An innovative mutual authentication based protocol design for securing wireless communications and environments.

(*Towards creating impregnable wireless network environments.*)

Ankit Panch
Department of CSE & Information Technology
Government Engineering College
Bharatpur, Rajasthan, India.
(email:ankitpanch@gmail.com)

***Abstract*—For organizations and individuals, wireless networks have became very common, almost all the laptops and mobile phones are wireless enabled. The portability and connectivity provided by wireless to the users has made the technology beneficial everywhere. With the benefits provided by wireless the security concerns and issues with wireless are also present, and are many. Wireless networks are relatively found easier to break into by hackers, and the wireless networks are also cracked to gain entry into the underlying wired networks. As a result, it becomes essential for enterprises to define effective wireless security policies that guard against unauthorized access to their sensitive resources. With the increased use of wireless technology, the risk to users has increased many folds too. There were lesser number of dangers when wireless technology was first introduced. With the great risks associated with the present wireless (authentication) protocols and encryption methods, which are easy to crack, allowing hackers to gain access and lure clients in disclosing their vital information and resource misuse, it becomes essential to define new sets of secure protocols and techniques. The institutions which have established Access Points are suffering severe losses in terms of security, as the wireless access points are easily vulnerable to many types of attacks, where the client's sensitive data and information is stolen. So, the options which remain with the institutions are either to patch the existing software or upgrade to costly hardware, but certain issues can be resolved with modifying the protocols of authentication. Researching on such an approach is the goal of this research.**

***Keywords*—Evil Twin, Wireless Authentication, Wireless Networks, Wireless Security**

I. INTRODUCTION

With the advancements in the technology, the wireless communication has become prevalent and popular in recent days. Application of wireless technology is easily visible almost everywhere, and with the ease of access, wireless has brought internet closer to people's reach, and has reduced the cost of establishing a wired network. Corporations and individuals are using wireless to provide portability with high speed communication access to data and networks. Nowadays, internet is within easy access to people through hotspots, and almost all the mobile phones and laptops are now wireless enabled. Wireless Access points; provide easy wireless connectivity to wireless users to underlying wired networks and services. To authenticate users and maintain security, certain mechanism and set of rules and standards were defined by IEEE, known as IEEE 802.1X. During recent years there has been a change in security framework in IEEE 802.11, and it has migrated from the flawed WEP (Wired Equivalent Privacy) to WPA (Wi-Fi Protected Access), to bring the wireless security to the next level, during mid 2004, a framework based on the 802.1X and the extensible authentication protocol (EAP) was introduced by the IEEE Working Group (WG); known as WPA2. Motorola AirDefense's Wireless Security Survey [1] monitored 7,940 access points in enterprise environment, discovered 32% were unencrypted and 25% of APs were still using Wired Equivalent Privacy (WEP), the weakest protocol for wireless data encryption, which can be cracked in minutes, the survey also found that 12% of all APs monitored were using WiFi Protected Access (WPA) while another 27% were using WPA-PSK (pre shared key), which is only as strong as the shared password used to protect them. In total, only 7% were using WPA2, which is the strongest WiFi security protocol available today.The formatter will need to create these components, incorporating the applicable criteria that follow.

A. A. Rogue Devices

As agreed by experts that with the proliferation of wireless LANs, the probability of infiltration by unauthorized wireless devices in the institution’s network, rises up by many folds. The unauthorized devices that connect with the enterprise network or a WLAN device like Access Point is known as Rogue wireless device. Such devices pose huge risks to the enterprise network security. Such rogue devices that can pose threat to the wireless and wired network, bypassing firewalls and other protections.

Rogue wireless devices can be classified under two types:

1. *Rogue Access Points:* These are those wireless rogue devices which work are configured to work as or are actual Access Points, transmitting a default SSID or an SSID similar

to enterprise's access point, and a large number of clients get automatically connected to this AP, which can then launch many attacks on the client or attempt to steal vital information by displaying a login page to the client over the misassociated wireless connection.

2. *Rogue Clients:* They are those computers or mobile phones equipped with WLAN adapters which are located within the range of an institution's wireless range and in turn attempt to get connected to the enterprise access point in order to either utilize services offered by it, or for getting access to the network. These devices are unauthorized to connect to the institution's wireless network.[2]

So, there is a need for some type of stronger authentication which allows the client to verify true identity of an access point and also to allow access point to identify client. So for that purpose, in this paper, a new protocol design is proposed. In this research securely authenticating the client and the Access Point, such that client does not get connected to a non genuine looking but fake institution's access point, and the genuine Access Point does not allows a fake client to get connected to it. It is essential to make authentication and mutual identification so efficient that the third malicious party cannot even get a weak point to enter the communication channel, and execute it malicious intentions.

