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

Implementation of OAEP Algorithm in Mobile Ad-hoc Networks

Chandni[1], Parminder Singh[2]

[1]Student, Department of Computer Science, Doaba Group of Colleges,
Kharar, Punjab, India
[1]chandni.cpc.cgc@gmail.com
[2]Assistant Professor, ECE Department, Doaba Group of Colleges,
Kharar, Punjab, India
[2]parminder.db@gmail.com

Abstract: *The Mobile ad-hoc networks have far more vulnerabilities than the traditional wired setup networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks that can come from any link that is in the radio range of any link in the network, at any time, and point to any other node in the network. To make matters bad, there are various link attacks that can jeopardize the mobile ad hoc network, which make it harder for the nodes in the network to resist the attacks. The attacks primarily adds passive eavesdropping, active interfering, and outflow of undisclosed information, data tampering, message replay, message contamination, and denial of request. Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme often used together with RSA encryption. The OAEP algorithm is a type of Feistel network which uses a pair of random oracles G and H to process the plaintext prior to asymmetric encryption. When linked with any secure trapdoor one-way permutation, this processing is proved in the arbitrary oracle model to result in a combined scheme which is semantically secure under chosen plaintext attack (IND-CPA). When implemented with certain trapdoor permutations (e.g., RSA), OAEP is also proved secure against chosen cipher text attack. OAEP can be help to build an all-or-nothing transform. In our proposed work we are modifying Optimal Asymmetric Encryption Padding scheme to reduce its complexity. After reducing its complexity we are implementing Optimal Asymmetric Encryption Padding in MANETs.*

Keywords: *MANET (mobile ad hoc network), RSA, Optimal Asymmetric Encryption Padding (OAEP), energy level.*

1. INTRODUCTION

Mobile Ad Hoc Network (also called MANET) is a collection of mobile nodes forming a temporary network without the help of any centralized access point or existing infrastructure. In this type of environment, routing protocols are required to transfer packets from source to destination as some mobile nodes can act as intermediate nodes to forward a packet to its destination, due to the fixed range of each mobile node's wireless transmissions. Mobile hosts and wireless networking are prevailing areas of research. Wireless networks are categorized as infrastructure based and infrastructure less networks. Infrastructure less networks are used where it may not be economically practical or physically possible to provide the necessary infrastructure or be-cause the expediency of the situation does not permit its installation via communication in areas affected by natural disasters, war areas, in meetings and conventions in which persons wish to quickly share information etc. In such situations, mobile hosts within the same vicinity can communicate with each other without the help of fixed wired infrastructure. This type of wireless network is known as an Ad hoc network. In such Ad hoc networks, all Routing protocols are required to route data packets from source to destination. Routing protocols are basically categorized in to table driven and on demand routing protocols. In table driven routing protocols, up-to-date routing information is maintained by each node in the network. One or more tables are required by each node in order to store routing information, and these tables are modified in response to changes in network topology by propagating updates among all nodes in the network.

On the other hand, on demand routing protocols concentrates on creating routes only when desired by the source node. When a fixed node requires a route to a destination, it starts a route discovery process within the network [1].

2. ROUTING PROTOCOLS IN MANETS

Most of the routing protocols in Mobile Ad Hoc networks are generally categorized as proactive protocols, reactive protocols, and hybrid protocols Proactive.

Proactive protocols: - These protocols require each node to maintain one or more tables to store update routing information and to propagate updates throughout the network. These protocols will try and adjust valid routes to all communication mobile nodes all the time, which means before a route is really needed. Periodic route updates are swapped in order to synchronize the tables. A few examples

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

of table driven ad hoc routing protocols include DSDV, OLSR and FSR.[2]

Reactive or on-demand routing protocol: -These protocols do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wishes to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection to transmit and receive the packet. DSR, AODV are the examples of reactive protocols.[3]

Hybrid protocols: - Hybrid routing protocols have the potential to provide higher scalability than pure reactive or proactive protocols. This is because they attempt to minimize the number of rebroadcasting nodes by defining a structure, which allows the nodes to work together in order organize how routing is to be performed. By working together the best suitable nodes can be used to perform route discovery for example ZRP [4].

