



Enhancement of Adhoc Wireless network Security by Customized Encryption Technology & using Multilayer of Security

¹Sumit Tuteja, Research Scholar, Geeta Engineering College, Naultha Panipat.

²Mr. Nikhil Sharma ,Assistant Professor , Geeta Engineering College, Naultha Panipat,

Abstract: Ad-hoc Wireless computing proposes new ways to provide services. These pioneering technical & pricing opportunities bring changes within way business operated. Lack of security is only barrier within wide adoption of Wireless Computing. The fastest development in Wireless computing has brought many security issues and challenges for users. Wireless computing offers many benefits, but it is also vulnerable to threats.



© JRPS International Journal for Research Publication & Seminar

[1] INTRODUCTION

A **wireless network** is any type of computer network which is using wireless data connections to enable sharing of information and data [1-3]. Wireless networking is a method by which domestic, telecommunications networks & enterprise installations avoid costly process of introducing cables in a building, due to wireless connection among different equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. Such implementation takes place at physical level of Open System Interface model network structure. The examples of wireless networks consist of cell phone networks, Wireless local networks, wireless sensor networks, satellite communication networks, & terrestrial microwave networks.

[2] TYPES OF WIRELESS NETWORKS

Wire-less PAN

Wireless is a personal area networks interconnect devices within a relatively small area that is commonly with a person's reach. Example, Both Bluetooth radio & invisible infrared light provides a Wireless PAN for interconnecting a headset to a laptop. ZigBee also supports Wireless PAN Applications. Wireless Fidelity PANs are becoming popular as equipment designers are starting to integrate Wireless Fidelity into the variety of consumer electronic devices. Intel My Wireless Fidelity & Windows seven virtual Wireless Fidelity capabilities have made Wi-Fi PANs simpler & easier to setup & configure, so it is very easy to transfer the data between various systems [1, 4].

Wireless LAN

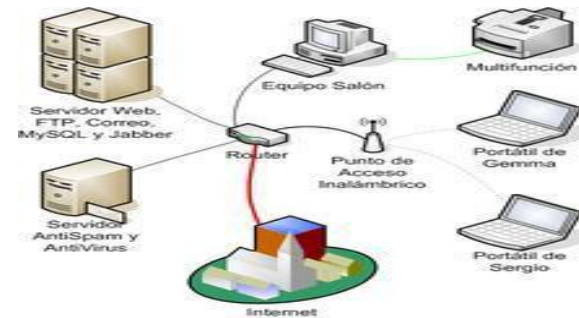


Fig. 1. Wireless Local area Network [4]

Wireless Local area networks is often used for connecting to local resources & to Internet. A wireless local area network (WLAN) links two and more than two devices over short distance using a wireless distribution method, usually providing a connection by defining an access point to access internet. The use for spread-spectrum or OFDM technologies could allow the users to move within a local coverage area, & still remain connected to network [1, 4].

Wireless mesh network

Wireless mesh network is made up for radio nodes organized with a mesh topology. Each node forwards messages on behalf of other nodes. Mesh networks could recover, automatically re-routing a node which has lost its power [1, 4].

Wireless MAN

Wireless metropolitan area networks are a type of wireless network which would connect several wireless LANs. Wireless MAX is a type of Wireless MAN & is described by IEEE 802.16 standard [1, 4].



Wireless WAN

Wireless WAN is a wireless networks that typical covered large areas, like between neighbouring towns & cities, also rural, urban & suburbs. These networks could be used to connect branch offices of business as a public internet access system. Wireless connections among access points are usually point to point microwave links using parabolic dishes on 2.4 GHz band, rather than omnidirectional antennas used with smaller networks. A typical system consists of base station gateways, access points & wireless bridging relays. Other configurations are mesh systems where every access point acts as a relay also. When combined with renewable energy systems like photovoltaic solar panels or wind systems they could be standalone systems [4].

Global area network

A global area network is used for supporting mobile across an arbitrary are number of the wireless LANs, satellite coverage areas, etc. The key challenge in mobile network is Hand's off any user communications from one local coverage area to other. In IEEE Project 802, this consists of a succession of terrestrial wireless LANs [4].

Space network

Space networks are the networks that are used for communication between spacecraft, usually within vicinity of Earth. For example, space network of NASA's [4].

