Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 3 (2017) pp. 471-479

http://www.ripublication.com

Securing Routing Protocols from External Attacks Using Enhanced Security Mechanism

Sandeep Dalal
Assistant professor, Computer Science and application
DCSA, Maharshi Dayanand, University, Rohtak, Haryana, India.

Jyoti Mahendia* & Neetu Dabas
M.tech Scholar,*
Computer Science and Application
DCSA, Maharshi Dayanand, University, Rohtak, Haryana, India.

Abstract

Routing protocol tells how routers communicate with one other, disseminating information which would enables them to find routes in any two nodes on computer network. Routing algorithms decides specific route. Router had been a priori knowledge of networks attached directly to it. Cryptography is process of changing plaintext using process encryption in cipher text by procedure decryption. Such procedure is used to secure communication between two & more parties within occurrence of third party. In it research paper we discuss Analysis & design algorithm to improve routing protocol & compare novel encryption with existing algorithm.

Keyboard: Ad Hoc, Fibre optics, Co-axial cable, Wireless Cable.

1. INTRODUCTION

Ad Hoc is often used to solutions that are developed on the fly for a important purpose. A Mobile network of Ad hoc NET work is a wireless mobile system nodes that dynamically self-organize with in arbitrary & temporary network topologies. People & vehicles could thus be internet worked with in areas without a pre existing information about structure or when use of such infrastructure requires wireless extension.

Wireless Ad-Hoc Network

Research on Wireless Ad Hoc Networks has been on going for decades. Ad hoc networks have play an significant role with in military applications & related research efforts, for example, global mobile information systems program & near-term digital radio program.

In Recent years have seen a new spate of industrial & commercial applications for wireless ad hoc networks, as viable communication equipment & portable computers become more compact & available.

Security is useful for all types of networks including Wireless Ad Hoc Networks. Security issues for Wireless Ad Hoc Networks are considered more complex as compare to fixed networks. This is due to system constraints with in mobile devices as well as frequent topology changes within Wireless networks. System constraints consist of low-power, small memory & bandwidth, & low battery power.

Routing protocol is considered Ad Hoc networking which is a Latin phrase that means for this purpose. It is often used to explain solutions which are developed on-the-fly for a particular purpose. In case of computer networking, ad hoc network means a network connection which is established for a single session and does not need a router or a wireless base station.

2. LITERATURE REVIEW

C. Sanchez-Avila structure Rijndael cipher (new AES), remarking its main advantages & limitations and its similarities & dissimilarities with DES & T-DES[4].

Susan et.al concluded that Security field is a fast moving career. It defines group of skills required by Network Security as network Security skills emphasize business practices, legal foundations. It aims at attack recognition, network optimization & describes active learning exercises. In order to students within learning such important skills.

Neetu Settia discussed security & attack aspects of cryptographic techniques also discussed dominant problem of security & various attacks. Finally, bench marked few well-known modern cryptographic algorithms within search for best compromise with in security. In research, Cryp Tool was used as a simulator to conduct experiments & to get result.

Punita Meel fundamental mathematics behind AES algorithm along with a brief description of some cryptographic primitives that are commonly used to with in field of communication security system because AES provides best of security & has been less implementation complexity & has been emerged as one of strongest & most efficient algorithms with in existence today.

3. PROBLEM STATEMENT

Security system Threats which are prone to our database and front end.

Data flooding

Not every successful are reading of a tag is useful for the business. More than amount of data could be generated which are not useful to managing inventory or other applications. Every clients are moving a object from one to another shelf, or a pallet load for articles which passes to several readers when it has moved in a warehouse, are events that do not produce data that is meaningful to an inventory control system.

4. PROPOSED WORK

1. Here IP filter is used to reject unauthenticated transmission of packets from server to client.
2. Here enhancement of network security is done by customizing existing encryption techniques.
3. To study loopholes of existing security mechanisms & enhance security of network.
4. To program own socket server & corresponding client to prevent unauthentic access during data transmission.
5. To make use of more complex key during encryption & decryption.
6. To develop a user interface to make client server communication.

