A Secure Communication using RSA Cryptography in Mobile Ad-hoc Networks

Ms. Swati Velaskar[1*], Mr. Abhishek Garg[2]
Department of Electronics and Communication, SDBCT, Indore (M.P.), India

Abstract - Wireless communications is emerging and most active area of technology development. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Due to open nature communication, it is vulnerable for various security threats. Information leakage and eavesdropping are most possible situations to compromise the communication. This research paper provides a technique to provide confidentiality over communication. It uses RSA algorithm to encrypt and decrypt the transmission. Proposed solution is implemented and simulated with NS-2 simulator. Performance observation concludes the proposed method gives better result and security over traditional once.

Keywords:- Ad- hoc, MANET, confidentiality, reliability.

1 INTRODUCTION

Wireless communication performance depend upon radio bandwidth and transmitting power this are the resources used to increase the scalability and capacity of wireless systems. But, these two resources are limited deployment in wireless networks. there are two major issue in wireless network vulnerability and resiliency ,hence the wireless networks has become a considerable research topic.

Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. Wireless technology is allowing to access information and services electronically from everywhere. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. Protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs).

Mobile Ad hoc Network (MANET) are used most commonly all around the world, because it has the ability to communicate each other without any fixed network. Security is an essential requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes eaves dropping and selective forwarding attacks.

MANETs may be deploys in structured or unstructured manner deploy with dynamic characteristics. Here, connections may be established through Pear-to-Pear or Dynamic mode without considering centralize infrastructure. It is shown in Figure 1 and Figure 2.

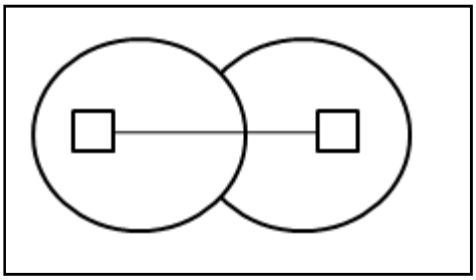

Figure 1: Pear to Pear Connection

MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service attack. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily.

Among the various protocols available AODV is most vulnerable to such attack. In AODV every mobile node maintains a routing table that stores the next hop node information for a route to a destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if such a route is available in its routing

table. Otherwise, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to the destination.

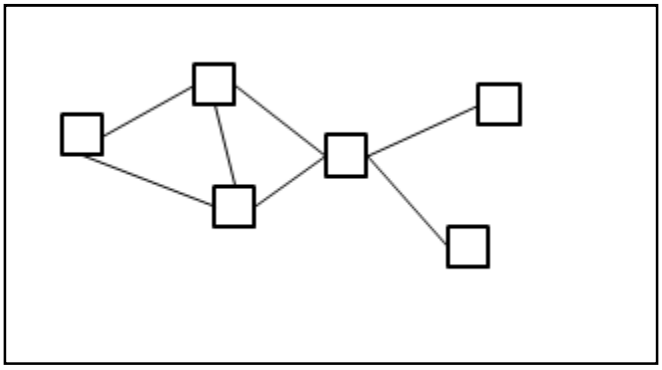

Figure 2: Dynamic Multi-hop Connection

Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus basic purpose of this model is too developed within which security services and mechanisms can be viewed.

The main purpose of this project is to provide an efficient way to user send or receive message over a secured channel. This system is basically aimed to provide strong security, confidentiality, reliability, completeness and non-repudiation of data transmission in P2P Communication.

Mobile Ad-hoc Networks Limitations:

MANET get popular due to wide range of applications and purpose to use. The best part of ad-hoc networks is, it does not require pre-existing infrastructure. To achieve best result and explore the research possibilities, work identified certain constraints in MANET which are;

1. Dynamic Node Topology:

Mobile node may join, move or relocate any time anywhere. It requires huge attention and updates on route discovery and maintenance. It also opens the possibilities for attacker to join and leave network as per convenience

2. Limited Energy;

Small size of battery and heavy consumption make it more important constraint to think before we make any changes in existing solution. It is high priority requirement to make energy consumption as low as possible to increase node as well network life.

3. Environmental Impact:

Due to wireless link connection variation into environment also create link failure or noise creation.

4. Decentralized Structure:

Due to open and shared nature, it is hard to deploy centralize monitoring and surveillance system.

The complete study observes that, security is the primary area for research and development. But also require considering all resource constraint for new proposed solution.

2. Vulnerabilities of MANETs

1. Open Communication

   Wireless nature of communication links make this network more susceptible and vulnerable for security threats like eavesdropping and traffic analysis. Passive attacks may able to degrade network performance. Furthermore, Due to heavy resource constraint and poor authentication process it may be open platform for attackers to deploy and configure active attacks using malicious nodes.

2. Dynamic Traffic and Topology Establishment

   Due to infrastructure-less culture of MANET, mobile node can join or leave node anytime or move anywhere. It make hard for surveillance to differentiate between normal node and malicious node.