II. MUTUAL AUTHENTICATION BASED PROTOCOL DESIGN

A. Background

In multiple connection environments, considering a situation where a Legitimate AP connected to an institution's gateway is providing access to a client A. The client A regularly gets connected to the AP, and utilizes its services. During a new session, a Fake AP, or evil twin, starts broadcasting the same SSID as of the real AP, and if the signal strength is high the Client AP gets connected to it & due to the preferred network settings or a deliberate connection. After the connection the client wishes to resume its services, unaware of the fact that the AP is illegitimate (rogue).

So, at such a point, there is a need for an authentication protocol where the client can identify if the AP it is getting connected to be genuine or not, so here a mutual authentication based protocol design which can be integrated as a protocol, is presented, as explained.

This authentication approach works mid way in the process of discovery and connection to a preferred AP which is illegitimate (rogue) in this case. Still the connection is established. Previously, we should not forget that there is a mutual key exchange between the server and the client, before the session is established. The approach elongates the authentication process with a very slight variation. The explanation is as below.

1. The server responds with the key exchange after mutual handshake, and the connection is established.

2. The client connecting to the authentication server needs to verify the legitimacy of the server, through probing.

3. If the server authenticates itself, then the connection can be maintained else it is dropped.

Here if the key or certificate exchange is compromised, or the AP provided another certificate to trust by the client which gets accepted. Then the chances of the illegitimate (Rogue) AP to establish a true look alike connection with the client are increased to many folds. [3].

B. Introduction

The approach here begins from the first connection established by the requesting client, as trust on first use, here a mechanism to provide the authenticity of the AP by probing about previous connections that were successfully established and managed, can lead to a decision making alternative for the client to either trust and connect or not to trust and drop the connection. This approach do not need any hardware modification or up gradation but requires for the generation of a system file or database named as, wireless connection session database (wC_SessionDB), which can provide the historical evidences of the authenticity of the AP. The purpose here is to maintain a record history of the previous successful connections and transactions between the client and the AP, and to maintain a system database for authentication purposes. As, only the genuine AP will know about the previous connections, probing about the previous connection history can lead to a true discovery of an AP's truthfulness.

C. Prerequisitec

Considering, the AP and the Client were already connected 1 time and a wCSession_DB field entry was created by the backend authentication server of the AP to the client to relish the connection services, can contain the following field types.

- Session Number -- sessionNum
- PreviousIP of client -- clientMacId
- Session Key -- sessionKey
- Session Date -- sessionDate
- Establishment Time -- sessionTime
- Others (if Any) (Please refer Figure 1).

This wireless session database can be configured and stored in the configured system database file on both client and server sides. Here, the inclusion of MacID, in to the hash creation can be included along with the session IP obtained by the client. The creation of Hash Table as shown in figure 1 can bring up the desirable results, and will ease in propagation of parameters. This happens when all the parameters of wCSession_DB are added through a hash conversion function and then are added together and stored as a hash digest.