[3] AD-HOC WIRELESS NETWORK

Ad-hoc Wireless Network are portrayed as the arrangement of remote systems that utilization multi-bounce radio exchanging and are fit for working without the assistance of any settled framework, henceforth they are false name foundation less systems. [5, 6]. Remote work organize framework and remote sensor arrange framework are explicit instances of remote impromptu systems [6]. The other sort of remote system is cell arrange otherwise called framework based system. The framework systems have settled and wired portals like the settled Base-stations that are associated with other Base-Stations with the assistance of wires. All hubs is inside the scope of a Base-Station. A Hand-off occurs as portable host goes from scope of one Base-Station to the scope of another and along these lines, cell phone can proceed with correspondence impeccably all through the system. Utilizations of this sort of systems incorporate remote neighbourhood and Mobile Phone. The other kind of remote frameworks, foundation less systems, false name Mobile Ad-hoc Networks (MANET). These have no settled switches, all hubs could be switch, are fit for development and can be associated. In Cellular System, the nearness of

base stations disentangles directing and asset the board, and the steering choices are made in an incorporated way with more data about the goal hub. Be that as it may, in an impromptu remote system framework, directing and asset the executives are done in a disseminated way in which all hubs arrange among themselves to empower correspondence. It requires each hub to be progressively astute with the goal that it capacities both as a system have for transmitting and accepting and as a system switch for directing bundles to and from different hubs. Remote versatile hubs in a specially appointed remote systems are more mind boggling than their partners in cell arranges however they are anything but difficult to introduce and practical in tasks. Ad hoc remote systems, because of their quick and financially savvy organization, discover applications in various zones, for example, in military applications, registering, crisis activities, remote work systems, remote sensor systems, and in crossover remote system structures. There are various techniques used to secure the Ad-hoc data transmission like socket programming [7], some used IP authentication [8], and basic cryptography [9] is used by many researchers, but they are not as much secure in transmitting the data.

[4] CHALLENGES

Lack of security is only barrier within wide adoption of Wireless Ad-hoc technologies [10]. The rapid growth for Wireless technologies have buy more security challenges for users. Wireless technology offers many benefits, but it is also vulnerable to threats. One of the main threat exist today is problem of unauthorized users or entities. To avoid this problem new technique is developed in it is that data owners could share their data with a large number of users, who might want to retrieve certain specific data files they are interested within during a given session.

[5] EXISTING IMPLEMENTATION

Cryptography

Cryptography is the technique to secure information. The term Cryptography is "hidden" derived from Greek kryptos. Cryptography means that hide info in storage or transit using techniques like microdots, merging words with image etc [11,12]. Cryptography is method of changing plain text (ordinary text, such as message) by using encryption technique into cipher text. This cipher text is then converted into plain text again at recipient side by using decryption technique. This system is used in secure transmission



between two parties. Encryption and Decryption steps are used according to predefined algorithm and these are used as discussed below:-

Encryption Steps:-

- Data would be encrypted with in Rivers Shamir Adleman algorithm for example RSA [13].
- A digital envelope is sent to receiver having cipher text encrypted.

Decryption Steps:

The Decryption of message received from sender's side would occur as follows:

- Digital envelope would reach receiver's side.
- Digital envelope would be opened to get encrypted data & decrypt using its own private key with RSA algorithm [13] & receiver get secret picture.
- Thus receiver would get plain text.

[6] PROBLEM STATEMENT

There was issue with existing security framework. In this there are the security threat by crypto analyst. Crypto analyst is individual who could access to change encrypted data into decrypted form using this cracking techniques.

[7] OBJECTIVE OF RESEARCH

Main objective of the research is to secure the data by using multiple layer of security, like integrating IP filtration, defining the port number and given a session for transmission and modifying the cryptographic encryption by combing multiple layer of keys in encryption for secure communication and to upgrade the security of cryptography based wireless network.

[8] PROPOSED MODEL & ANALYSIS

In proposed model we would work on multiple layered security

1. Security layer first would be customized the cryptography algorithm of AES to enhance security.
2. Security layer second used for specific User defined port.
3. Security layer third would be drop packets from an unauthentic IP addresses.

4. In this way we will be able to secure wireless network from external attacks and unauthentic access.

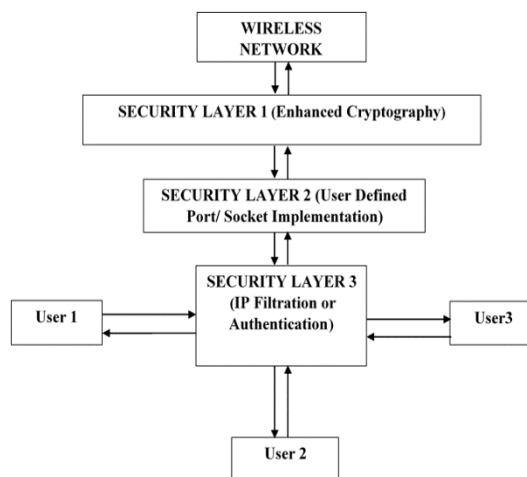


Fig. 2. Multiple Layer Security

• SECURITY LAYER 1

Enhanced Cryptography

In this model an integrated approach to improve cryptography technique used to secure the data. In this three layer cryptography is done like, defining pass key , salt key and vi key , all are combined in this approach by which it is very hard to decode it as we can see in image below even a message hello is coded as seen in figure below.

