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

Implementing Rabin Cryptosystem in iMANET and Comparison with RSA Cryptosystem

Harpreet Kaur[1], Parminder Singh[2]

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

Abstract: *An approach to providing wireless connectivity is through the formation of a mobile ad hoc network. A mobile ad hoc network (MANET) is a collection of mobile nodes that temporarily integrate with each other to form a network. This type of network does not require the existence of a typical network infrastructure. There is no central entity system in the authority to administer the services and configurations over the network. There are no restrictions on the movements of the nodes. It also allows node to join and leave the network liberally without affecting the network's operability. One of the important challenges that the MANETs still face is providing secure communication between the Mobile nodes. In this paper we are modifying Rabin cryptosystem and then we will apply this algorithm in Mobile ad-hoc networks. The Rabin Cryptosystem is an asymmetric key encryption based on number-theoretic problems related to the hardness of factoring. In terms of efficiency, the Rabin encryption process requires to compute roots modulo n more efficient then the RSA which requires the computation of nth powers. Rabin cryptosystem is secure against a chosen plaintext attacks. It is possible to prove that the problem of the Rabin cryptosystem is as hard as integer factorization, while hardness of solving the RSA problem is not possible to relate to the hardness of factoring, that makes the Rabin cryptosystem more secure in this way than the RSA. We have also Compared Rabin Cryptosystem with RSA Cryptosystem for analyzing the performance.*

Keywords: *MANET (mobile ad hoc network), RSA, DSS, AODV protocol, energy level.*

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are autonomously self-organized networks without any type of framework support. In a mobile ad hoc network, nodes move arbitrarily; therefore the network may experience rapid and unpredictable topology changes. Because the nodes in a MANET normally have limited range of transmission, some nodes cannot communicate directly with each other. Hence, routing tracks in mobile ad hoc networks potentially contain numerous hops, and every node in mobile ad hoc networks has the responsibility to perform like a router. Unlike devices in traditional Wireless LAN solutions, all nodes are mobile and the topology of the network is changing dynamically in an Ad Hoc Networks, which brings big and great challenges to the security of Ad Hoc Networks. A wide variety of security attacks such as black hole and grey-hole attacks address routing procedure. In the black hole and grey-hole attacks the selfish nodes are refused to forward all or part the traffic received from its neighbors. Security and robustness of the protocol will be improved if nodes could make informed decisions regarding route selection based on transmitted route requests and extra information enclosed in received route replies[1][9].

MANETs lack central administration and pre-existing organization, so the security issues are different and thus requires different security mechanisms than in conventional networks. Wireless links in MANET make them more prostrate to attacks. It is easier for hackers to attack these networks easily and thus gain access to confidential information. They may be directly attack the network to delete messages, add malicious messages, or dissimulation as a node. This disrupts the network goals of integrity, confidentiality, authenticity and authorization. MANET require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, such as battlefields during wars, military applications,

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

and bailed out situations at the time of disasters[2].

2. ATTACKS ON MANETS

There are various kinds of attacks on ad hoc network which are following:

Location Disclosure- Location disclosure is an attack that targets the confidentiality requirements of an ad hoc network. By using traffic analysis techniques, simpler astute and monitoring approaches, an attacker is able to detect the section of a node, or the structure of the whole network.

Black Hole- In a black hole attack a malicious node add false route responses to the route requests, announcing it as having the smallest path to a destination. These fraudulent replies can be fabricated to alter network traffic through the malicious node for simply to attract all traffic towards it in order to perform a denial of service attack by abandon the received packets.

Wormhole- The wormhole attack is one of the most powerful presented here since it involves the cooperation between two nasty nodes that participate in the network. The connection between the nodes that have established paths over the wormhole link is completely under the control of the two connive attackers. The packet strap is the solution to this attack.

Blackmail- This attack is relevant against routing protocols that use mechanisms for the identification of nasty nodes and propagate messages that try to blacklist the attacker. An attacker may construct such reporting messages and try to confine legitimate nodes from the network.