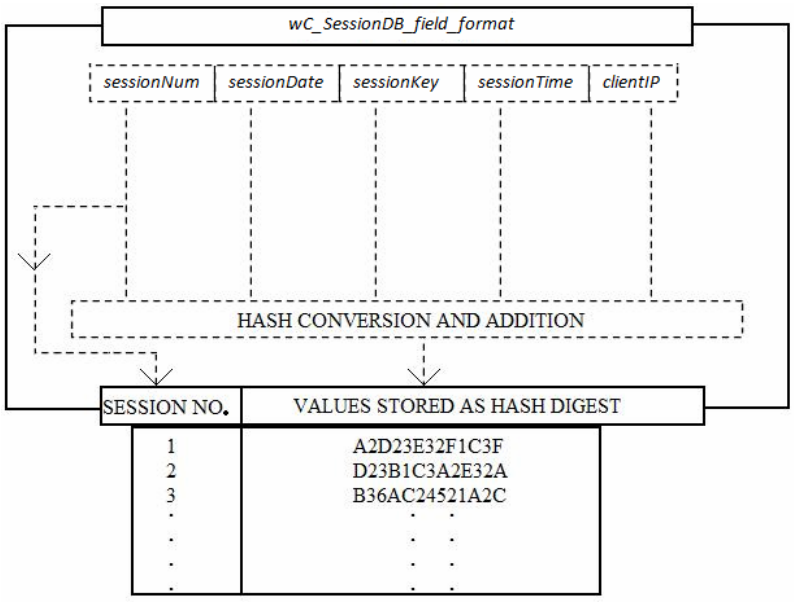


FIGURE 1. HASH DIGEST GENERATION

D. *Functioning*

A system database file is maintained and updated as required on the server and client side, updates only occur after the client and the server both agree after authentication themselves for the ongoing session. The requesting client can probe the server about connection history, through hash digest exchange. As it is only the genuine AP / server, which has the same updated client specific Wireless Session Database, as the same whose carbon copy lies on the client side, can easily make the client distinguish between the Real and the illegitimate (rogue) AP. The illegitimate (rogue) server cannot answer the probing questions by the client so the client do not trusts the AP and drops the connection, with a warning message to the end user.

E. *Working*

This approach works in a way where no secrets are shared, and the client can probe the server's authenticity by sending query packets and receiving the server's reply, the query by the client and the reply of the server are using wireless connection session database in background, as the query and reply are based on the field entries of it.

1. During the procedure of handshake, the client asks the server randomly for any hash digest of any random entry or a group of entries, as explained in the Protocol Algorithm.
2. Trying this procedure for say, n times, if the server is not able to provide the satisfying probing answers, the connection is terminated, with a warning message to the end user (route 2 on Figure 2).
3. If in case the server is able to identify by answering the probing questions rightly, the connection can be established, and a newly generated session id is transmitted to the client, where then both of the sides update their tables. On mutually acceptable grounds, (route 1 on Figure 2).

F. *Protocol Design*

This approach can be easily integrated in an application layer protocol or EAP framework, and can be installed on the client and on the authentication server side of the AP. The approach exhibits its best performance when working as a protocol, for authenticating the client and the server, mutually.

This approach is a dual authentication method, which can be used in an institutional environment, where number of users is limited, and the client machines can be configured to obey the protocol laws. The protocol can be well understood by the algorithm it adapts for its functioning.

The client and Server side of Algorithm, represent the Client as the one which sends probing packets, to authenticate the other, and the server representing the one who replies over the probing requests, but this should be considered that, one way authentication, when the real client authenticates the other should be sufficient to authenticate the both, and If still there is a requirement for the AP to validate the client further, the server will run the client side of algorithm, and begin to send the appropriate packet. (Please refer Figure 3)

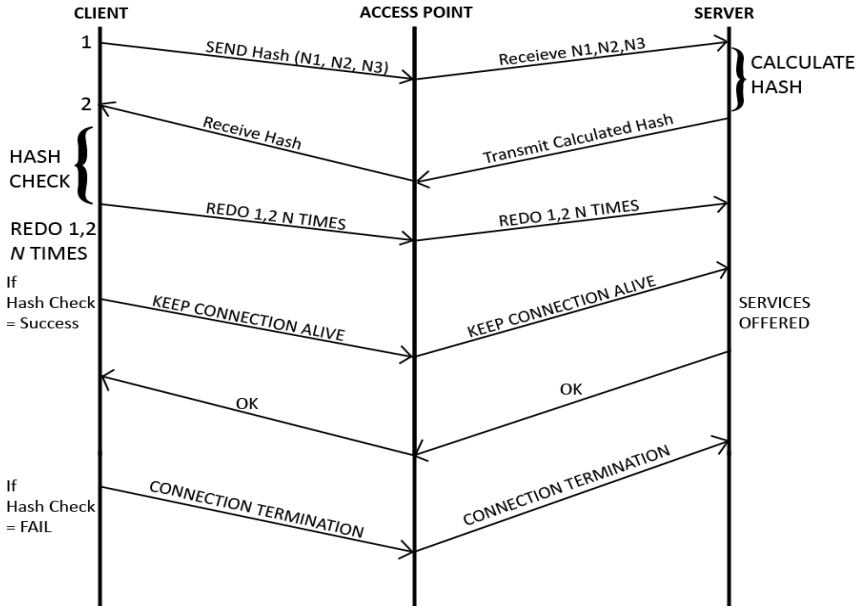


FIGURE 3. PROTOCOL WORKING

The algorithms for the client and server role are presented as below.

