic linear authenticator) based mechanism is used to verify the malicious node which is responsible for packet dropping. RSA technique is used for securing data transmission. This is symmetric encryption algorithm. In this encryption key is publically known to everyone and decryption key is kept secret. To maintain and assure the accuracy and consistency of data, integrity of data, message digest algorithm which produces 128 bit hash value is used.

II. ENCRYPTION TECHNIQUES

There are many encryptions techniques are used in wireless adhoc networks. These encryption techniques used to avoid the eavesdropping attack in adhoc network. The information which is to be send from source node to destination node is firstly change into cipher text and then transmits it through transmission media. Only user who has knowledge about the key can encrypt and decrypt the message. There are many symmetric and asymmetric encryption techniques are used in wireless networks. A symmetric encryption technique uses same keys of user at sending or receiving side. And an asymmetric key uses different set of keys to encrypt and decrypt the message.

S. Sumathy et.al in [13] has worked on key exchange mechanism RSA (Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman) in wireless adhoc networks. They have shown that the key which is used to encrypt and decrypt the message exchanges between the nodes which are authenticated in network. Only authenticated nodes can participate in network operation as these nodes have knowledge about the key and packet. They have worked on spanning tree which are used to construct the network in this network nodes are plotted which exchanges the information. Only authorized nodes can take part in communication. This provides security to packet and reduces the chances of packet dropping.

Shelbala Solanki et.al in [14] has worked with Hybrid Security Using Digital Signature & RSA Encryption for AODV in MANET. Security is prime concern in any network as it is quite difficult for network administrator because many nodes participate in network operation for transmission of packet from sender to receiver. Due to security issues in MANET every packet is signed by a digital signature and message is encrypted by a encryption key at sender side and this message is decrypted by decryption

key at receiver side. The encryption key is known to everyone that's why it is known as public key and decryption key is kept private so it is called as private key. In this paper authors performed authentication based on SHA-I which is a digital signature algorithm. Only nodes which have knowledge about the signature and key can encrypt and decrypt the message.

This proposed scheme allows low storage overhead in multicast environment.

III. SPANNING TREE CONSTRUCTION

Nodes are plotted on x-coordinate and y-coordinate and the distance between them are measured by distance,

$$(i,j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$$

This tree gives the information about the nodes present in network and minimum distance between the working nodes. This construction is cheap and effective. Once the tree is constructed the packets are starts transferred to source node to destination node. In a spanning tree every node is connected with other nodes with minimum distances.

This makes highly effective to work in wireless network as chances of malicious node gets reduces in this way of transmission.

The flow chart of constructing spanning tree:

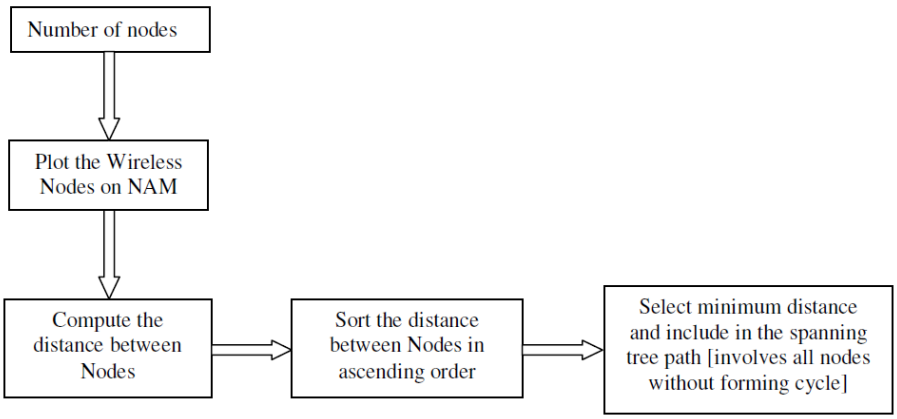

Fig 1.Construction of spanning tree [13]

IV. ENCRYPTION AND DECRYPTION ALGORITHM

As shown in flow chart the RSA algorithm is used to secure the message over open air medium or can say that message is only encrypted using private key.

