ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cluster Based Authentication algorithm to deliver packet data over 802.11

Rajwinder Kaur*
M. Tech (C.S.E.)
C.E.C. Landran, Mohali.,
Shahkot, India
rajkhinda18@gmail.com

Mr. Sandeep Singh Kang
(Sr. Lecturer)
C.E.C. Landran, Mohali.,
Amritsar, India
sskang4u1@rediffmail.com

Hina Wadhwan
M. Tech (C.S.E.)
C.E.C. Landran, Mohali.,
Bathinda, India
hinawadhawan@gmail.com

Abstract: In the near future, computing environment can be expected based on the recent progresses and advances in computing and communication technologies. Next generation of mobile communications will include both prestigious infrastructure wireless networks. IEEE Standards 802 ease the deployment of networking infrastructures and provides employers to access corporate networks while travelling. These standards provide two modes of communication called infrastructure and ad hoc modes. At present Wireless network has been deployed worldwide, but some security issues in wireless network might have prevented its further acceptance. IEEE 802.1X specification is a technique for port-based network handover control and one of the solutions to overcome the limitation of wireless network security, which is based on Rivest, Shamir and Adleman. It is an authentication framework that can support public-key cryptography. Base station algorithm involves three steps: key generation, password based encryption, decryption between base stations and it is flexible in its implementation. Protocol is safe against all type of passive and active attack; and the authenticator authenticate each other which reduces the authentication packet loss and encryption/decryption time.

Keywords: IEEE 802.11, Wireless, Simulation, Network security and Performance, EAP**.**

I. INTRODUCTION

The ease improvement of 802.11 technologies results in wide applications in our daily lives. Wireless communications provide benefits such as flexibility, mobility, portability and low deploy cost for organizations and users. Mobile devices like PDAs, laptops and mobile phones are widely used for various purposes: accessing emails, sharing files, real-time communications etc. While value-added service providers are relying on wireless technologies to provide services to their clients in a more convenient way. Wireless technologies provide different capabilities that satisfy different users and requirements.

Wireless local area networks (WLAN), such as IEEE 802.11; [3] provide short-range, high-speed wireless data connections between mobile devices and nearby access points. Wireless personal area networks like Bluetooth provide a method for interconnecting devices centred on an individual person's workspace. Providing a wireless coverage larger than WLAN, wireless metropolitan area networks (WMAN) enable users to establish wireless connections between multiple places within a metropolitan area like a city campus. However, a wireless ad hoc network is a self-organized infrastructure less network formed by a group of mobile nodes [15]. Such a network provides great advantage and flexibility for users since no infrastructure is required within the network.

A. 802.11 Architecture:

The 802.11 architecture comprises several components and services that interact to provide station mobility invisible to the higher layers of the network stack. The LAN station in wireless is the most basic component of the wireless network.

Typically the 802.11 functions are implemented in the hardware and software of a network interface card. A station could be a laptop, a handheld device, or an access point [16]. Stations may be mobile, portable and all stations support the 802.11 station services of authentication, de-authentication, privacy, and data delivery. Wireless access points are commonly built into broadband routers, providing both wired and wireless connectivity for a small network. A typical architecture of wireless LAN is illustrated in Fig. 2.1. The access points are connected by the backbone network to provide wireless access and services for mobile stations [8].

II. RELATED WORK

A. Security Issues in 802.11:

Security issues in wireless networks can be considered from two aspects: security requirements, security attacks. Various security mechanisms are designed to fulfil security requirements so as to counter against different security attacks. Due to characteristics and constraints of wireless

networks, wireless networks are facing more security threats than wired counterparts. In this section, we discuss these two aspects of security issues for wireless networks in detail, respectively.

a. Security Attacks:

Security research in traditional networks has identifies various attacks against communicating parties, and such attacks can be also applied against wireless networks. Generally, these attacks can be divided into two major types:-

i. Passive Attacks: - This kind of attack targets at collecting valuable information from the network. The information includes transferred data, the identification of communicating nodes, node location and network topology. Eavesdropping is the most simple and effective type of wireless attack. This kind of attach leaves no trace of the hacker's presence on or near the network. This kind of attack is also the most difficult to be detected.

ii. Active Attacks: - Active attackers try to disrupt the normal operation of nodes in the network or try to damage data or even try to bring the whole network down. These attacks can be divided into following major types:-

b. Security Requirements: -

In traditional networks, authentication, confidentiality and integrity are the three fundamental security requirements studied for tens of years in research. These requirements are also basic objectives in wireless environments.