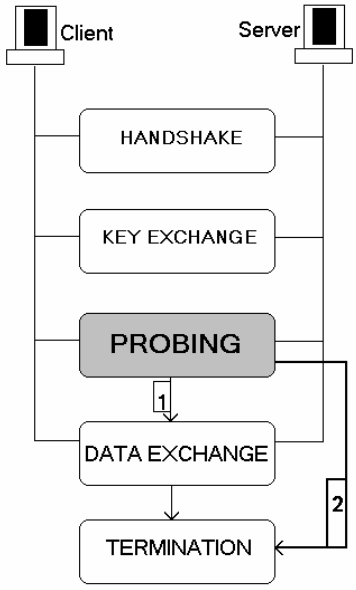


FIGURE 2. FUNCTIONING FLOWCHART

G. Protocol Client (Sender) Side Algorithm

Declaration: Trust = NoTrust =0, n= total number of entries in the database, N1, N2,N3=0.

Establish : Connection, Cryptographic key

Open: Wireless Connection Session Database

Generate: 1. Random number N1 < n

2. Random number N2 > n.

3. Random Number N3 > or < n.

Send: (N1, N2, N3) as hash digest to Server.

Sleep: 1. Till reply is received.

2. Else on timeout Start Generate again.

On Reply: Hash Check Module Begins at Client

Check: Reply (If (reply == True), Trust ++), If (reply == False), NoTrust++)

Redo: Generate, Send, Sleep, On Reply, Check for N times in total, on completion go to Result.

Result: If (Trust/N X 100) > 80, Allow Services from Server, Else, Terminate Connection.

H. Protocol Server (Receiver) Side Algorithm

Declaration: T = Total Number of Database Entries for Client.

Establish : Connection, Cryptographic key

Open: Wireless Connection Database

Receieve: N1,N2,N3 from client, & compare which of N1,N2,N3 falls under T

Calculate: 1. If only one of N1,N2,N3 is such that its <=T

a. Get Corresponding Hash Digest

b. Substract it from total hash

c. transmit.

2. If two of N1, N2, N3 are such that its <=T

a.Get Corresponding Hash Digests, add them.

b. Substract it from total hash

c. transmit.

3. If All of N1, N2, N3 are such that they are <= T

a. Get Corresponding Hash Digests, add them.

b. Substract it from total hash

c.Transmit.

4. If none of N1, N2, N3 are such that they are <= T

a. Generate a random hash, transmit.

Sleep: Till reply is receieved.

On Reply: Start receieve

Check: If client authentication is required, if yes, follow Protocol Client Side Algorithm.

Result: Wait for client's response for accessing services, or Terminating connection.

On the client side of algorithm, client is the one which is trying to check the authenticity of the other. In the first, the algorithm initiates 6 variables, Trust, NoTrust, N1, N2, N3 and n. Where the N1, N2, N3, Trust and NoTrust are initially declared as 0, n represents the total number of entries in the Wireless Connection Session Database. The client then starts to handshake with the server, agrees upon the Encryption mechanism, and then generates a random number R such that first it is lesser than n, and then it is greater than n, and in the third case it may be greater or lesser than n. The Range for R > n can be, R:R|R < 3n.

After generating the three values, the client encapsulates them in a query packet as a hash digest, such that it is possible for the server receiving it to again generate the three numbers. The cause behind generation of these numbers is explained in Section III.a. The client then transmits these values to the server, and sleeps till the reply is received or after timeout it regenerates the packet and sends to the server. Upon receiving the server reply packet, client checks the reply to validate the server, the Hash Check Module which do this process is explained in Section III.b. and III.c.

If the hash check is successful, the client increments the value of Trust and on failed hash check it increments the value of NoTrust, and regenerates the three numbers, and repeats the transmission, waits for the reply, receives the reply, and performs the hash check, N number of times.

On completion of N times the client, generates the trust percentage by the following formula, taking in consideration the values of Trust and NoTrust.

$$Trust\ Percentage = Trust\ /(Trust+NoTrust)\ X\ 100$$

The client chooses to stay connected to the AP, if Trust Percentage is greater than 80, else it chooses to disconnect from it.

