Khushdeep Kaur, Er.Seema / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.914-917

Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices.

Khushdeep Kaur1, Er. Seema 2

1.Research scholar, 2.Assistant professor

Department of Computer Engineering, Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo

Abstract

Security is the one of the biggest concern in different type of networks. Due to diversify nature of network, security breaching became a common issue in different form of networks. Solutions for network security comes with concepts like cryptography in which distribution of keys have been done. If you want to send data to some other persons through network then if you truly want to keep the information secret, you need to agree on some sort of key that you and he can use to encode/decode messages. But you don't want to keep using the same key, or you will make it easier and easier for others to crack your cipher.

As Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we are focusing on security enhancing by enhancing the level of encryption in network. This study's main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques. In our research we have proposed a combination of DSA, RSA and MD5as a hybrid link for wireless devices. We have also considered case study for Manet networks so that we can suggest the applications of proposed algorithm.

Keywords: RSA, Digital Signatures, Message Digest, Encryption.

1. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

The privacy requirements normally encountered in the traditional paper document world are increasingly expected in Internet transactions today. So with the rapid spread of digital communication networks, there is great need for security and privacy of transmitted data. Therefore, the methods of securing information are becoming a major issue, for which the encryption and decryption systems have been created.

Secure digital communications are necessary for web-based e-commerce, mandated privacy for medical information, etc.Many hardware and software protocols have been implemented to improve the security of information, but the only true method of securing data is to encrypt it. . The national and societal view of the role of encryption will be one of the defining issues for our culture in the twenty-first century. Network security problems can be divided roughly into four intertwined areas: Secrecy, Authentication, Nonrepudiation and Integrity control. Secrecy has to do with keeping information out of hands of unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information non repudiation deals with signature. Security in networking is based on cryptography

Encryption is the vital part of information sharing so we have put our efforts into encryption area for RSA algorithm with DSA powered by MD5 security so that we can make security harder by giving a hybrid algorithm.

2. Problem Formulation:

As Encryption became a vital tool for preventing the threats to data sharing and tool to preserve the data integrity so we have focused on security enhancement by enhancing the level of encryption in network. For required research we have worked on well-known encryption algorithms RSA and DSA with MD5. We have proposed the hybrid algorithm for RSA Algorithm with digital signatures powered by MD5 security with a small case study of applications for this hybrid algorithm.

3. Objectives of the Study

- To study the issues of Security for Different networks. To Harden up the Encryption Process for Network Security
- To study the already implemented algorithms for public key exchange in communication of data.

- To provide a stable encryption, this can make good communication without carrying about data integrity threat.
- To test the performance of mobile device networks for proposed experiment.

4. Research Methodology

To achieve the set objectives, our research focused on the performance measurement of network structure with implementation of Different security algorithm. We have considered RSA, DSA and MD5 algorithm for checking response time, load, throughput and reliability of Ad-hoc networks with implementation of these algorithms. We have considered OLSR protocol for general connectivity in between the ad-hoc network. We have considered different servers like Blade servers for providing different services to network. We start with different scenarios in OPNET simulator for checking out the performance and reliability of the network. Our research focused on these algorithms implementation in Six Phases

1st Phase: This phase contains the basic functionality and layout of network using servers and ad-hoc devices.
2nd Phase: In this phase, we have implemented the different tasks to network by configuring the task management through task manger in OPNET. After configuring tasks, we have configured the traffic type i.e. FTP and HTTP. After all configurations of applications, finally we have configured the profile for different scenarios. We have created topologies with help of Wlan Ethernet Router, Wlan Workstation, Manet Station, Blade servers and Database servers.
3rd Phase: In this phase, we have implemented the different scenarios and different scenarios including a scenario without any security algorithm, a scenario with RSA algorithm, a scenario with DSA algorithm and a scenario with different algorithms (RSA, DSA, MD5).

4th Phase: We have implemented manet protocol i.e. OLSR in network for general routing purposes.
5th Phase: We have done simulation of these networks implemented with different type of security algorithm for 10 minutes in OPNET.

6th Phase: Results from all Scenarios have compared with proposed scenario (with all three algorithm) to fetch parameters like End to End Delay, Overall Throughput, Response time, Packet delivery. Ethernet delay, Traffic receive, Traffic sent, Load etc.