Authentication means that a communication partner can be unambiguously identified during the communication. Sometimes only unilateral authentication is enough for secure communication, while mutual authentication is desired to avoid attacks in most cases. Various authentication protocols are employed to provide mutual authentication for communication networks.

Non-repudiation this requirement prevents either the sender or the receiver from denying a transmitted message, and digital signature is usually used to provide non-repudiation as well as integrity.

Confidentiality means that the exchanged information during the communication is not disclosed to unauthorized parties. Encryption, implemented by stream ciphers and block ciphers, is used to achieve confidentiality.

B. Wireless LAN Authentication:

EAP authentication method implemented in wireless LAN infrastructure network. Describes three essential factors that influence the choice of authentication method, which are security requirements, performance.

a. Security Phases :

Prior concern to the implementation of authentication protocol is the security factor. The design of EAP method must address the threats outlined in EAP standard. Using EAP security threat model, a protocol designer would be able to know when he has completed his work by proving that the authentication protocol is able to resist all the threats [12].

b. Performance:

Authentication method should consider the protocol efficiency because users need an instant connection to network. In WLAN network, performance is an important factor in the handoff process. When we enable the security during the handoff process, there must be a technique to tell the new AP and roaming station a secret key (PMK) at a good pace to data communication.

C. Password and Certificate Authentication Protocols:

a. Protected EAP and Tunnelled TLS:

Protected EAP protocol (PEAP) and tunnelled TLS authentication protocol use the secure session negotiated by TLS to protect subsequent client-to-server authentication [3]. These protocols need to protect other authentication protocols against hacking, man-in-the middle and other cryptographic attacks. Besides that, both protocol provide client identity protection when the actual client- to-server authentication occur inside the secure tunnel. The protocols have two phases; in the first phase, TLS handshake is *executed* with the server-to-client authentication by performing server's certificate. In the next phase, for PEAP, the client who was not authenticated with a certificate performs second EAPauthentication in the generated TLS channel..

b. Transport Layer Based Security:

The design of TLS assumes that adversaries have substantial computational resources to capture, modify, delete, replay, and tamper the messages sent over the communication channel and without the knowledge of secret information from sources outside the protocol.[4] The TLS protocol is built from two different layers, TLS record and TLS handshake. The lower layer, TLS record, uses symmetric cryptography to provide data privacy and integrity. On the other hand, asymmetric cryptography is used by TLS handshake protocol for user authentication and key exchange.

c. Password Authentication Protocol:

Password Authentication Protocol is the simplest authentication method, which is completed in two messages exchange [3]. Plaintext passwords or hashed passwords are send "in the clear" over a communication channel. Remote server compares with the stored password, and replies the result. Clearly, PAP by itself cannot meet the requirement of EAP methods. However, with a protection layer established prior to PAP execution, then it can be used safely and efficiently.

d. Challenge Handshake Authentication Protocol:

The security of CHAP depends on randomness and uniqueness of the challenge send by server, and also strength of the one-way hash function. Random challenge is introduced to prevent replay attack and computation of one-way hash function helps to protect against eavesdropping. The standard recommends choosing a password as long as the length of hash value for the chosen hashing algorithm, in order to avoid dictionary attack [5]. The protocol requires storing passwords in plaintext form at both ends. First, a server issues CHAP challenge packet containing packet identifier and random challenge byte. The client appends

identifier, password and challenge bytes received as the input to compute one-way hash function and reply the CHAP response packet. The server also computes the expected result and compares with the response value. If both are identical, the server replies with a CHAP success packet.