3. ADVANTAGES AND DISADVANTAGES OF MANET'S

Advantages of MANET:

- They represent access to information and services respective to geographic location.
- These networks can be managed at any place and time.
- These networks operate without the help of any pre-existing infrastructure.
- They can be used in emergency services.[5]

Disadvantages of MANET:

There are some disadvantages of MANETS:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust defenceless to attacks, lack of authorization facilities.
- Volatile network topology makes it complex to detect malicious nodes.
- Higher Packet loss
- Energy constrained operation.[5]

4. LITERATURE SURVEY

In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, in series from military to civilian and commercial uses. The security has become one of the prime concern in the MANETS are being used at large scale. To achieve security goals like: authentication, integrity, non-repudiation, a secret key is must required to be shared between the sender and the receiver. Some of the popular key exchange protocols have some demerits in case of MANETs which are due to mainly the requirement of high computational capability. We considered security enhancements to DSR for providing an on-demand secure routing protocol. We also proposed an algorithm to exchange shared / session key between the source and the destination during the route creation itself. For the performance enhancement, NS2 simulator has been used and comparisons are made with the basic DSR protocol. This Security Enabled DSR (SEDSR) ensures security goals and can withstand against single node compromise [6].

Existing proposals are typically based on one specific attack. They would work better in the presence of designated attacks, but there are many other unanticipated or combined attacks that remain undiscovered. Maximum of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research may be done on the robust key management system, trust-based protocols, integrated tends to routing security, and data security at different layers. Security must be ensured in the entire system including the security primitives, such as key management protocols, since overall security level is determined by the system's weakest point [7].

The main security issues in MANETs. They have most of the problems of wired networks and many more besides due to their specific features: dynamic topology, limited resources (e.g. bandwidth, power), deficiency of central management points. Firstly we have presented specific vulnerabilities of this new environment. Then surveyed the attacks exploit these vulnerabilities and, proactive and reactive results proposed in the literature. Attacks are classified into passive and active attacks at the top level. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insider attacks are analyzed on our exemplar routing protocol AODV [8].

An encryption keys creation technique for MANETs based on The Diffie-Hellman key exchange. The technique is very simple and reserves the ad hoc nature of MANETs. By publishing this work, we are trying to initiate a paradigm shift in securing MANETs. In the new paradigm that we are proposing, the focus should be on building security primitives purposely for MANETs, and not on adapting primitives that were meant for conventional wired networks [9].

Importance of MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, without wired shared medium, heterogeneous resources and stringent resource constraints etc. It reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and maintenance, secure architecture, intrusion detection and protection etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities Similarly MANETs security can also be exploited due to its distributed nature. Ad-Hoc networks pose an interesting problem in networking with

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

dynamic routing and highly insecure working environment Need of Secure, Scalable, Reliable, Efficient algorithms for Key management and Routing[10].

5. PRESENT WORK

Diffie-Hellman is the popular key exchange and secure path establishment algorithm. In this algorithm we use asymmetric key cryptography to establish secure path between the sender and receiver. Both the communicating parties select the private and publish keys to establish secure channel for communication. The Diffie-Hellman Algorithm works as follows:

Assumptions:-

- G is a finite cyclic group with a generator g.
- A and B are two entities who want to establish a shared secret key.

Steps: -

1. A chooses a large random number x such that 0<x<p-1 and calculate R1=gx mod p
2. B chooses a large random number y such that 0<y<p-1 and calculate R2= gy mod p
3. A sends R1 to B .
4. B sends R2 to A
5. A calculates K=(R2)x mod p.
6. B calculates K=(R1)y mod p.
7. Values of keys should be same.