The server upon receiving the encapsulated hash digest, disintegrates it and obtains the number N1, N2, and N3, and checks these numbers against the total number of entries in the client specific database table. If it finds one of the number lying valid under the total number of Wireless Connection Session Database entries, procures the corresponding hash, subtracts it from the total hash and transmits. If there are two or more values lying under the total number of database entries, then it adds the corresponding hashes, subtracts it from the total hash and transmits. If it finds all the numbers are greater than the total number of database entries, then it generates a random hash and transmits to the client.

The client then choose either to verify the client, upon a successful check by the client, or choose to let it utilize the services, in any of the cases, still the algorithm is secure, as the client's valuable information, is not lost to a fake AP.

This algorithm chooses to disclose no secrets, as there can be a possibility of a man in the middle in such a scenario. So, the algorithm gives no scope for the man in the middle to know anything about the ongoing conversation between the client and server. The transmission of random numbers, and the transmission of the resultant hash after the hash calculation be the server end, also will not give any hints to the man in the middle. The database is queried on both the sides, but no information is transmitted out from it, so it provides secure procedure. This procedure is explained as a diagram in figure 3.

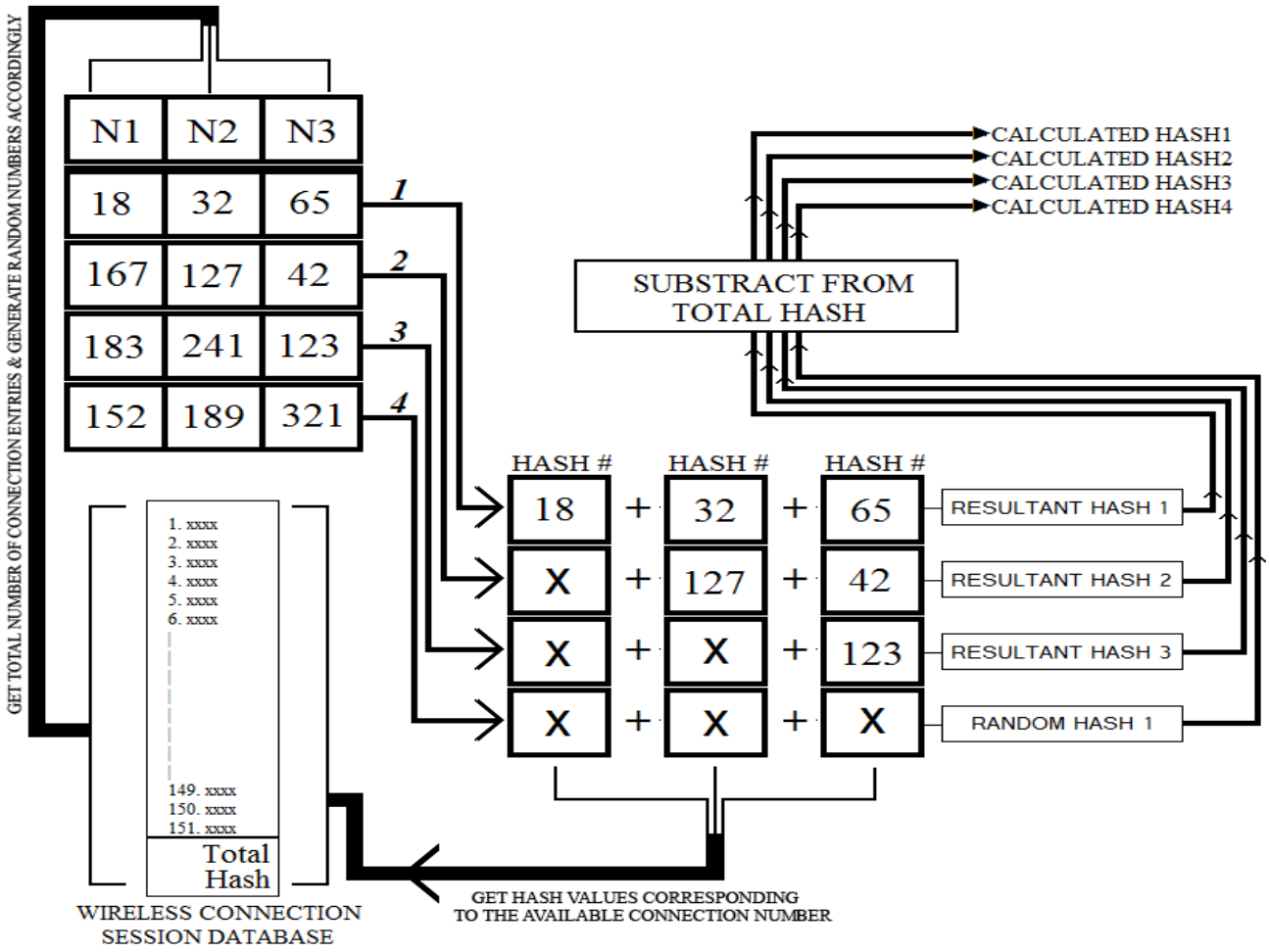


FIGURE 4. HASH CALCULATION

III. MUTUAL AUTHENTICATION BASED PROTOCOL MODULES & PROCEDURES

A. *Client Side Random Number Generation*

The client generates three random numbers depending on total number of connection entries, and sends them to the server. The logic behind the generation of these random numbers is as explained below.

1. As there is a possibility of many entries in the database if the client is frequently connecting to the AP. It is preferable to select values for query packet randomly.
2. The client should not send all three values, lying under the maximum number of connection entries because, for the Man-in-the-middle it may benefit, with some information about the transmission, at least about the total number of database entries.
3. Even if the Man-in-the-middle decodes the packet, it will be confusing for it.
4. Only the genuine server on getting multiple values, knows which value is valid and falls under the database entry, and procures it and subtracts it from total hash and sends, for two values it procures both of them adds them and subtracts from total hash and sends. So, in this way no secret is transmitted.

B. *Hash Calculation*