Decryption of message is done by using private key. At the source side message is encrypted and changes into cipher text and sends to destination node. The message is decoded into original format using private key. This private key is kept secret and reduces the attacks on the network as only the owner is known to this key another node does not have any information about this private key. Neighborhood nodes are used to decrease the storage overhead on single node. Neighborhood nodes are participating in network operation to reduce the complex computational operations.

If a source node wants to transmit a message to another node which is destination of the message. Source node sends a request to neighborhood node then this neighborhood node also sends this request to another intermediate node. The chain process is formed and all participating nodes then sends reply to source node to destination node.

This chain process forms the routing path between two communicating nodes. Selecting two prime numbers namely 'p' and 'q' and also selecting two random numbers 'x' and 'y'. Calculates the product of these numbers using n1=p*q*x*y and n2=x*y. Eular's totient is calculated by using p-1*q-1*x-1*y-1. Encryption and decryption exponent are also prime numbers if this is even number then assign the next large prime number to it. Then calculates the encryption of message c=m^e mod(n1) and decryption of message m=c^d mod(n2). The figure shown below gives the encryption of the message procedure at sender side.

Firstly nodes are created according to the network size and then distances between nodes are calculated and spanning tree is constructed after this receiver's public key is used to encrypt the message and key exchange is performed between sender and receiver. At the receiver side message is decrypted with the help of receiver's private key.

This construction provides security to the concerned packets and reduces storage overhead at the node levels.

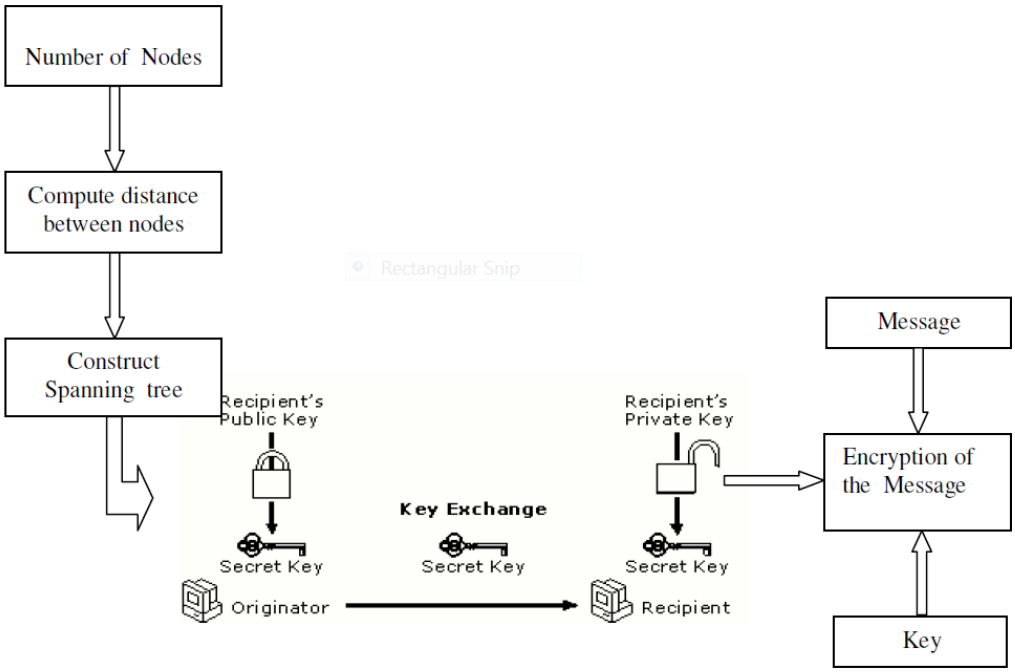

Fig 2. Encryption and decryption of message [13]

