INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Improving Security in MANET using modified Elgamal Algorithm

Isha Gaba[1], Parminder Singh[2]

[1]Research Scholar, Department of Computer Science, Doaba Group of Colleges, Kharar, Punjab, India
[1]*isha.gaba123@gmail.com*
[2]Assistant Professor, ECE Department, Doaba Group of Colleges, Kharar, Punjab, India
[2]*Parminder.db@gmail.com*

Abstract: *The advances in mobile computing and wireless communications, mobile ad hoc networks (MANETs) are becoming more attractive for use in military applications. Supporting security-sensitive applications in hostile environments has become an important research area for MANETs since MANETs introduce various security risks due to their open communication medium, node mobility, lack of centralized security services, and lack of prior security association. In high-security MANETs, user authentication is critical in preventing unauthorized users from accessing or modifying network resources. In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984 ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. In our proposed work we are modifying Elgamal cryptosystem so as to reduce computations on mobile nodes. It will not only improve the battery life of mobile nodes but also increase data transfer rate. After modifying the algorithm we have implemented it in Mobile ad hoc networks.*

Keywords: *MANET (mobile ad hoc network), Elgamal Encryption, Asymmetric Key, Digital Signature, energy level.*

1. INTRODUCTION

MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. It is a self configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. In other words, ad hoc network do not rely on any fixed infrastructure (i.e. the mobile ad hoc network is infrastructure less wireless network.

The Communication in MANET is take place by using multi-hop paths. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET [1].

2. CHARACTERSTICS OF MANET'S

Autonomous behavior- In MANET, each node acts as both host and router. It means that a node has ability of host and can also perform switching functions as router so endpoints and switches are indistinguishable.

Multi-hop transmission- When a source node and destination node for a message is out of the transmission range, the MANETs are capable of multi-hop transmission.

Distributed nature of operation- As a centralized control is absent here, the control and operation of the network is distributed among the nodes. The nodes should collaborate to implement many functions mainly security and routing.

Dynamically changing topology- Due to mobile nodes, the change in topology is frequent and dynamic in nature. The connectivity among the nodes may vary with time and dynamically establish routing among them as they move about [2].

Inferior link capacity- The reliability, scalability, efficiency and capacity of wireless links are often inferior when compared with wired links. One end to end path can be shared by several sessions. This shows the fluctuating link bandwidth of wireless links.

Symmetric environment- All nodes have identical fe-atures with similar responsibilities and capabilities. Every node can function as a router or host and hence it forms completely symmetric environment.

Light weight features- MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.

Absence of Infrastructure- Ad-hoc networks are supposed to operate independently of any fixed infrastructure.[3]

3. APPLICATIONS OF MOBILE ADHOC NETWORKS

Military battlefield- Military equipment now routinely contains some sort of computer equipment. Through ad-hoc

networking, the military could take the advantage of commonplace network technology to maintain an information network among the vehicles, soldiers and military head quarters. Basically the techniques of ad-hoc networks came from this field.[4][5].

Commercial sector- Ad hoc can be used in emergency/rescue operations for natural calamities relief efforts, e.g. in fire, flood, or earthquake. Rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is delivered from one rescue team member to another.[6][7]

Local level- Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference

Personal Area Network (PAN)- Short-range MANET can simplify the intercommunication between various mobile devices (such as a mobile phone, laptops, and wearable computers). MANET can also extend to access the Internet or other networks by mechanisms e.g. Wireless LAN [3].

4. SOME ISSUES AND DIFFICULTIES IN MANETS

MANETs differ from the traditional wired Internet infrastructures. The differences introduce difficulties for achieving Quality of Service in such networks. The following list itemizes some of the problems:

Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology - which is typically multi-hop - may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Bandwidth-constrained, variable capacity links: Wireless links will continue tn o have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.- is often much less than a radio's maximum transmission rate. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking.

Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. .