Limitations of Diffie-Hellman Algorithm:-

The Diffie-Hellman protocol that employed in MANET is primarily subjected to two types of attacks:-

- Brute force attack
- Man-in-middle attack

In a brute force attack, an attacker may exhaustively try all possible keys to decrypt an encrypted message. In successfully performing such an attack would be equivalent to solving the discrete logarithm problem. This is a difficult problem. In a man-in-the-middle attack, a third malicious entity presents itself as a legitimate entity in the protocol exchange. For example, a malicious principle C can pretend to be principle B with regard to the exchange with principle A and pretend to be A with regard to B.

6. OUR PROPOSED METHODOLOGY

Simulation Scenario steps to be implemented in Network Simulator.

Step-1 Defining parameters

Provide the information for different types of layers such as: channel, radio interface, MAC, interface queue type, link layer, antenna, topography, Max packet in ifq, routing protocol used, number of mobile nodes used, simulation time etc.

Step-2 Define global variables for creating simulator trace file objects as required.

Step-3 Create General Operation Director (GOD) such as:

Step-4 Create mobile nodes: - set node (0) [$ns node]

Step-5 Generate topology

Step-6 Applying optimal asymmetric encryption padding algorithm.

Step-7 Assign traffic pattern for the network

Step-8 Define a finish procedure.

Step-9 Set the start and stop time for the simulator.

7. RESULTS

In our proposed work we have successfully implemented Optimal Asymmetric Encryption Padding Algorithm in Mobile Ad-hoc Network. Firstly, we have reduced the complexity of the algorithm by reducing the number of steps for the Encryption and Decryption of the text. Secondly, we have implemented the modified algorithm in MANET and verified the performance in form of graphs. Parameters considered for graphs are:-

Simulation Assumptions:

- Ubuntu version:- 13.10
- Simulator version: - NS-2.35
- Number of Nodes:- 10
- Area:- 800x800
- Protocol :- AODV
- Channel:- Wireless
- Queue length :- 50
- Antenna type :- Omni-Antenna
- Simulation End Time:- 4
- Propagation:- Two Ray Ground

Throughput: - Throughput is the ratio of number of packets received successfully by a node within a given period of time. Throughput of the network fluctuates with respect to time depends upon the size of the interface queue. Graph below indicates the throughput of the algorithm at different intervals of time.

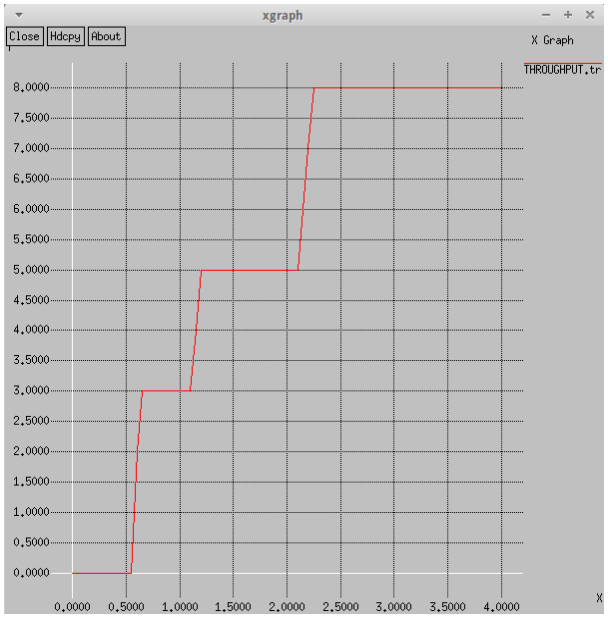

Figure 1: Throughput

Packet Loss Ratio: - Packet loss is the failure of one or more transmitted packets to arrive at destination.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