D. Password-based Public Key Cryptographic Technique:

The most crucial characteristic in the design of password-only authentication and key agreement protocol is the resistance against offline dictionary attack [5]. It is not easy to design a password authenticated key agreement securing a small piece of secret from all sorts of attacks. Many password authenticated key agreement protocol have been proposed, but some end up with either design flaw or burdened with heavy computation.

III. ALGORITHM USED

The proposed Base Station algorithm we will use for make the password based authentication between the two base nodes using the public key cryptographic technique. In this algorithm we follow the following steps that helps in makes the password based authentication between two nodes [4].

a. Algo. (Si, Di)
b. Si and Di are the Mobile Station
c. Si refers to source node.
d. Di refers to destination node.
e. Request send by Si to its Base Station B1
f. The Base Station will look the path for the Destination Node Base Station. It will perform the Routing between source and the destination base station
g. Data will be transferred from the Efficient Shortest path
h. On the Reciver side
i. Public key & private key
j. key pr = private key(Di)
k. key pu = public key(Di)
l. Send public to Si
m. Base Station will perform the Secure Key Exchange Between Nodes
n. The public key arrived at Source Node Si
o. Encode the packet of source Si by using public key (key pu).
p. Send the encoded packet to the destination side.
q. On the receiver side, decode the encrypted packet by help of the private key on destination side.
r. Exit

IV. EXPERIMENTATION

Our Proposed work is on Fair share algorithm. The Algorithm will be implemented using Network Simulator 2. , The mobile adhoc network comprising of 10 mobile nodes is constructed in the NS-2 simulator with the use of TCL script in the topological boundary area of 670 m x 670 m. The position of the mobile nodes is defined in terms of X and Y coordinates values and it is written in the movement scenario file. In these we utilize the bandwidth. The Scenario of AODV is shown in the given figure 1.

The below figure is the Wireless simulation of a clustered network. The complete network is divided in 5 clusters. Each cluster has 10 nodes. Each cluster has 1 base station and 9 mobile stations. Base stations are represented in blue colour. The above figure representing the communication between the inter clustered node. The sender and reciver both are present in different clusters. The figure shows the coverage area of different nodes.

The proposed system is a secure wireless network. In which the complete network performs the secure data communication over the network. The system provides 2-way handshaking for data transmission over the

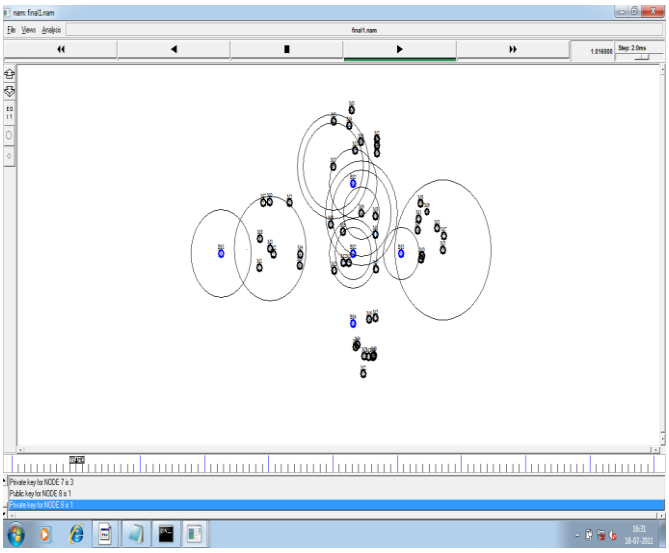

Figure 1: Screenshot of packets handover over base stations network. The secure handshaking is performed using the public key cryptography.

Each mobile station begins the simulation by selecting a random destination of base stations in the defined area and moves to that destination at a random speed and security by public key cryptography based algorithm.

The figure 7.2 represents that when the base station source node sends the data to the base station receiver node by sending Request using cryptography key method, it immediately transferring the data without any packet loss. The graph represents the simulation time (X-Axis) and Throughput of sending data (Y-Axis). As observed from the graph that the resultant throughput is high at the sending time when the node (base source node) to the base receiver node.