3. Strategy Considerations

Several routing protocols are defined to discover a route. They use network resources and configure required information on same. Sometime this configuration or updating may done through malicious node and misuse by attacker.

4. Resource Constraints

Limited resources make it an opportunity for attacker to target and degrade the expected performance. For example, DDOS attack or flooding attacks are used to increase bandwidth and battery consumption. It leads to degrade node life and delay in packet delivery.

5. Lack of Centralize Control

Because MANET does not evolve any central management it becomes confusing and vulnerable for attackers to create misunderstanding about information.

6. Undefined Boundary

Wireless range is used to define the communication area of mobile node. No one can define the fix boundary of communication like wired networks. These phenomena make it vulnerable to access the network communication from boundary level and leave the network very soon.

3. Problem Statement

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. Direct Communication is prone for eavesdropping attack and may responsible for leakage of credentials and sensitive information. The complete study observes that, AODV is a insecure routing protocol and does not incorporate any mechanism to detect and prevent communication from malicious affect.

Solution Domain

The complete study observe that there is need to make communication secure from unauthorized access and unwanted information leakage. Proposed solution consider RSA encryption algorithm, to achieve confidentiality during communication. Here, automatically key generation technique has been used to generate key for encryption. All participating nodes generate public key and broadcast to every possible nodes. Now, sender encrypts the message with receiver's public key and transmits to receiver. Receiver converts the cipher text into plain text by decrypting the message through private key. The complete solution is implements with NS-2 simulator and compared on basis of network without RSA and network with RSA. Throughput, PDR and E2E delay parameters are used to observe the performance and evaluate the impact of RSA encryption on MANET.

4.Results

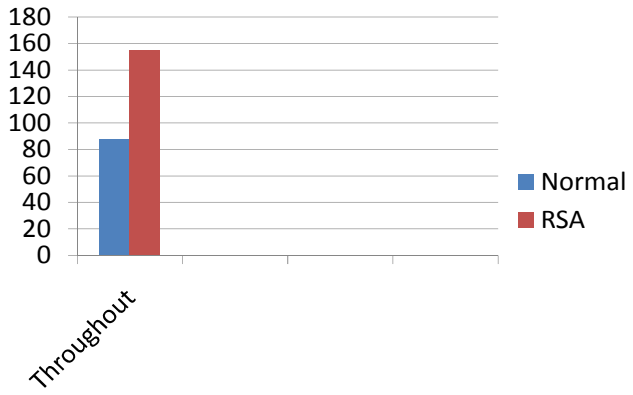

Fig.1. Throughput

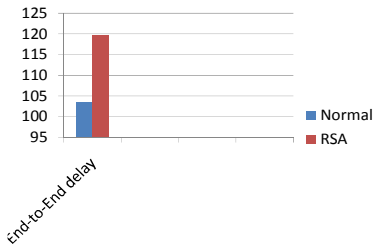

Fig.2 End-to-end delay

	Normal	RSA
Throughput	87.47	154.76

	Normal	RSA
End-to-End delay	103.53	119.64

Fig.3.Packet

	Normal	RSA
PACKET	97.14	215.74

5. Conclusion

The complete result observation concludes that proposed solution not only gives better PDR and throughput but also reduce E2E delay. It also provide confidentiality through RSA over communication. Thus complete work conclude that proposed solution will not only gives better security but also good performance.

6. References

[1] Rajan.S.Jamgekar,Geeta Shantanu Joshi,"File encryption and decryption using secure RSA", in International journal of Engineering science and engineering (IJESE),ISSN:2319-6378,Volume-1,ISSUE-4,February-2013.

[2] Nentawe Y.Goshwe,"Data encryption and decryption using RSA algorithm in a network environment", Department of electrical/electronics engineering university of agriculture,Makurdi",International journal of computer science and network security,Vol.13NO.7,JULY-2013.

[3] Sapan Saxena,Bhanu Kapoor,"An efficient parallelalgorithm for secured data communication using RSA public key cryptography method"IEEE-2014.

[4] P.Srinivasarao,P.V.Lakshmipriya,P.C.S.Azad,T.Alekhya,K.Raghavendrarao and K.Kishore,"A technique for data encryption and ddecryption ",International journal of future generation communication and networking (IJFGCN),ISSN:2233-7857,VOL.7-2014.

[5] Sombir Singh,Sunil.K.Maakar,Dr.Sudesh Kumar,"A performance analysis of DES and RSA cryptography",International journal of emerging trends & Technology in computer science (IJETTCS),ISSN:2278-6856,VOL-2,ISSUE-3,MAY-JUNE-2013.

[6] Karamjeet Singh,Chakshu goel,"Using MD5 and RSA algorithm improve security in MANET system", International journal of advances in science and technology (IJAST),VOL-2,ISSUE-2(JUNE-2014).