Denial of Service- Denial of service attacks aim at the complete disruption of the routing function and therefore the complete operation of the ad hoc network. In a routing table format overflow attack the malicious links floods the network with fraudulent route creation packets in order to consume the resources of the participating nodes and disturb the establishment of legal routes.

Routing Table Poisoning- Routing protocols maintain tables that provide information regarding routes of the network. In these kind of attacks, the malicious links generate and send fabricated signaling traffic, or update legitimate messages from other nodes, in order to injects false entries in the tables of the participating nodes[2] [8].

3. MANET PROTOCOLS

Destination Sequenced Distance Vector (DSDV) Protocol: The destination sequenced distance vector routing protocol is a proactive routing protocol which is a updating of conventional Bellman-Ford routing algorithm. This protocol injects a new attribute, sequence number, to each route table entry at every node. Routing table is maintained at every node and with this table, node exchange the packets to another nodes in the network [3].

Ad-hoc On-Demand Distance Vector (AODV) Protocol: AODV algorithm was motivated by the limited bandwidth that is available in the media which are used for wireless communications. It bring in most of the advantageous concept from DSDV algorithm. The required route discovery and hop-by-hop routing, management of node sequence numbers from DSDV make the algorithm cope up with topology and routing information.

Dynamic Source Routing Protocol (DSR): The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node provide routing table containing information about the routes to destination. The nodes modify entries in the route cache as it learns about new routes.[10]

Associativity Based Routing (ABR): The Associativity Based Routing (ABR) protocol is a new scheme for routing. It defines a new metric for routing called as the degree of association stability. It is free of loops, deadlock, and packet delicacy. In ABR, a route is selected on the basis of associativity states of nodes.[4]

Temporally Ordered Routing Algorithm (TORA): The Temporally Ordered Routing Algorithm is one of the efficient and expandable distributed routing algorithm based on the idea of link reversal. TORA is used for highly dynamic mobile network and multi-path wireless networks.[5]

4. LITERATURE SURVEY

Exchange of confidential values in MANET is inconsistent and computationally insecure due to its dynamic nature. In past years, key generation, encryption and decryption have emerge as important techniques for providing secure routing in MANETs. Many researchers are participating in solving the secret sharing

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

problem. Shamir's proposal is one of the prominent secret sharing schemes. However, this scheme does not add secure key generation. This research explains the use of the mathematical theory of Chinese remainder theorem combine with the commonly used RSA for generating keys .Computational complexity of CRT is less than RSA modular exponentiation scheme. This aid to reduce the computational problems. Once a secure key has been generated, it has been pre-owned for finding a secure route between source and destination. The final path is selected based on the highest weighted trust value of the routes. The three phased access is aimed to increase the overall performance.

In this proposed protocol encryption is done using RSA and decryption is done using CRT because computational cost of CRT is less than RSA modular exponentiation scheme. In addition the scheme can detect malicious node and broadcasts the information to all the nodes in the network. After detecting several secure routes, source node considers the route as most secure one whose average weight is maximum. Weight of a node at particular time duration is determined by its trust value, existing battery power and mobility at that time. This way source node selects route for sending messages to the destination which is most trust worthy, powerful and stable among all selected secure routes in the network. The entire process is repeated from time to time to propagate messages from source to destination through the most secure routes. This paper proposes a new security scheme in MANET.[6]

Mobile ad hoc networks (MANETs) have received considerable attention while their special characteristics make them vulnerable against different attacks. In this paper a new deterministic scheme for key management in MANETs is explained. Since public and private keys in this algorithm have an unforgeable relationship, there is no usage for any certificate. Proposed scheme assign the role of the key generation center (KGC) among all nodes, therefore the private key is issued by assigned KGCs (DKGCs) and the node itself. Moreover, each pair of nodes can share a symmetric key in a non-interactive way while communicating with each other. The deterministic scheme is certificate-less, does not require any devoted authority and also it can solve the key insurance problem. Since there are some limitations for memory and process capabilities in MANETs, storing all the keys in whole nodes is not efficient, even if possible. This problem is more highlighted in large-scale MANETs. In this paper we proposed a novel key management algorithm for large-scale MANETs. The proposed algorithm is compared analytically with IMKM and B-BLS algorithms and it is shown that the novel proposed algorithm outperforms the others [7].