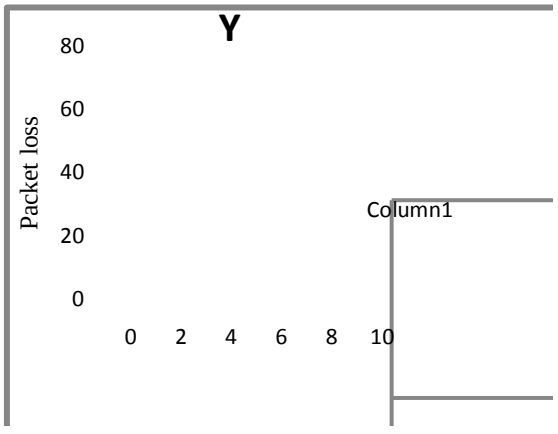

Figure 2: Packet loss during transmission

The Following figure shows the results of Throughput vs. Time of cluster based routing. It shows the packet transmission graph and throughput defined as the amount of data moved successfully from one place to another in a give time period and calculated as Bit/s. In this figure the X-axis represents the time and Y-axis represents the packet transmitted over the network.

The Throughput of AODV using cluster based routing is calculated as total bits received by destination node per second.

The delay occurs, when there is no communication between nodes and throughput is zero. The data is more stable when AODV and cluster based routing Protocol runs and packets are protected are protected with public key cryptography in cluster based mechanism.

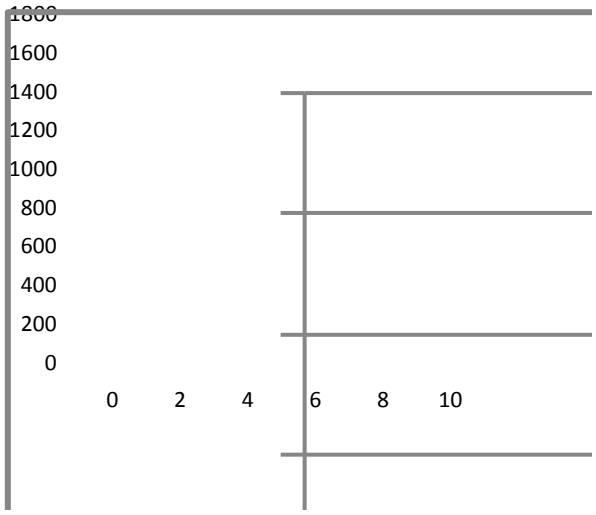

Figure 3: Throughput during sending of packets

The good put means when sender sends the packet to the receiver and how many packets lost and delay occurred during the transmission. This was calculated by the total data packet sent divided by the total packets transmitted in the network where the good put is higher in the case of AODV and cluster based mechanism due to re-transmission of the packets which has been lost and delayed due to interference, error and less security.

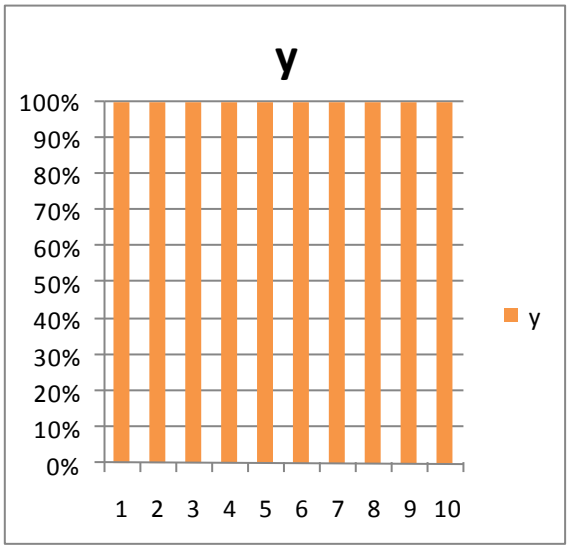

Figure: 4 Total packets transmitted in the network

Fig 4: Good put (packets) after cryptography algorithm

In our Simulation results, we provide the authentication in wireless network by using base station cryptography based algorithm between authenticated nodes [1]. BS-Client nodes that have been authenticated can authenticate each other using their public key & passwords received from master node. After that process BS-client nodes will exchange their public & private key, checking the validity, thus proving their identities. Here we use the base station Algorithm that employ authentication. Wireless network scenario we must have improve Performance, Security and throughput in wireless network using cryptography based algorithm between the Base stations.

