© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Enhanced of multilayer Security using Wireless AD-HOC Network in Network Routing

[1]Preeti Makkar, Research Scholar, Department of CSA, CDLU, Sirsa
[2]Dr Raghuvinder (Assistant Professor), Department of CSA, CDLU, Sirsa.

ABSTRACT: W**ireless network** is any type of computer network that uses wireless data/information connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. This implementation takes place at physical level of OSI model network structure. Ad Hoc is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.

Keyword: Server, Technology, Multimedia, Organization, Rick, Partnership, Network, Resource

[1]Introduction

WIRELESS AD-HOC NETWORK

Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program. Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available.

Since their emergence in 1970's, wireless networks have become increasingly popular in the communication industry. These networks provide mobile users with ubiquitous computing capability and information access regardless of the users' location. There are currently two variations of mobile wireless networks: infrastructure and infrastructureless networks. The infrastructured networks have fixed and wired gateways or the fixed Base-Stations which are connected to other Base-Stations through wires.

TYPES OF ATTACK

Five types of attacks are as follow:

1. Passive Attack
2. Active Attack
3. Distributed Attack
4. Insider Attack
5. Close in Attack

HACKING

A **hacker** has been somebody who exploits & seek weaknesses within computer network or computer system. hacker can be motivated by multitude of reasons, such as profit, challenge or protest. grouping that has evolved everywhere hackers has been often referred to as computer underground & these days they are well known community.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

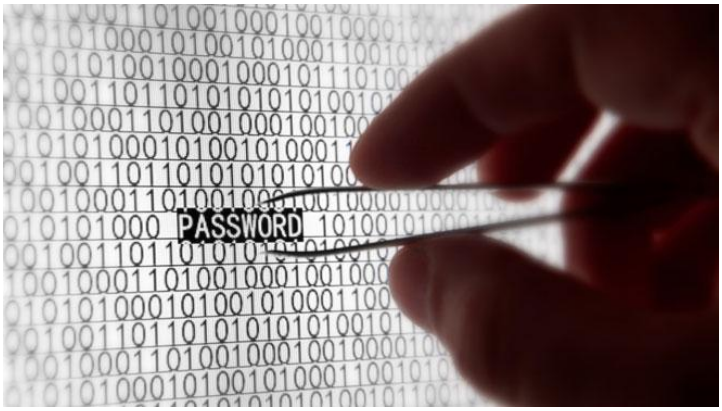

Fig 1. Password cracker

[2] Literature review

Research Titled "**ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES**"[10] published by Natasha Saini, Nitin Pandey & Ajeet Pal Singh focus on various types of security issues which include confidentiality, integrity & availability of data.There exists various threats to security issues traffic analysis, snooping, spoofing, denial of service attack etc. asymmetric key encryption techniques may provide higher level of security but compared to symmetric key encryption Although they have existing techniques symmetric & assymetric key cryptography methods but there exists security concerns.

Raghav Mathur, Vishnu Sharma ans Shruti Agarwal published their research titled "**Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey**" [11] in which they talk about advancements in wireless networking have been initiated idea of mobile computing, where user does not have to be bound to fixed physical location in order to exchange any data benefits of on-the-move connectivity are several but there exist serious networking & security issues that need to be solved before realizing full benefits of mobile computing.

"**A Modified RSA Algorithm to Enhance Security for Digital Signature**"[12]was research paper published by "Sangita A. Jaju, & Santosh S. Chowhan in which they talk about digital signature been providing security services to secure electronic transaction over internet. Rivest, Shamir & Adlemen (RSA) algorithm was most widely used to provide security technique. Here they have modified RSA algorithm to enhance its level of security.

"**Wireless Network Security Using Dynamic Rule Generation of Firewall**" published by Bhushan Chaudhari, Prathmesh Gothankar, Abhishek Iyer & D. D. Ambawade describe wireless computing has evolved tremendously & is being used almost everywhere these days. With the obvious advantage of mobility & easy installation, it also provides service comparable to its wired counterpart. Wireless LANs are implemented in colleges, offices ,campuses, & are fast growing.

[3] Tools & Technology

ADVANCED ENCRYPTION STANDARD

The AES that is known as **Rijndael** , has been specification for encryption of electronic data established by U.S. National Institute of Standards & Technology in 2001. AES has been based on Rijndael cipher developed by two Belgian cryptographers, Joan Daemen & Vincent Rijmen, who submitted proposal to NIST during AES selection process. Rijndael has been family of ciphers with different key & block sizes. For AES, NIST selected three members of Rijndael family, each with block size of 128 bits, but three different key lengths: 128, 192 & 256 bits.