5. PREVIOUS WORK

A Schnorr signature is a digital signature produced by the Schnorr signature algorithm. Its security is depending on the intractability of some specified discrete logarithm problems. It is determined the simplest digital signature scheme to be provably secure in a random oracle model.

Choosing parameters

Every users of the signature scheme agree on a group G with generator g of prime order q in which the discrete log problem is hard.

Key generation

- Choose a private signing key x.
- The public verification key is y = gx.

Signing:

To sign a message M:

- Choose a random k.
- Let r = gk
- Let e = H(M | | r), where || denotes concatenation and r is represented as a bit string. H is a cryptographic hash function.
- Let s = (k − xe).

The signature is the pair (s,e).

Verifying

- Let rV = gSye
- Let eV = H(M | | rV)

If eV = e then the signature is verified.

6. OUR PROPOSED METHDOLOGY

Step-1 Defining topological requirements:- Number of nodes, protocol, channel, simulation time etc.

Step-2 Creating a temporary network

Step-3 Handshaking and Connection Establishment

Step-4 Route computation from source to destination by considering various parameters such as hop count, energy level etc.

Step-5 Using an Rabin Cryptosystem for encrypting and decrypting data.

Step-6 Data compression for saving battery life

Step -7 Connection terminations.

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

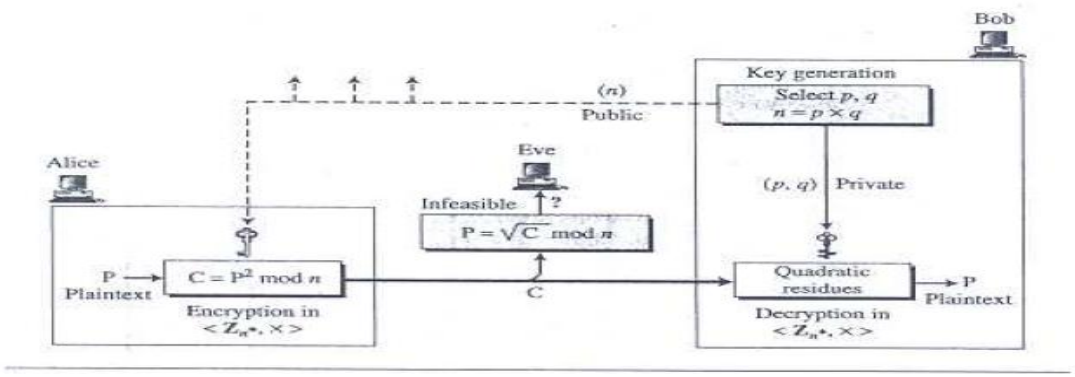

Figure 1: Rabin Cryptosystem

7. RESULTS AND CONCLUSION

In our proposed work, we have implemented Rabin Cryptosystem in Mobile Ad-hoc Network. After implementing RABIN Cryptosystem in MANET we have analyzed its performance on the basis of following parameters:-

- Throughput
- Energy

Throughput is the ratio of number of packets received successfully by a node within a given period of time.