V. CONCLUSIONS

In this Paper, we introduce the public key cryptographic algorithm. The congestion and packet loss level at every node is checked. We utilize the password based mechanism with the help of public key cryptographic algorithm. Before this the packets handover was not good due to collision and packet loss between nodes without base stations. We remove the packet loss between nodes, made the base stations to improve the secure transmission of packets and the authenticator authenticates each other which reduce the packet and increase the throughput.

VI. REFERENCES

[1]. Levente Buttyana, Laszlo Dora, Fabio Martinelli, Marinella Petrocchi, “Fast Certificate-based Authentication Scheme in Multi-operator maintained Wireless Mesh Networks” Hungary bIstituto di Informatica e Telematica (IIT), National Research Council (CNR), Pisa, Italy,January 27, 2010.

[2]. C. Rigney, A. Rubens, W. Simpson, and S. Willens, “Remote authentication dial in user service (RADIUS)”, Elbrys Networks, Inc., RFC 2865, August, 2009

[3]. Emmanuel Bresson, “A security solution for IEEE 802.11s ad hoc mode: password-authentication and group Diffie–Hellman key exchange”, Volume 2, Number 1, pages 4–13, Inderscience, 2007.

[4]. Yalin Chen1, Jue-Sam Chou, Chun-Hui Huang, “Improvements on two password-based authentication protocols”, Institute of information systems and applications, National Tsing Hua University, 2007

[5]. David P. Jablon Integrity Sciences, Inc. In “Strong Password-Only Authenticated Key Exchange”,September25, 1996.

[6]. Michel Abdalla and David Pointcheval “Interactive Diffe-Hellman Assumptions With Applications to Password-Based Authentication”, Springer-Verlag,Berlin, Germany. Vol- 3570, pages 341–356, Feb. 28 – Mar. 3, 2005.

[7]. Art Conklin, Glenn Dietrich, Diane Walz, “Password-Based Authentication: A System Perspective” The University of Texas at San Antonio, 2004.

[8]. Yair Amir, Claudiu Danilov, Michael Hilsdale, Raluca Mus_aloiu-Elefteri, Nilo Rivera, “Fast Handoff for Seamless Wireless Mesh Networks”,2008

[9]. Dr. A. K. Verma, , Secure routing in Wireless sensor networks", Computer Science and engineering department, Thapar university, Patiala, May 2009.

[10]. Dragorad Milovanovic, Zoran Bojkovic, "On performance of TCP and VoIP traffic in mobile WiMAX networks", Issue 5, Volume 9, (2010).

[11]. Maneesh Bakshi, "VoIP / Multimedia over WiMAX (802.16), 9, 2010.

[12]. IEEE Xplore, "Security Challenge and Defense in VoIP Infrastructures by D Butcher", 2007.

[13]. S.C. Wang, H.H. Liang and K.Q. Yan, "Capability Based Clustering Mechanism in WiMAX", Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol I IMECS, 2009.

[14]. Harshal A. Arolkar, "Ant Colony based Approach for Intrusion Detection on Cluster Heads in WSN", 1997.

[15]. Lin SHEN and Xiangquan SHI, " A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks", International Journal Of Intelligent Control And Systems, Vol. 13, No. 2, 146-151,2008.

[16]. Tim Daniel Hollerung," The Cluster-Based Routing Protocol", project group 'Mobile Ad-Hoc Networks Based on Wireless LAN', University of Paderborn, winter semester 2003/2004

[17]. Suraj Kumar Sharma, Sanjay Kumar Jena," SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks", 978-1-4244-9730-0/10/$26.00 © IEEE, 2010.