5. Scope and significance of study:

There is an ample scope of research in the stated area. Present study will reflect the importance of security in network and will provides the better encryption technique for currently implemented encryption techniques. It will explore how to tackle with the threats to data integrity and for safe passage of data from one node to another. This research will provides the great feasibility for authentication process improvement for security in network.

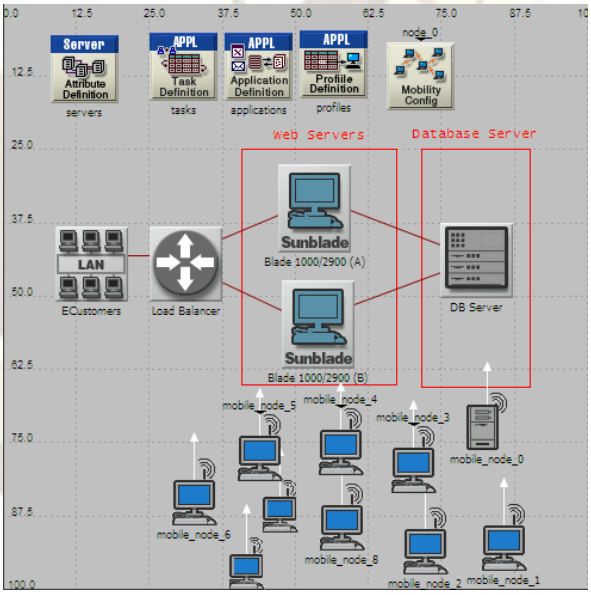
6. SIMULATION AND RESULTS

For evaluation the performance of Manet Network for our proposed work, in this section, we use a simulation tool OPNET to conduct several experiments

A. Simulation environment and parameters

*In our simulations, we consider four different scenarios of sensing area: 100 m*1000m, each is with 10 randomly deployed mobile nodes. The BS is located on the corner of sensing field. Every mobile node is initially equipped with 10m/s speed. We define the database server and two blade servers for testing our proposed research connected with 15 nodes LAN. We used a layer 2 router for load balancing between servers. Different tasks have been implemented by task manager in OPNET according to the server management in Server manager. Applications used are FTP and HTTP for checking the behaviour of traffic filtered by encryption algorithms. Single profile for whole simulation has been done with random waypoint mobility algorithm for mobile nodes.*