V. SIMULATION RESULTS AND DISCUSIONS

After creation of nodes we again create a network with 16 nodes and one node is assumed as a malicious node entered into the network. In this phase spanning tree is formed to measure the distance between nodes. This distance is measured by formula,

$$(i,j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$$

Tree is formed to ensure the privacy of the network as only authorized nodes can take part in communication only and authorized nodes could not affect the network as they don't have any knowledge about the keys. Selecting two prime numbers namely 'p' and 'q' and also selecting two random numbers 'x' and 'y'. Calculates the product of these numbers using n1=p*q*x*y and n2=x*y. Eular's totient is calculated by using p-1*q-1*x-1*y-1. Encryption and decryption exponent are also prime numbers if this is even number then assign the next large prime number to it. Then calculates the encryption of message c=m^e mod(n1) and decryption of message m=c^d mod(n2).

The figure shown below gives the encryption of the message procedure at sender side. Firstly nodes are created according to the network size and then distances between nodes are calculated and spanning tree is constructed after this receiver's public key is used to encrypt the message and key exchange is performed between sender and receiver. At the receiver side message is decrypted with the help of receiver's private key. This construction provides security to the concerned packets and reduces storage overhead at the node levels.

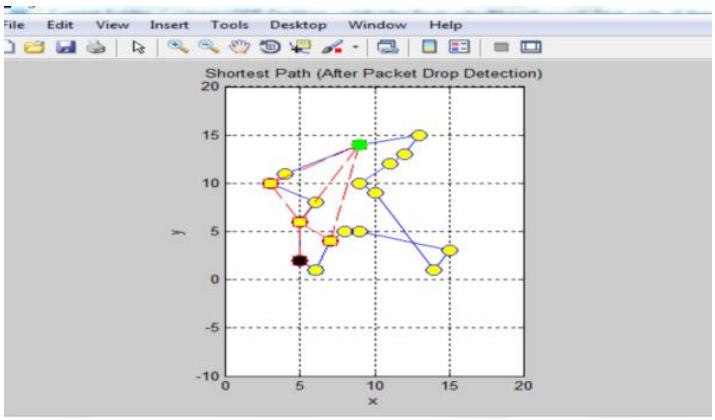

Fig3. Spanning tree or shortest path

As shown in above spanning tree green dot is represents the source node and yellow dots represents the neighboring node and black dot represents the destination node. And minimum distance of nodes is shown by dotted lines.

Figure 4 shows the throughput which is observed on the basis on total packet in the network and received packet by the destination node. This graph shows that the throughput is increased as the number of nodes present in the network and it starts decreases as the number of nodes increases in network. Because if there is large number of nodes present in network the chances of attack higher and in less number of nodes these chances are minimum. By using RSA throughput of network is improved.

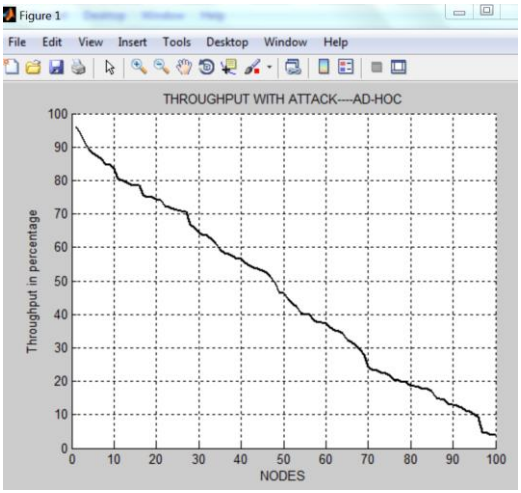

Fig4. Throughput of network

The graph between number of nods present in the network and throughput in percentage. The nodes also give the result of sending and receiving the packets from source to destination. The calculation of throughput is based on number of nodes present in the network and numbers of packet are successfully received at the destination end. It is assumed in this work that if nodes are authenticated then these transmit the packet to next node immediately but if node is not authenticated then it takes time to transmit the packet. From this we calculated the number of packet successfully received at the destination within minimum amount of time and throughput is calculated by given formula:

thr in % (throughput of network) = number of packets received at the destination successfully / total number of packets

As we are working on static nature of network nodes the throughput of network is high because delay between packet transmissions is less. This makes the adhoc network more reliable and fast working networks in wireless areas.