Security Issues: Mobile wireless networks are generally more prone to security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.[8]

Error-prone channel state : The characteristics of the links in a wireless network typically vary, and this calls for an interaction between the routing protocol, if necessary, find alternate routes.[4]

5. LITERATURE SURVEY

Mobile Ad hoc Network (MANET) Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. Many researchers choose the best they found and use it in different combination to provide security to the data in cloud. On the similar terms, we have chosen to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as "Three way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.[9]

A Mobile Ad hoc Network (MANET) is an infrastructure-less system having no designated access points or routers and it has a dynamic topology. MANETs follow a distributed architecture, in which each node can move randomly in an area of operation. MANETs are vulnerable to various attacks. Security services in these kinds of networks are more complex than in traditional networks. In this paper, we implement a new RSA-Threshold Cryptography-based scheme for MANETs using Verifiable Secret Sharing (VSS) scheme. Threshold Cryptography (TC) provides a promise of securing these networks. The proposed scheme is based on the Chinese Remainder Theorem (CRT) under the consideration of Asmuth-Bloom secret sharing scheme. To the best of our knowledge, such a work does not exist in MANETs. The proposed scheme is efficient in terms of computational security.[10]

Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points,

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions. The effort has been made on the comparative study of Reactive, Proactive and Hybrid routing protocols. There are various shortcomings in different routing protocols and it is difficult to choose routing protocol for different situations as there is tradeoff between various protocols. There are various challenges that need to be met, so these networks are going to have widespread use in the future.[11]

6. RELATED WORK

Rivest-Shamir-Adleman (RSA) A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. RSA formed the basis for a number of encryption programs, including Pretty Good Privacy (PGP). RSA is an algorithm for public key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys.

6.1 Steps of this algorithm are as:

- Choose two large prime numbers p and q.
- Calculate n = p x q.
- Select the public key (i.e. encryption key) e such that it is not a factor of (p – 1) and (q -1).
- Select the private key (i.e. the decryption key) d such that the following equation is true(d x e) mod (p – 1) x (q – 1)= 1.
- For encryption, calculate the cipher text CT from the plain text PT as follows: CT = PTe mod n
- Then send CT as the cipher text to the receiver.
- For decryption, calculate the plain text PT from the cipher text CT as follows: PT = CTd mod n

6.2 Limitations of RSA are as:

- Every RSA initialization process requires random selection of two very large prime numbers (p and q).
- In the real world the encryption capabilities of RSA are rarely used for one simple reason: the length of plain text that can be encrypted is limited to the size of n=p*q.
- RSA is much slower than DES and other symmetric cryptosystems.
- If any one of p, q, e, d is known, then the other values can be calculated. So secrecy is important.
- To protect the encryption, the minimum number of bits in n should be 1024.

7. OUR PROPOSED WORK

Step-1 :- Defining topology
Step-2 :- Establishing Connection between mobile nodes
Step-3 :- Path Selection from source to destination
Step-4 :- Applying Elgamal cryptosystem for data encryption and decryption.
Step-5 :- Connection Termination

8. RESULTS

In our proposed work we have implemented Elgamal Cryptosystem. Firstly, we have reduced the complexity of Elgamal Cryptosystem and then implemented it in Mobile Ad-hoc Network. Secondly we analyzed the performance of Elgamal Cryptosystem through various graphs Such as Delay and Packet Delivery Ratio.

Delay: - Network delay is an important design and performance characteristic of a computer network or telecommunications network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