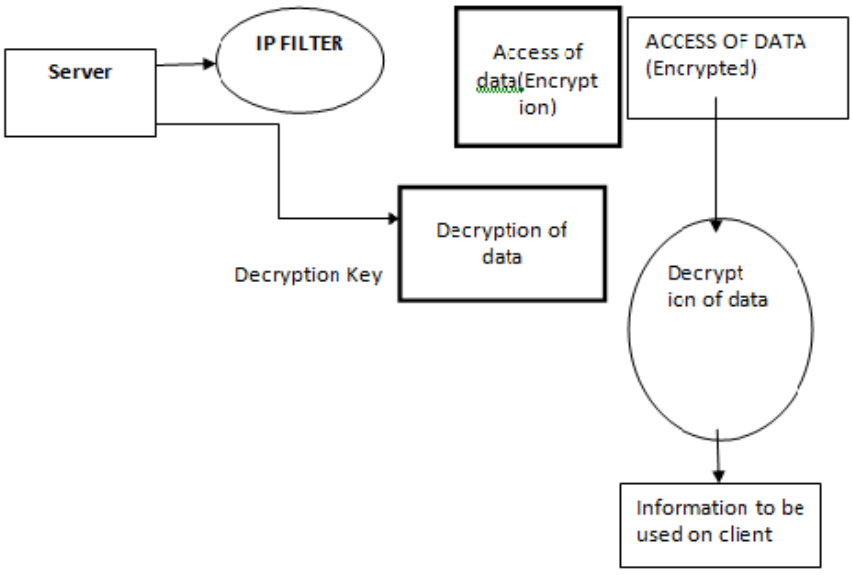

Fig 2. Proposed model

5. DATA ANALYSIS:-

Here reading of packet transmission time in different cases such as fiber optic, coaxial, twisted pair cable is made.

Table 1: Data in case of Fiber optics

Sno	Security Level	H	L	Avg
1	Layer1(cr)	20	40	30
2	Layer2(ip)	15	30	22.5
3	Layer3(otp)	10	20	15
4	L1+L2	40	80	60
5	L1+L3	35	70	52.5
6	L2+L3	30	60	45
7	L1+L2+L3(slow_net)	55	110	82.5
8	L1+L2+L3(avg_net)	50	100	75
9	L1+L2+L3(High_net)	48	96	72
10	L1+L2(avg_net)	45	90	67.5
11	L1+L3(avg_net)	40	80	60
12	L2+L3(avg_net)	35	70	52.5