The sender (client in this case) generates N1, N2, N3, where they represent the connection number, with a unique hash value belonging to it, and sends it to the server, and which generates the calculated hash corresponding to its query, along with that the client also calculates the hash on its own as well, depending on the numbers, N1, N2, N3, so it can compare the hash calculated by its own, and the hash it receives as reply from the server, the procedure is highlighted in figure 4.

Four cases are considered while generating the calculated hash, (here Total number of Wireless Connection Database Entries is being denoted by t.) which are:

1. If N1, N2, N3 < t
   In this case, the client and servers both procure the corresponding hash values from the connection database, add them, and subtract it from the total hash.
2. If N1 > t, N2, N3 < t
   In this case, the client and server both procure the corresponding hash values of only N2, N3 from the database, add them, and subtract from the total hash, N3 is ignored.
3. If N1, N2 > t, N3 < t
   In this case, the client and server both procure the corresponding hash value of only N3 from the connection database, and subtract it from total hash. N1, N2 are ignored.
4. If N1, N2, N3 > t
   In this case, the client knows that N1, N2, N3 do not represent any corresponding value, and awaits a random reply from the server, and understands that the server has recognized it, and upon getting a random hash it recognizes, another way along with that upon getting such a packet, the server chooses not to reply, and client expects a no reply till time out, for the previous case, the server generates a random hash, can either transmit it directly or do so after subtracting it from the total hash.

C. Hash Compare

The client (sender) calculates the hash corresponding to the numbers N1, N2, N3, it sends N1, N2, N3 to the server (receiver) as a hash digest, and upon receiving the reply compares the calculated hash received with its own generated calculated hash. If the hash matches, then it increments the value of Trust, else NoTrust is incremented. When the client sends N1, N2, N3 > t, it proceeds as explained in Section III.a, and increments Trust, upon receiving, a random reply, or a noreply till time out, as settled during protocol implementation.

D. wC_SessionDB Database Updating

The database wC_SessionDB needs to be updated with new values stores if the client authenticates the server / AP as genuine, this happens as explained.

1. Upon successfully authenticating the AP / Server, the client asks for an encrypted session key from the server, along with a time stamp.
2. The client and server then mutually pass the remaining values in the hash creating function as shown in figure 1, and then update their databases, using the same algorithms. Here, the inclusion of MacID, in to the hash creation can be included along with the session IP obtained by the client.
3. As the client and server both are configured to use the same value processing, hash creating algorithms, their updates must be same.
4. On the completion of such a procedure, the server or client may choose to transmit, either first 2 characters or last 2 characters of their updated hashes, for confirming if their updates were same.