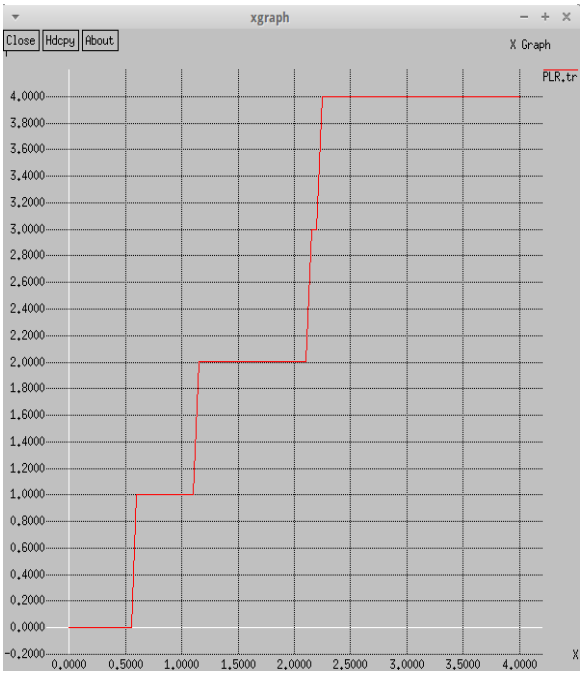

Figure 2: Packet Loss Ratio

8. CONCLUSION AND FUTURE SCOPE

In this research, Optimal Asymmetric Encryption padding algorithm is implemented in Mobile Ad-hoc Networks. We have successfully reduced the complexity of the algorithm and thus maximized the battery life of Mobile nodes. In the same way many other complex algorithms such as DES, AES, RSA can be modified and implemented in Mobile ad-hoc Networks with minimal compromise of Security. Our proposed work not only provides security and confidentiality but integrity of data also. Therefore, it is very important to cover all the security aspects before implementing a particular security algorithm in an open wireless Network

REFERENCES

[1] Dr. Sapna Gambhir, Parul Tomar(2012) "Optimal Path Selection Routing Protocol in MANETs" International Journal of Scientific & Engineering Research Volume 3, Issue 7, June-2012 1ISSN 2229-5518 IJSER © 2012

[2] G.Poornima1, Mr. M Rajasenathipathi (2013) "REVIEW ON ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013 ISSN: 2278 – 1323.

[3] P.S. Patheja , Akhilesh A. Waoo , Lokesh Malviya (2012) "Multipath Dynanic Source Routing Protocol for Ad-Hoc Network", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 3, March 2012.

[4] E. Sivajothi, N. Vijayalakshmi, A. Swaminathan, Dr. P. Vivekanandan (2013) "An Overview of Route Discovery Mechanisms of Multicast Routing Protocols for MANETs", International Journal of Engineering and Technology (IJET) ISSN : 0975-4024 Vol 5 No 5 Oct-Nov 2013 3958.

[5] Priya Shrivastava, Sushil Kumar Manish, Shrivastava (2014) "Study of Mobile Ad hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 86 – No 3, January 2014.

[6] Aruna Sanjay Khubalkar, Dr. Lata R. Ragha (2013) "Security Enabled DSR for Establishing Symmetric Key and Security in MANETs" 978-1-4673-5999-3/13/$31.00 ©2013 IEEE

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei (2006) "A Survey of Various Attacks in Mobile Adhoc Networks" International Journal of Computer Science and Mobile Computing Vol.2 Issue. 10, October- 2013, pg. 171-185

[8] Sevil Şen, John A. Clark, Juan E. Tapiador "Security Threats in Mobile Ad Hoc Networks"University of York, YO10 5DD, UK.

[9] Abdulrahman H. Altalhi (2013) "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks" Communications and Network Vol. 4 No. 1 (2013) , Article ID: 17503 , 5 pagesDOI:10.4236/cn.2013.41011

[10] Garg Nishu, Mahapatra R. P (2009) "MANET Security Issue" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.