AES has been adopted by U.S. government & has been now used worldwide. It supersedes Data Encryption Standard, which was published in 1977. Algorithm described by AES has been symmetric-key algorithm, meaning same key has been used for both encrypting & decrypting data..

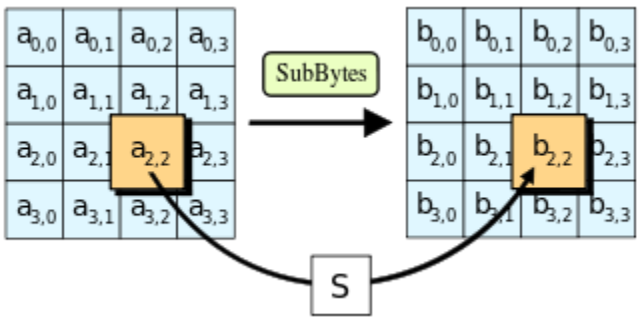

Fig 2 In SubBytes step, each byte in state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

The ShiftRows step

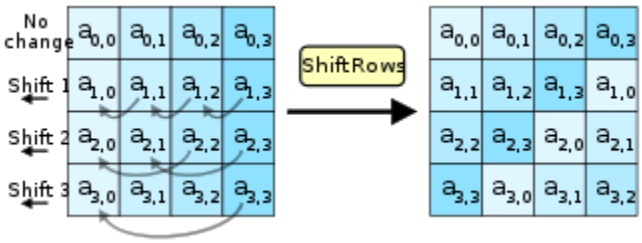

Fig 3 In ShiftRows step, bytes in each row of state are shifted cyclically to left. number of places each byte is shifted differs for each row.

The MixColumns step

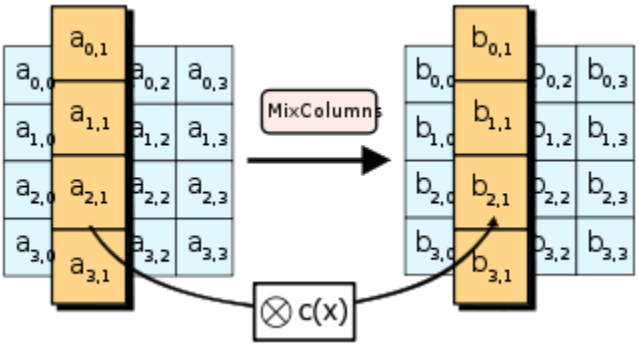

Fig 4 In MixColumns step, each column of state is multiplied with a fixed polynomial *c(x)*.

[4] Proposed Implementation

CHALLENGES TO EXISTING NETWORK SECURITY

Much of theoretical work within cryptography is to cryptographic primitive algorithms with basic cryptographic properties & their relationship to other cryptographic problems. More complex cryptographic tools are then built from these basic primitives. Such primitives provide fundamental properties which are used in development of more complex tools called cryptosystems or cryptographic protocols that guarantee high-level security properties.

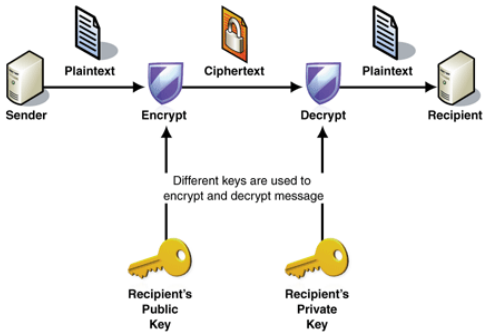

Fig 5 Encryption & decryption

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}
Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig 6 Generation of Key within encryption & decryption

[5] Implementation

In order to simulate encryption & decryption of multimedia file we need following:

Hardware Requirements

- CPU (1GHZ or above)
- RAM(1 GB OR MORE)
- 5GB FREE SPACE IN HARDDISK
- HIGH RESOLUTION MONITOR

Data Analysis work

We have make reading of packet transmission time in different cases such as fiber optic, coaxial, twisted pair cable