E. E. Malicious encounters & Triggers:

The clients when encounters a illegitimate (rogue) AP, transmitting the same SSID, it cannot differentiate between it and the genuine one, until it starts its authentication, the authentication will begin, and the fake AP if not able to answer any of the query packets of the client will loose its trust, and the client will choose to disconnect from it, and vice versa in case of AP authenticating a client. Along with it, certain triggers can start the authentication process, post authentication, all over again, such as

1. A sudden increase in the radio frequency.
2. A malicious packet obtained during the ongoing service utilization.
3. Any suspicious activity reported by firewall.
4. Any new certificate binding issue.
5. A lost transaction.
6. Any reconnect attempt.
7. Malware force download issues.
8. Any request to access any of the client's network services like file sharing etc.
9. Any ongoing suspicious activity in client's machine.
10. Any other suspicious attempts.
11. Any decrease in the SINR values. (Section IV.b.)

IV. MUTUAL AUTHENTICATION BASED PROTOCOL PROTOCOL SIMULATION

This section deals with the simulations of the proposed approach / protocol. In the simulation, the protocol algorithm is simulated, for the purpose of performance check, and its efficiency. In the first simulation procedure, the protocol algorithm is simulated over the number of clients to the time taken by algorithm to authenticate, this simulation can be beneficial for understanding the performance of algorithm in simultaneous multiple client authentications. In the second procedure, the SINR values at 40 degree climatic conditions were calculated with number of nodes being increased, as it is essential to understand the SINR values in comparison with the number of nodes to establish an authentication trigger to launch the authentication procedure.

A. Simulation Mutual Authentication Based Protocol vs RADIUS

In the first simulation setup, the protocol algorithm was simulated, and the graph plotted over the time consumed by the algorithm, to the number of clients, the time in seconds is

multiplied by 10000, for ease of plotting. Along with that the Radius Authentication Protocol was also simulated over the same number of clients and the results were compared as shown in figure 5.

As visible in the simulation graph of figure 5, the Radius authentication protocol initially works slower than the ESWA Protocol Algorithm, while the proposed protocol algorithm takes up a near average linear path. The Radius protocol gains up speed after reaching a total of 160 numbers of clients, while the proposed protocol still remains linear, so after 160 numbers of clients, the proposed protocol becomes minutely slower than the Radius protocol. Thus the simulation provides us with the idea that the proposed protocol is quite similar to the Radius protocol's time based efficiency but offers much reinforced authentication.

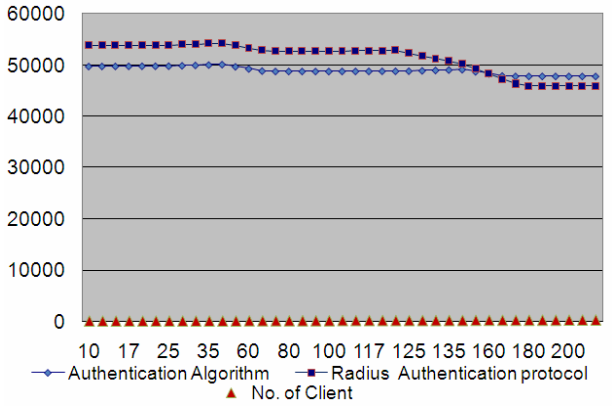
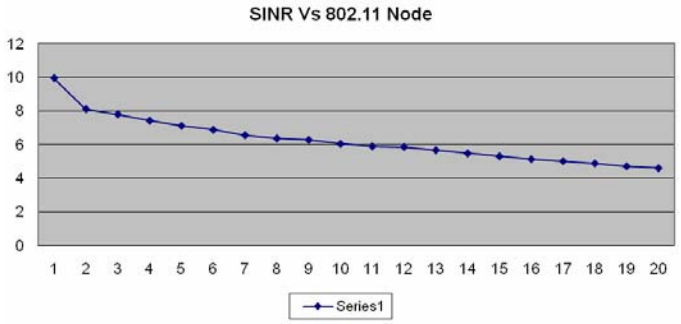


FIGURE 5. SIMULATION OF PROPOSED AUTHENTICATION ALGORITHM VS RADIUS PROTOCOL

B. Simulation SINR vs 802.11 Node

To understand the effect of the increase in number of nodes on the SINR, a simulation was conducted, in this simulation the behavior of SINR or the increasing number of nodes, at 40 degree atmospheric temperature was plotted. As it is visible from figure 6 with the increase in the number of nodes, the value of SINR drops drastically, the number of nodes here may represent any device legitimate or illegitimate broadcasting its radio transmission, once detected a decrease in the value of SINR, a trigger can be established to initiate the proposed authentication protocol, as with the constant number of users already connected to the Access Point at a constant value of SINR are already verified, a decrease in the SINR value can either trigger ESWA Protocol to reauthenticate all the users connected to it, or with the help of monitoring RF transmission, can ease in locating an illegitimate(rogue) device and challenge it for authentication, if failed the device, is not able to access any type of services offered by the AP.