VI. CONCLUSION

In this paper we have proposed an RSA encryption scheme which provides security and privacy to adhoc network. We have shown the spanning tree construction which shows how nodes participate in transferring message from one node to another node. The shortest path is formed after the packet drop due to malicious node. We also show improvement in throughput in adhoc network in the presence of malicious node. It shows that percentage of throughput increases when number of nodes decreases in network. If there is 50 nodes in network with malicious node then throughput remains 50% only if nodes decreases in network then throughput improves to 90% to 95%.

REFERENCES

[1] W. Kozma Jr. and L. Lazos, “Dealing with liars: Misbehavior identification via Renyi-Ulam games, ” presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009
[2] W. Kozma Jr., and L. Lazos, “REAct: Resource-efficient accountability for node misbehavior in adhoc networks based on random audits, ” in Proc. ACM Conf. Wireless Netw. Secur., pp. 103–110, 2009.
[3] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, “Castor: Scalable secure routing for adhoc networks, ” in Proc. IEEE INFOCOM, pp.1 –9, Mar. 2010.
[4] Y. Zhang, L. Lazos, and W. Kozma, “AMD: Audit-based misbehavior detection in wireless adhoc networks, ” IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.
[5] AmitangshuPal, “LocalizationAlgorithm in wireless sensor networks: current approaches and future challenges”, Network protocol and Algorithm , ISSN 1942-3581 vol.2 no.1, 2010.
[6] Bobby Sharma Kakoty, S.M. Hazarika, N.Sarma, “NAOD- Distributed Packet Dropping Attack detection in MANETs”, International Journal of Computer Applications (0975-8887), vol.83-no.11, dec 2013.
[7] Mr. Deepak Sharma, Ms.Palvee, Ms. Manpreet Kaur Gill, “BFO Algorithm Based efficient clustered network design for optimized wireless sensor Throughput and node capacity ”, International journal of advanced research in Computer science and Software engineering, ISSN: 2277128X, vol.3, Issue 9, sept 2013.

[8] Dr.C Kumar Charliepaul, K. Megala Devi, "Secure routing and attack detection in Wireless adhoc network", International journal on Engineering Technology and Sciences, ISSN 2349-3968, vol.1, Issue 6, oct 2014.
[9] R Reena1*, B Hemalatha1, K Heerajan1, A Jenifercruz1, and P Menaka, "Detection Of Packet Dropping In Adhoc Networks", International journal of Engineering Research and Science & Technology, 2nd National Conference on ''Recent Advances in Science, Engineering Technologies'' RASET-2015, ISSN 2319-5991 Special Issue, vol. 1, no. 2, April 2015.
[10] Noble George1, Sujitha M2, **"**Truthful Detection of Packet Dropping Attack in MANET**",** International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) 2278-1021 ISSN (Print) 2319 5940, vol. 4, Issue 7, July 2015.
[11] Haiying Shen, Senior Member of IEEE, Ze Li, and Chenxi Qiu, "A Distributed Three hop Routing Protocol to increase the capacity of Hybrid Wireless networks", IEEE Transactions on mobile computing, vol.14, no.10, oct 2015.
[12] Tao Shu and Marwan Krunz, Fellow, IEEE, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Adhoc Networks", IEEE Transactions on mobile computing, vol. 14, no. 4, 2015
[13] S. Sumathy and B.Upendra Kumar, "Security exchange and encryption mechanism for group communication in wireless adhoc network", journal on application ofgraph theory in wireless adhoc networks and sensor networks (JGRAPH-HOC) vol.2, no.1, march 2010.
[14] Shelbala Solanki, Anand Gadwal, "Hybrid securities using Digital Signature and RSA encryption in ADOV in MANET ", International journal of computer science and information technology, vol.6(3), 2630-2635, 2015.