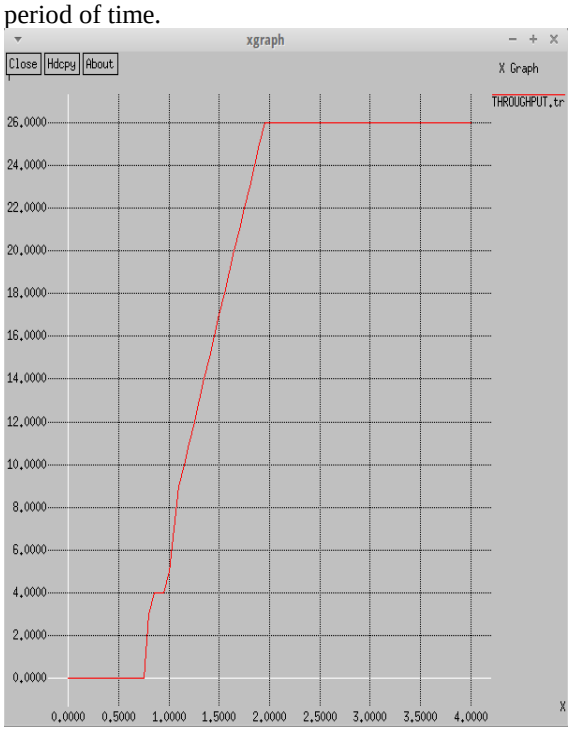

Figure 2 Throughput of Rabin Cryptosystem

Throughput of the network fluctuates with respect to time depends upon the size of the interface queue. Figure below shows the Throughput graph after applying Rabin Cryptosystem. It is evident from graph that the throughput obtained is acceptable.

Graphs below show the energy of each node. Rabin Cryptosystem is simple as compared to RSA. The energy level of nodes in Rabin Cryptosystem is more because of the less computation at nodes. Graphs below also show the Energy consumption by nodes after implementing RSA algorithm. We have concluded that energy consumption is less in RABIN Cryptosystem

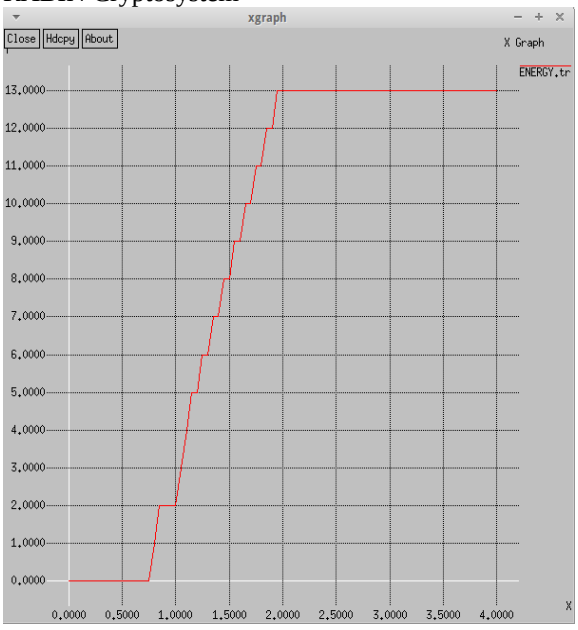

Figure 3 Energy consumption

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

REFERENCES

[1] **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 1 ISSN 2229-5518.**

[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] **Guoyou He *"Destination-Sequenced Distance Vector (DSDV) Protocol"* Helsinki University of Technology.**

[4] **Atul Yadav, Parag Joshi *"Performance of Flat Routing Protocols in MANET'* International Journal of Electronics and Computer Science Engineering 2035 ISSN 2277-1956/V1N4-2035-2041.**

[5] **Vincent D. Park and M. Scott Corsonb (1997) *"A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks"* 0-8186-7780-5/97 $10.00 1997 IEEE.**

[6] **Ditipriya Sinha, Rituparna Chaki, Uma Bhattacharya(2011) *"A Secure Routing Scheme in MANET with CRT based Secret Sharing"* 978-1-4673-4836-2/12/$31.00 ©2012 IEEE 2**

[7] **Zahra Moradlu, Mohammad Ali Doostari, Mohammed Gharib, Ali Movaghar (2013) *"Fully Distributed Self Certified Key Management for Large-Scale MANETs"* 978-1-4799-2481-3/13 $31.00 © 2013 IEEE DOI 10.1109/UIC-ATC.2013.60.**

[8] **Jawandhiya, Pradip M. Mangesh M. Ghonge. PROF. Deshpande J.S. DR. Ali M.S. (2010) *"A Survey of Mobile Ad Hoc Network Attacks"* International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071**

[9] **H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, *"Security in Mobile Ad Hoc Networks: Challenges and Solutions,"* IEEE Wireless Communications,.**

[10] **Parvathavarthini, A. Dr.Dhenakaran S.S (2013) *"An Overview of Routing Protocols in Mobile Ad-Hoc Network"* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 2, February 2013 ISSN: 2277 12**