Sno	Security_Level	H	L	Avg

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

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

Table 1 Data in case of Fiber optics

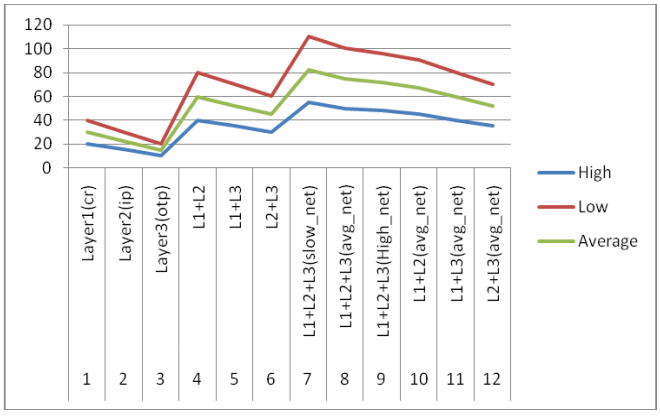

Fig 7 Analysis of transmission speed of packet in case of Fiber optics

Sn.	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

Table 2 Data in case of Coaxial Cable

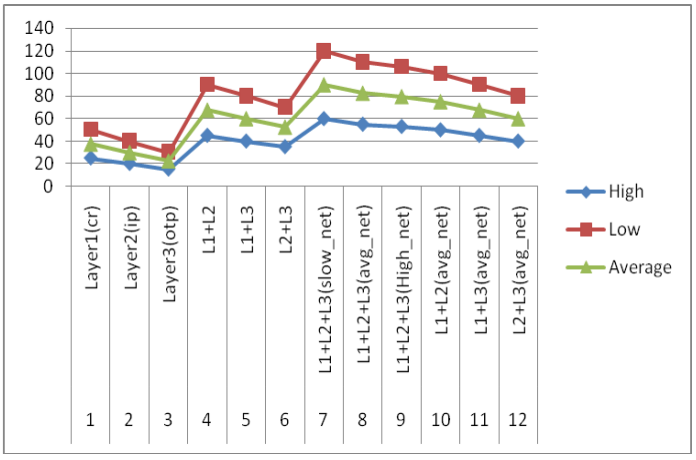

Fig 8 Analysis of transmission speed of packet in

Sno	Security_Level	H	L	Avg

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

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

Table 3 Data in case of Twisted Cable

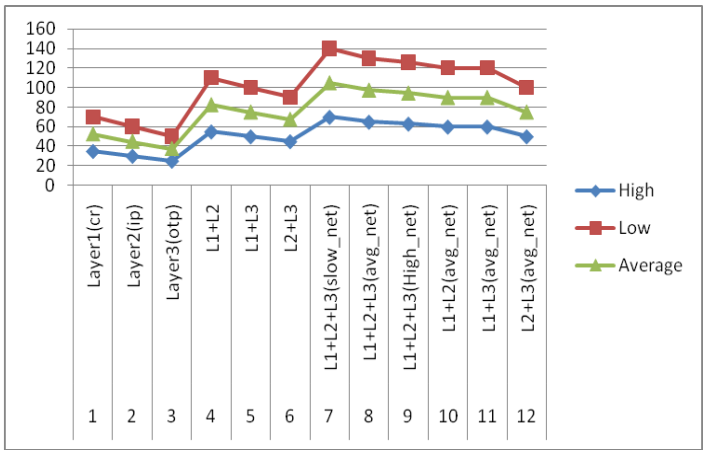

Fig 9 Analysis of transmission speed of packet in case of Wireless network

[6] Conclusion

AD HOC Networking has been still evolving but its benefits are enormous. AD HOC Networking provides excellent support for amazing infrastructures, applications & services such as shared resource pool, broad network base, reduced this cost or rapid elasticity of network to handle varying customers demands as well as AD Hoc network computing various service & deployment models that has been part of main reason for adopting this computing system. Thus this makes network computing open shared system volatile to security breaches & other challenges.

So there has been need to focus on solutions of various challenges to maintain dependence level of organization for deploying AD HOC networking without any hesitation & also need of technical support for elastic scalability to serve ever pressing demand of customer.

References

[1] David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions & One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice & Theory within Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012, Darmstadt, Gerseveral)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein & T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, Distributed Public-Key Cryptography from Weak Secrets, (18_20 march 2009, Irvine, CA, USA), S. Jarecki & G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, Password-Authenticated Group Key Agreement with Adaptive Security & Contributiveness, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, Analysis & design of secure key exchange scheme, Information Sciences 179 (2009) , Elsevier

[10] Research Titled "**ENHANCEMENT OF SECURITY USING CRYPTOGRAPHIC TECHNIQUES**" published by Natasha Saini, Nitin Pandey & Ajeet Pal Singh

[11] Raghav Mathur, Vishnu Sharma ans Shruti Agarwal published their research titled "**Solving Security Issues in Mobile Computing using Cryptography Techniques -A Survey**"

[12] "**A Modified RSA Algorithm to Enhance Security for Digital Signature**" was research paper published by "Sangita A. Jaju, & Santosh S. Chowhan