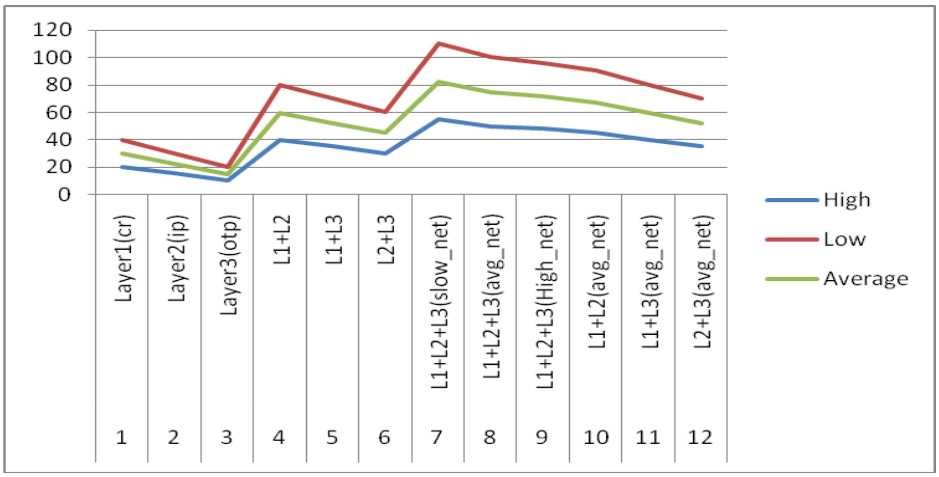

Fig 3. Analysis of transmission speed of packet in case of Fiber optics

Table 2 Data in case of Coaxial Cable

Sno.	Security_Level	H	L	Avg
1	Layer1(cr)	25	50	37.5
2	Layer2(ip)	20	40	30
3	Layer3(otp)	15	30	22.5
4	L1+L2	45	90	67.5
5	L1+L3	40	80	60
6	L2+L3	35	70	52.5
7	L1+L2+L3(slow_net)	60	120	90
8	L1+L2+L3(avg_net)	55	110	82.5
9	L1+L2+L3(High_net)	53	106	79.5
10	L1+L2(avg_net)	50	100	75
11	L1+L3(avg_net)	45	90	67.5
12	L2+L3(avg_net)	40	80	60

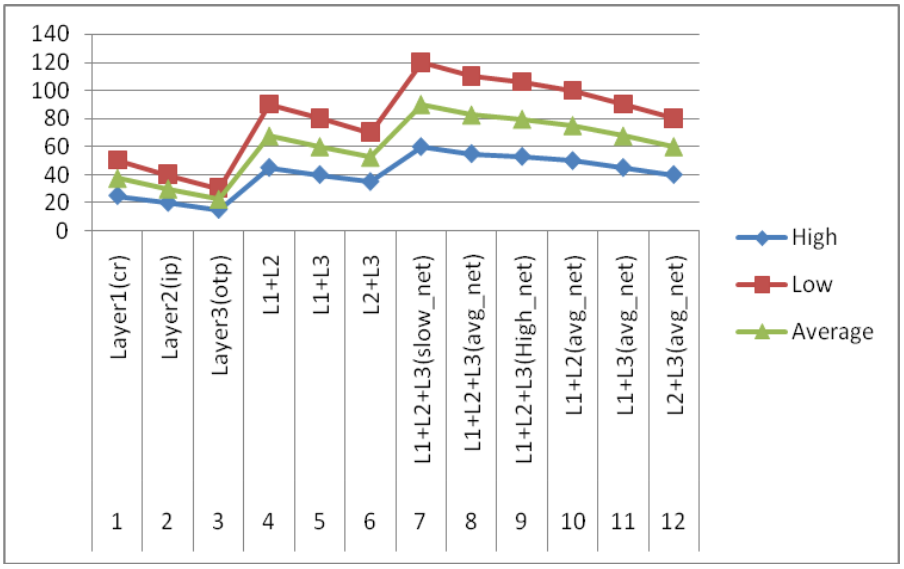

Fig 4. Analysis of transmission speed of packet in case of Coaxial Cable

Table 3 Data in case of Twisted Cable

Sno.	Security_Level	H	L	Avg
1	Layer1(cr)	30	60	45
2	Layer2(ip)	25	50	37.5
3	Layer3(otp)	20	40	30
4	L1+L2	50	100	75
5	L1+L3	45	90	67.5
6	L2+L3	40	80	60
7	L1+L2+L3(slow_net)	65	130	97.5
8	L1+L2+L3(avg_net)	60	120	90
9	L1+L2+L3(High_net)	58	116	87
10	L1+L2(avg_net)	55	110	82.5
11	L1+L3(avg_net)	50	100	75
12	L2+L3(avg_net)	45	90	67.5