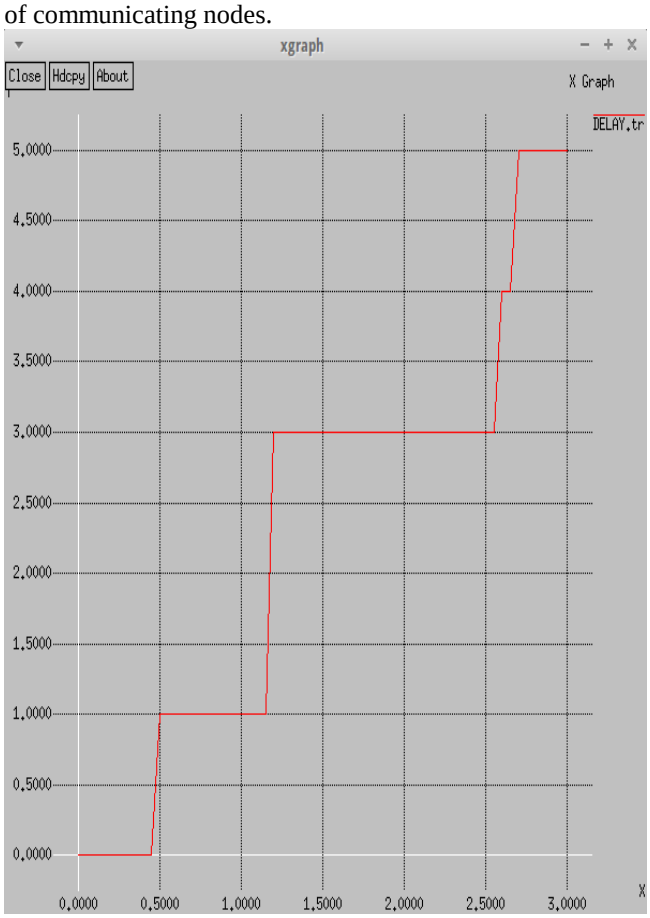

Figure 2 Average Delay Analyses

Packet Delivery Ratio:- The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

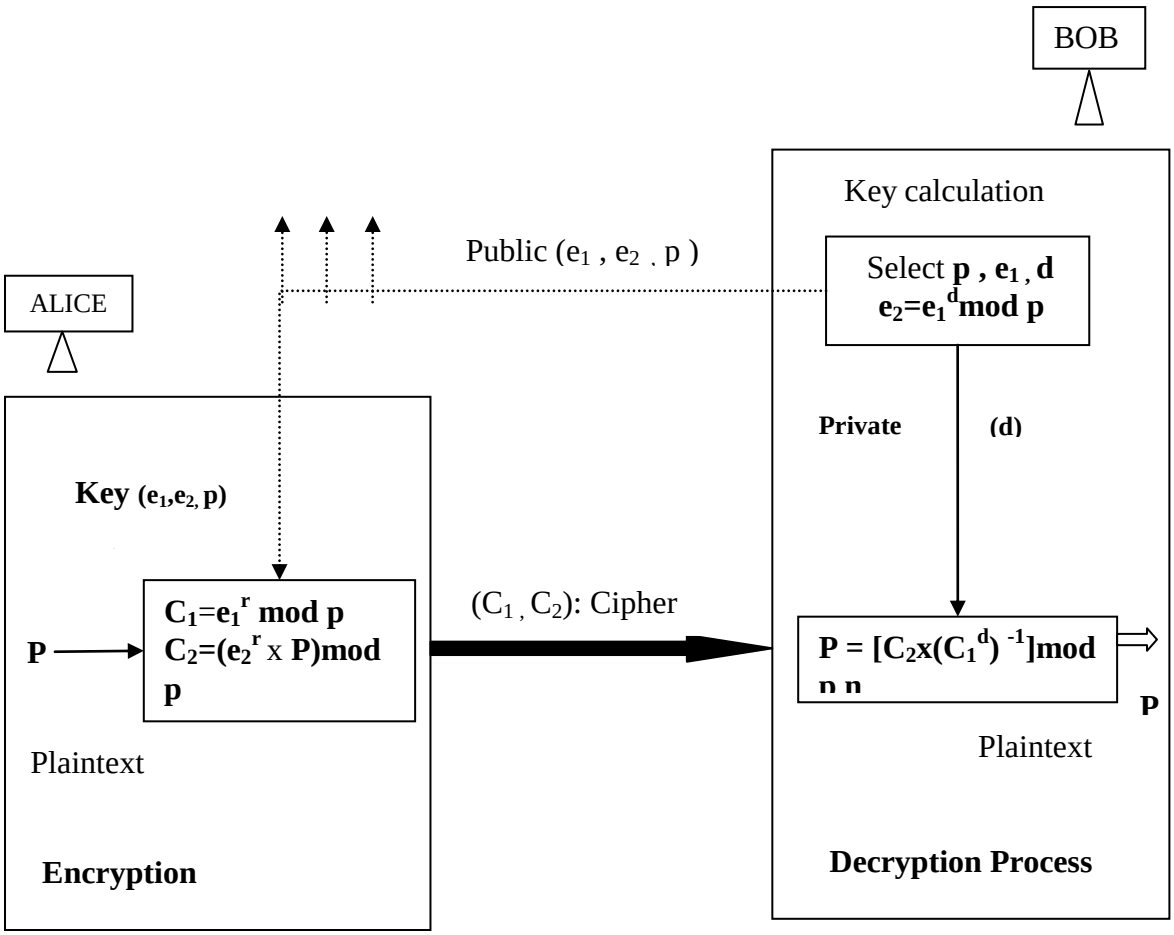

Figure 1 Elgamal cryptosystem

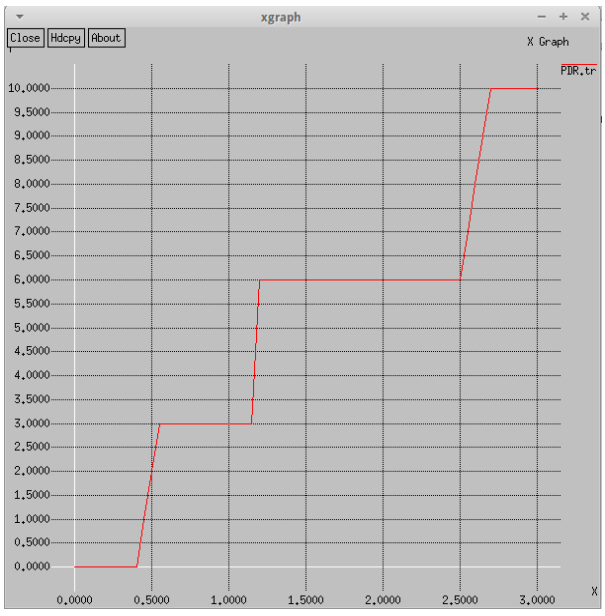

Figure 3: Packet Delivery Ratio

8.1 SIMULATION ASSUMPTIONS

- Radio Propagation Model: - Two Ray Ground
- Antenna type:- Omni Antenna
- Max packet in ifq:- 50
- Number of Mobile Nodes: - 7
- Routing protocol:- AODV
- Simulation area:- 800x800(m)

9. CONCLUSION AND FUTURE SCOPE

In our proposed Elgamal Cryptosystem has been implemented successfully and the results obtained are satisfactory. Further, In Future work we can enhance the performance of the algorithm by reducing its complexity further. We will also try to combine it with some security algorithm so that we can obtain enough security possible.

REFERENCES

[1] Mohit Kumar, Rashmi Mishra (2012) ***"An Overview of MANET: History, Challenges and Applications"*** **ISSN: 0976-5166 Vol. 3 No. 1 Feb-Mar 2012.**

[2] Jagtar Singh, Natasha Dhiman (2013) "*A Review Paper on Introduction to Mobile Ad Hoc Networks*" International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 2 Issue 4 July 2013 143 ISSN: 2278-621X.

[3] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal (2012*) "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges".*

[4] Kemal Akkaya , Mohamed Younis (2005) *"A Survey on Routing Protocols for Wireless Sensor Networks"*