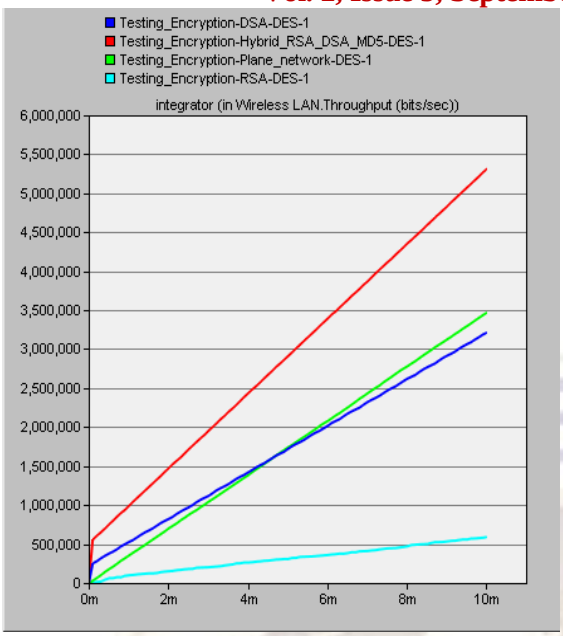
B. Simulation results



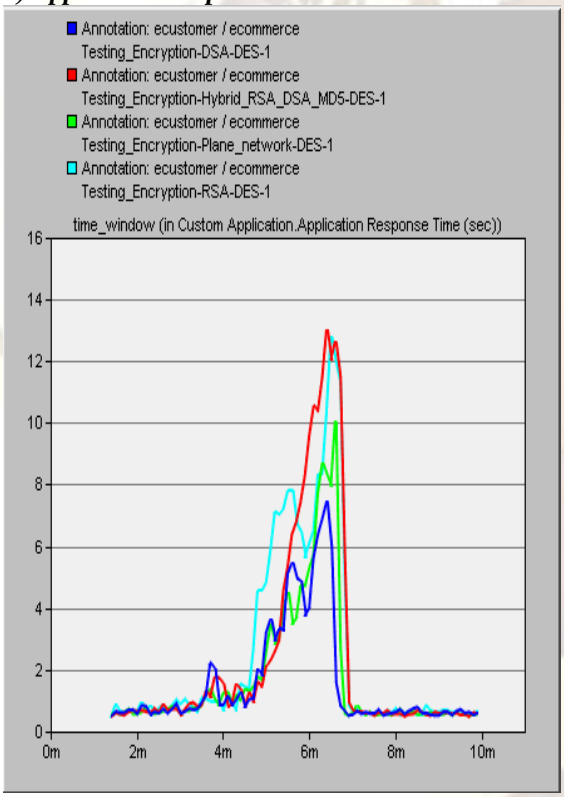
Above Figure shows the simulation scenario for testing different encryption schemes.

Comparison of Our proposed hybrid algorithm with Plane network, Network with RSA, Network with DSA.