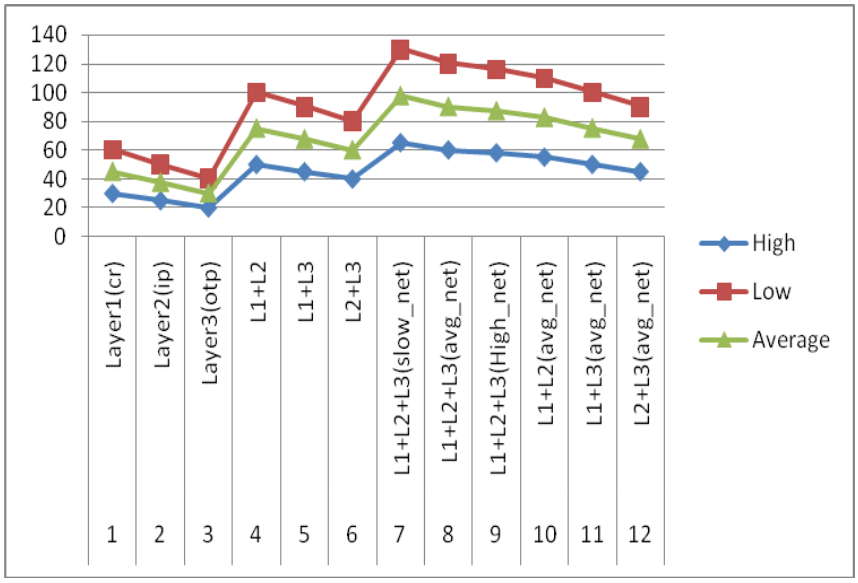

Fig 5. Analysis of transmission speed of packet in case of Twisted Cable

Table 4: Data in case of Wireless Network

Sr. No.	Security_Level	H	L	Avg
1	Layer1(cr)	35	70	52.5
2	Layer2(ip)	30	60	45
3	Layer3(otp)	25	50	37.5
4	L1+L2	55	110	82.5
5	L1+L3	50	100	75
6	L2+L3	45	90	67.5
7	L1+L2+L3(slow_net)	70	140	105
8	L1+L2+L3(avg_net)	65	130	97.5
9	L1+L2+L3(High_net)	63	126	94.5
10	L1+L2(avg_net)	60	120	90
11	L1+L3(avg_net)	60	120	90
12	L2+L3(avg_net)	50	100	75

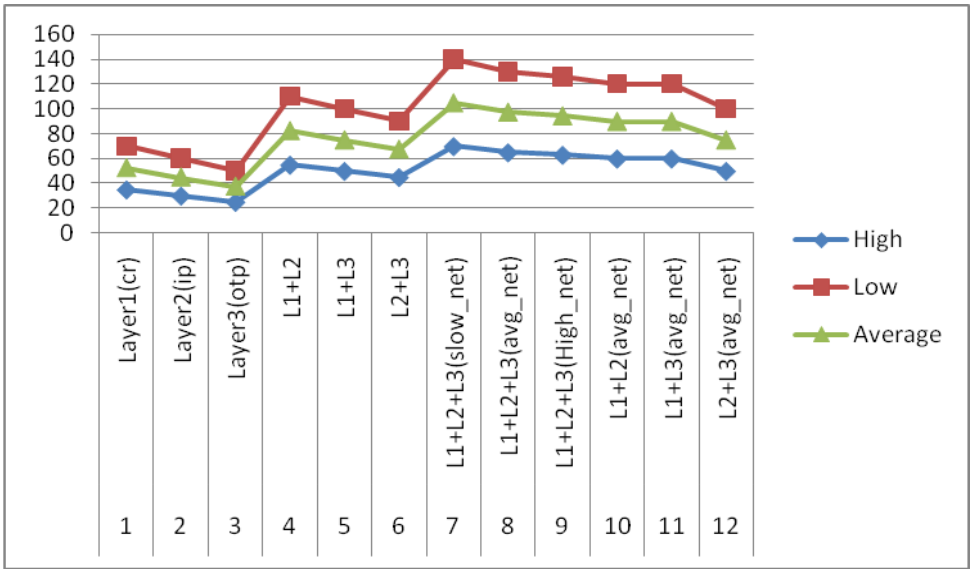

Fig 6. Analysis of transmission speed of packet in case of Wireless network

6. CONCLUSION

Problem of ADHOC Network security is demand of day. The proposed work implementation has enhanced the security of ADHOC Network. Data transmission could be made more than secure from hacker used to by encrypting data on sender side and decrypt it on client side. In order to perform we had been to merge two technologies.