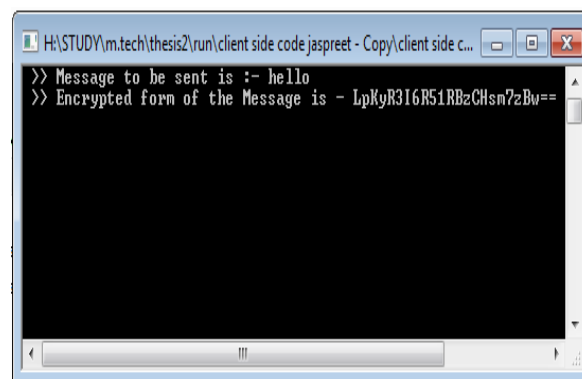


Fig. 3. Encrypted Data

• SECURITY LAYER 2

Socket implementation after Cryptography

Here we would create our server & client communication protocol using own port and socket programming.



- **First step is to define server side port using following algorithm**
 - Create Server Socket object using our own port 8888.
 - Acknowledge client request using Server socket object.
 - Receive data from client in the form of input data stream of object.
 - Convert data stream object to string.
 - Input data stream is within form of cipher data decrypted are using proposed algorithm.
 - The Close Connection.

- **Second step is to create Client side interface to connect the server.**
 - Create Server Socket object using our own port 8888 to connect to server.
 - Encrypt the data to be sent before sending.
 - Send the data using the data output stream object.
 - Clear the output buffer/cache.
 - Terminate connection.

If Server and Client socket matches only then it shows a message Server Client Connected as shown in figure given below and allows the further transmission of data.

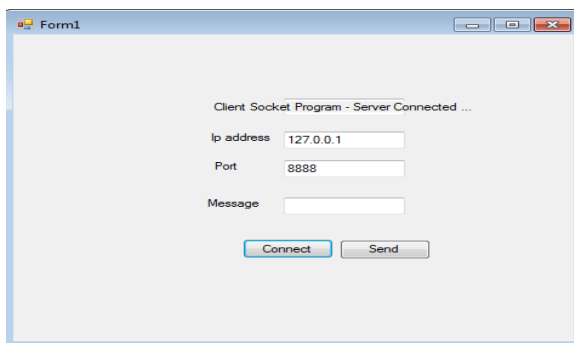


Fig. 4. Socket Matched

If Server and Client socket does not match then it does not allow the client to connect with server and gives a message No Connection could be made because the target machine refuse it as shown in figure given below and no further transmission is allowed.

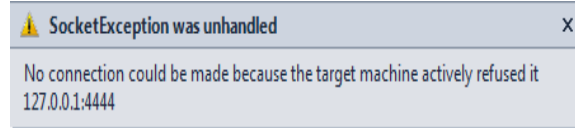


Fig. 5. Socket Mismatch

• SECURITY LAYER 3

IP Filtration

Centralized database of internet protocol address would be created on centralized server and decryption request from authentic internet protocol would be acknowledged. If Internet protocol is not found in database or its status is zero then Decryption would not be allowed. As we can see in image below if IP matches then accepts request otherwise gives an error invalid IP.

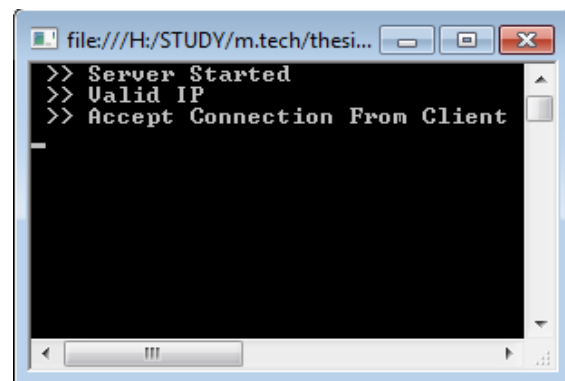


Fig. 6. Accepts Connection

If not matched refused the connection and shows Invalid IP and does not allow the machines to communicate between them and no connection is established.