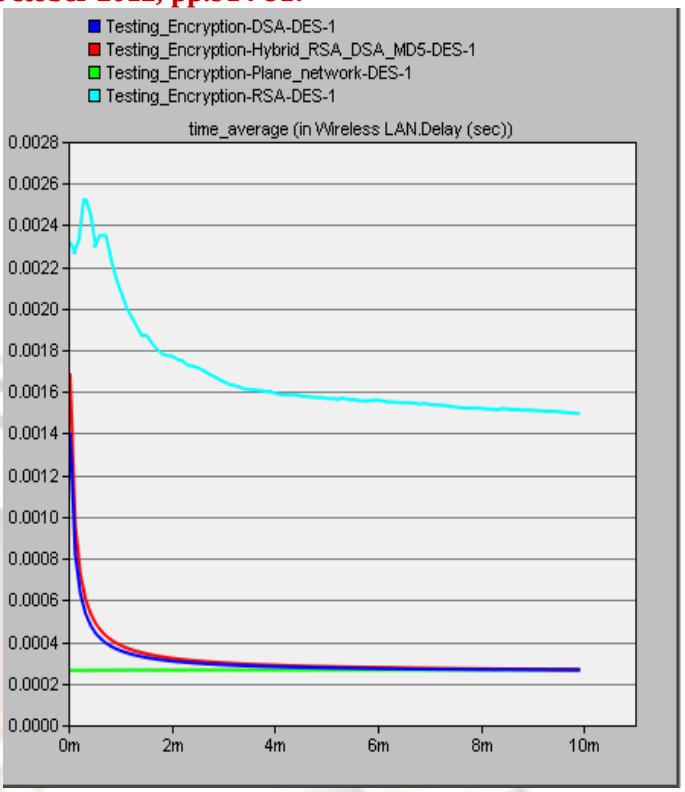
1)Throughput



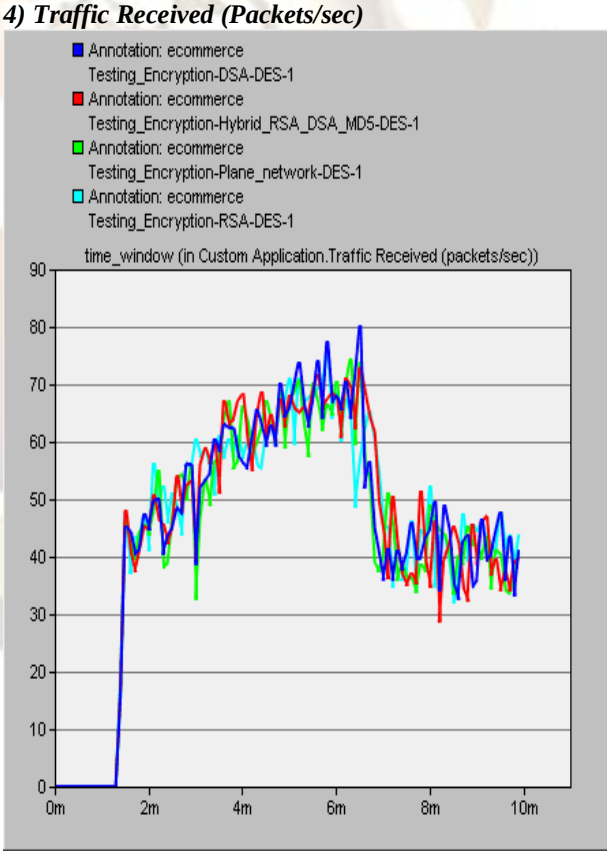
2) ***Application Response Time***



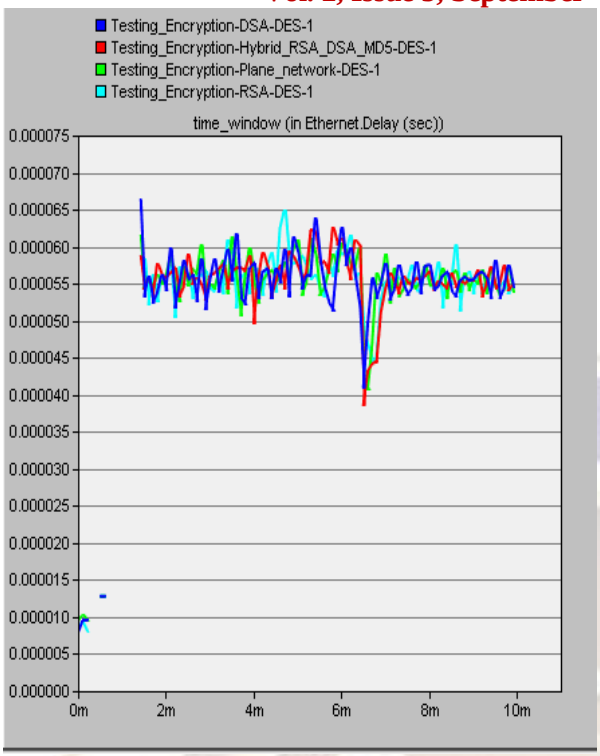
3) Delay



4) Traffic Received (Packets/sec)



5) Ethernet Delay



Overall Comparison in form of table

Parameters	Plane Network	RSA	DSA	Hybrid
Application Response Time	10 seconds	12 seconds	7 seconds	12.3 seconds
Packet Network Delay	0.00052 seconds	0.00053 seconds	0.00053 seconds	0.00051 seconds
Traffic Received	76500 bytes/sec	74000 bytes/sec	82000 bytes/sec	76000 bytes/sec
Traffic Sent	74 packets/sec	76 packets/sec	81 packets/sec	74 packets/sec
Ethernet Delay	0.000041 seconds	0.000051 seconds	0.000052 seconds	0.000038 seconds
Throughput	7000 bits/sec	3750 bits/sec	6000 bits/sec	9000 bits/sec
Load	1650 bits/sec	1400 bits/sec	968 bits/sec	1000 bits/sec

7. CONCLUSION

In this paper, we discuss an efficient and secure hybrid algorithm for providing security to mobile nodes. Since we have tested our proposed algorithm with different scenarios and it is providing better response time, less network delay and best throughput. These parameters have been shown in above table. We got better results than other algorithms so proposed algorithm can be implemented to mobile nodes for security purposes. Also our research shows that it is helping in efficient routing of packet with much less load on servers.

.

References

[1]] B. Schneier, " *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C* ", John Wiley & Sons, Inc., 1996..

[2] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, " Digital Signature Standard (DSS)", june 2009, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8900.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" in 1978.

[4] U. Somani, K. Lakhani, M. Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing". *1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010) 978-1-4244-7674-9/10/©2010 IEEE*

[5] R. Nagpal, " An Introduction to Digital Signatures", *Asian School of Cyber Laws in 2008.*

[6] Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 26 November 2001 .

[7] M.Ayoub Khan, Y.P.Singh, "On the Security of Joint Signature and Hybrid Encryption",*Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication, vol.1, no., pp.1-4,*

[8] R.L. Rivest, A. Shamir, and L. Adleman," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" in 2006.

[9] P. Kitsos, N. Sklavos and O. Koufopavlou," An Efficient Implementation of the Digital Signature Algorithm", VLSI Design Laboratory, Electrical and Computer Engineering Department, University of Patras. Patras, GREECE 2002.

[10] R. Rivest, "The MD5 Message-Digest Algorithm*", RFC 1321, Network Working Group, April 1992.*