V. DISCUSSION & CONCLUSION

An institutional network security becomes weak with vulnerabilities in its wireless interface, due to which institutional losses in terms of vital information, data, network efficiency and cost get higher. Costly hardware and software upgrades become essential to patch up the network to be efficient against such security concerns. Illegitimate (rogue) devices trying to bring down the network security are leaving no stone left unturned to exploit the loopholes present, and due to which the security of the legitimate users getting access to the enterprises' resources, is at stake. With understanding the present methods of authentication and identity verification, and trying to define a new method of secure authentication, which is portable and easily deployable in institutional scenarios, is the need of the time. It is essential to further research on the process of authentication because discrepancy and loopholes present at this level of network access can lead to disastrous outcomes.

The research carried out for designing the Mutual Authentication Based Protocol, meets all of these requirements and pre-requisites, and can guarantee a secure authentication platform, and keep the infiltrators at bay. The Mutual Authentication Based Protocol is an innovative approach which directly aims at nullifying the present loophole, and in co-operating with the present standards and protocols, can lead to a future of extremely secure wireless networks. The mechanisms of ideal information security should exist at all layers of the OSI model, but the application layer is extremely important to be worked upon, as the generation of the information and the retrieval of the same, happens at the application layer. Mutual Authentication Based Protocol is best suited for the institutional adoption as their primary secure authentication protocol, mainly due to the reason that it is very economical, secure, needs no hardware upgrades and can be easily integrated as a separate application layer protocol, or can be accommodated in Extensible Authentication Protocol (EAP) or within the Radius architecture or as a separate authentication entity. In any of the cases the Mutual Authentication Based Algorithmic approach works efficiently by recognizing devices on the basis of their previous communications, this happens as human's recall the familiar faces of people, after seeing them, and then reconfirming their identity, by counter questioning them, but the added advantage of the ESWA approach is that, during its processing no secrets are shared, and it is ensured

that no information is disclosed which can benefit the man-in-the-middle (MITM).

The proposed protocol can be further researched to be working in integration with Firewalls, IDS, Operating Systems, Payment Gateways, wireless Hotspots etc, and with integration and with the known methods of RF monitoring, its efficiency shall increase by many folds, through securing its own perimeter of the trusted clients, and selectively disallowing the illegitimate (rogue) devices to affect any of its services. The security issues with the wireless networks can always be minimized with the proper use and combinations of the available resources, Mutual Authentication Based Protocol when is deployed to work can fairly demonstrate good results, due to is adaptability, and is easily put on task by installing the Mutual Authentication Based Protocol on the client and the server machines.

The deployment of Mutual Authentication Based Protocol, by institutions can increase the trust of the benefitting clients and will assist the intuitional minimization of the network security & maintenance costs, and the legitimate users can securely access the services which are available for only them.

Proposed authentication proposed will ease in the following way.

1. Genuine Client Connecting to illegitimate (rogue) AP: If the Client and Real AP are preconfigured to authenticate each other through proposed protocol design, there is no question of a client getting connected with the Rogue AP or evil twin, the client starts the authentication as usual here.
2. Illegitimate (rogue) Client Connecting to Genuine AP: The access point first check the MAC address of the client, and if it is not trusted, will send an authentication challenge (as proposed) to begin authentication, the rogue client will not be able to reply accordingly and the AP will not allow the services.

REFERENCES

[1] Motorola Global Survey, http://www.airdefense.net/newsandpress/01_28_09.php
[2] Airtight Networks, The New Threat to Enterprise Security – Wi-Fi, 2005
[3] A. Panch, S.K. Singh, A novel approach for evil twin mitigation in enterprise wireless environment, IJSIA 2011

AUTHORS PROFILE

Ankit Panch received his B.Engg. degree in Computer Engineering from Birla Vishwakarma Mahavidyalaya, under Sardar Patel University, Gujarat, India, year 2007 and M.Tech in Software Engineering at the School of Engineering, Gyan Vihar University, Jaipur, India in year 2011. His current research interests include information security, intrusion detection & mitigation and wireless networks. He is presently working as Assistant Professor in Department of CSE & Information Technology, Government Engineering College, Bharatpur, Rajasthan, India.