And on the part of Integrated development environment play its best role to develop GUI interface to make system easy to operate by user

I. Socket Programming

II. Data Encryption.

REFERENCES

[1] Abraham, C., Ahuja, V., Ghosh, A.K., and Pakanati, P. (n.d.) "Inventory Management Using Passive RFID Tags: A Survey." [10 August 2007]

[2] AIM UK (n.d.) "RFID Technical Basics." [online] available from [10 August 2007] Andreou, A.G., Kalayjian, Z.K., Apsel, A., Pouliquen, P.O., Athale, R.A., Simonis, G., and Reedy, R. (2001) "Silicon on Sapphire CMOS for Optoelectronic Microsystems." IEEE Circuits and Systems Magazine 1, (3)

[3] Avoine, G. (2007) "Bibliography on Security and Privacy in RFID Systems." [online] available from [10 August 2007]

[4] Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I. (2006)"An Elliptic Curve Processor Suitable For RFID-Tags." Cryptology ePrint Archive [online] Report 2006/227. Available from [10 August 2007]

[5] Baude, P.F., Ender, D.A., Kelley, T.W., Haase, M.A., Muyres, D.V., and Theiss, S.D.(2003) "Organic Semiconductor RFID Transponders." IEEE International Electron Devices Meeting Technical Digest [online] available from [10 August 2007]

[6] Z. Ren, C. J. Anumba, J. Tah, "RFID-facilitated construction materials management (RFID-CMM) - a case study of water-supply project", Advanced Engineering Informatics, Vol.25, No.2, pp. 198-207, 2011.

[7] C. Chao, J. Yang, W. Jen, "Determining technology trends and forecasts of RFID by a historical review and bibliometric analysis from 1991 to 2005", Technovation, Vol.27, pp. 268-279, 2007.

[8] S. Jiang, M. J. Skibniewski, Y. Yuan, C. Sun, Y. Lu, "Ultra-wide band applications in industry: a critical review", Journal of Civil Engineering and Management, Vol.17, No.3, pp. 437-444, 2011.

[9] W. Lu, G. Huang, H. Li, "Scenarios for applying RFID technology in construction project management", Automation in Construction, Vol.20, No.2, pp. 101-106, 2011.

[10] J. Lee, J. Song, K. Oh, N. Gu, "Information lifecycle management with RFID for material control on construction sites", Advanced Engineering Informatics, sVol.27, No.1, pp. 108-119, 2013.

[11] E. J. Jalelkis, M. R. Anderson, C. T. Jahren, Y. Rodriguez S. Njos, "Radio-Frequency Identification Applications in Construction Industry", Journal of Construction Engineering Management, Vol.121, No.2, pp.189-196,1995.

[12] K. Domdouzis, B. Kumar, C. Anumba, "Radio-frequency identification (RFID) applications: a brief introduction", Advanced Engineering Informatics, Vol.21, No.4, pp. 350–355, 2007.

[13] E. W. T. Ngai, K. K. L. Moon, F. J. Riggins, C. Y. Yi, "RFID research: An academic literature review (1995-2005) and future research directions", International Journal of Production Economics, Vol.112, pp. 510-520, 2008.

[14] D. Henrici, "Security and Privacy in large-scale RFID system: challenges and solutions" (PhD dissertation), University of Kaiserslautern, 2008.

[15] J. Landt, "The history of RFID", IEEE Potentials, Vol.24, No.4, pp. 8-11, 2005.

[16] J. Landt, "Shrouds of Time: the history of RFID", AIM, IncUSA, 2001.