[5] Gurpinder Singh, Jaswinder Singh (2012) "*MANET: Issues and Behavior Analysis of Routing Protocols*" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012 ISSN: 2277 128X .

[6] Yogendra Kumar Jain, Nikesh Kumar Sharma (2012) *"Secure Trust Based Dynamic Source Routing in MANETs"* International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 ISSN 2229-5518

[7] B.Ruxanayasmin , B. Ananda Krishna (2013) "*Minimization of Power Consumption in Mobile Ad hoc Networks"* I.J.Computer Network and Information Security, 2013, 2, 38-44 Published Online January 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.02.06.

[8] T.R. Panke , B.M.Patil (2013) "Improved Certificate Revocation Method in Mobile Ad Hoc Network " International Journal of Computer Applications (0975 – 8887} Volume 80 – No 12, October 2013

[9] Mr. Prashant Rewaga, Ms.Yogita Pawar(2013) "*Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing"* 978-0-7695-4958-3/13 $26.00 © 2013 IEEE.

[10] S. Sarkar, B. Kisku, S. Misra, M. S. Obaidat(2009) *"Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET Using Verifiable Secret Sharing Scheme"* 978-0-7695-3841-9/09 $26.00 © 2009 IEEE

[11] Dr. V.R. Singh, Bharat Bhushan naib (2013) *"Design and Analysis of Secure Quality-Of- Service Routing in Mobile Ad Hoc Networks"* International Journal of Research in Computer Engineering and Electronics. 1 ISSN 2319-376X VOl : 2 ISSUE :1 (Feb 2013) IJRCEE@2013 http://www.ijrcee.org .