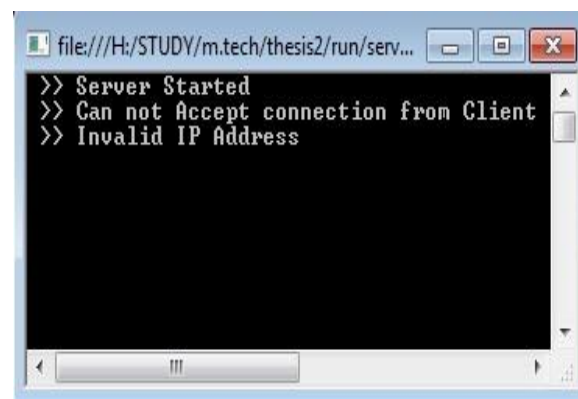
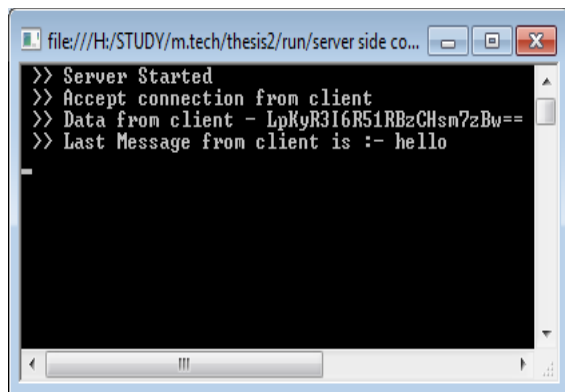


Fig. 7. Invalid IP



Combination of All the three layers

It gives a more secure form of wireless communication in which encrypted data is transmitted and after listening on specific port and IP authentication, it allows data to be decrypted, otherwise refuses it.



```

file:///H:/STUDY/m.tech/thesis2/run/server side co...
>> Server Started
>> Accept connection from client
>> Data from client - LpKyR316R51RBzCHsm7zBw==
>> Last Message from client is :- hello
  
```

Fig. 8. Data Transmitted with Enhanced security

[9] Conclusion & Future Scope

We have enhanced security by enhancing encryption algorithm. Here we have also defined our own ports for server & client & defined new rules for encryption & decryption & involved multiple layer of security like internet protocol Filter this would definitely improve security mechanism within Wireless computing environment.

Future study could be made on various networks and topology and additional one time password should be implemented as an Additional security layer in wireless networks.

References

[1] Gast, Matthew S., 2005, *802.11 Wireless Networks: The Definitive Guide, 2nd Edition*, O'Reilly Media, Inc., Sebastopol, CA, USA, pp. 23-33.

[2] Steve Rockley, 2007, *Wireless Network Technology*, Elsevier Linacre House, Jordan Hill, Burlington MA.

[3] Benny, H., Kumar, C. S., Deepthi, D.V.V., Rao, S. K., and Raju, G. S.V.P., 2013 "Overcome of Router/Gateway Problems in Wireless Networks", *International Journal on Advanced Computer Theory and Engineering (IJACTE)*, vol. 2 (5), pp. 66-67.

[4] Wikipedia Contributor's, 2016, "Wireless Networks", [online]. Available: <https://en.wiki>

[pedia.org/w/index.php?title=Wireless_network&oldid=721993952](https://en.wikipedia.org/w/index.php?title=Wireless_network&oldid=721993952). [Accessed May 26, 2016].

[5] C.Siva Ram Murthy and B.S.Manoj, 2004, *Ad Hoc Wireless Networks – Architectures and Protocols*, Pearson Education, Upper Saddle River, New Jersey.

[6] C.K.Toth, 2002, *Ad Hoc Mobile Wireless Networks*, Pearson Education, Upper Saddle River, New Jersey.

[7] Kalita, L., 2014, "Socket Programming", *International Journal of Computer Science and Information Technologies*, vol. 5 (3), pp. 4802-4807.

[8] Symantec, (2007), "Overview of IP addressing and subnetting", [Online]. Available: https://support.symantec.com/en_US/article.TEC_H82138.html [Accessed Feb. 3, 2016].

[9] Kahate, A., 2008, *Cryptography and network security*, second edition, TataMc Graw-Hill, New Delhi.

[10] Sarvesh Tanwar, Prema K.V., 2013, "Threats & Security Issues in Ad hoc network: A Survey Report", *International Journal of Soft Computing and Engineering (IJSCE)*, vol.2 (6), pp.138-143.

[11] Aggarwal, S., Jaiswal, U., 2011, "Kryptos+Graphein =Cryptography", *International Journal of Engineering Science and Technology (IJEST)*, vol. 3 (9), pp. 7080-7084.

[12] Vahed, A., AL., and Sakhavi, H., 2011, "An overview of modern cryptography", *World Applied Programming*, vol. 1 (1), pp. 55-61.

[13] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L., 1978, "A method for obtaining digital signatures and public-key cryptosystems", *CACM*, vol. 21(2), pp. 120-126.