

**INCREASING THE SECURITY OF WIRELESS NETWORK AGAINST MAC ADDRESS
SPOOFED-ATTACKS**

A Dissertation submitted

By AARTI JOSHI

To

Department of Computer Science and Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Asst. Prof. Md. Ataulah

May-2015

ABSTRACT

As security is being a big issue these days therefore main focus is on increasing the security by any mean. Media access control (MAC) spoofing is common in these days. As it is a permanent address assigned to interface of each device network card connected to the internet. They function at layer 2 (i.e. data link layer). MAC address can easily be spoofed in WLAN network i.e. being a problem because the intruder can access the resources or do some criminal activity without the knowledge of other and all blame for it will go to the original one. Even if we detect the presence of intruder it is difficult to tell which one is the original one as both node claim itself as genuine node so it's difficult for server to find which one is the original one. So our main purpose is to identify the genuine client from the outsiders to avoid mac spoofing and to provide a secure environment for communication.

CERTIFICATE

This is to certify that AARTI JOSHI has completed M.Tech dissertation titled **Increasing the Security of Wireless Network against MAC Address Spoofed-Attacks** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions for the award of M. Tech Computer Science and Engineering.

Date: 4 May, 2015

Signature of advisor

Name: Md. Atullah

UID: 16915

ACKNOWLEDGEMENT

I am highly grateful to lovely professional university and also Md. Ataulah Sir, for providing this opportunity to carry out the dissertation work.

The constant guidance and encouragement received from Md. Ataulah sir has been of great help in carrying out the project work and it's acknowledged with the reverential thanks He actually laid the ground for conceptual understanding of technologies used in project.

Without the wise counsel the able guidance, it would have been impossible to complete the dissertation report in this manner.

We express gratitude to other faculty member of CSE/IT department of Lovely Professional University for their intellectual support throughout the course of this work.

DECLARATION

I hereby declare that the dissertation entitled, “**Increasing the Security of Wireless Network against MAC Address Spoofed-Attacks**” submitted for the M. Tech degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: 4 May, 2015

Aarti Joshi

Regn. No. 11008652

CONTENTS	PAGE NUMBER
1) Introduction	1
1.1) Wireless network	1
1.2) Wireless operating mode	2
1.3) Advantages and Disadvantages of Wireless Mode	3
1.4) Benefits of wireless network	4
1.5) Different types of wireless Systems	4
1.6) Mac address	8
1.7) Networking model	9
1.8) Different Wireless Encryption Protocol	10
1.9) Steps For Implementing Security In Wireless Network	10
1.10) Attacks on wireless network	12
1.11) Disadvantages of wireless network	13
1.12) Organization of thesis	14
2) Literature review	15
2.1) Lightweight detection of spoofing attacks in wireless network	15
2.2) An improved method of detecting spoofed attack in wireless LAN	15
2.3) Using constant traffic to specific ip destinations for detecting spoofed MAC addresses in Local area networks	16
2.4) Using constant traffic to specific ip destinations for detecting spoofed MAC addresses in Local area networks	16
2.5) A design of egress NAC using an authentication visa checking mechanism to protect against MAC against spoofing attacks	17
2.6) Media access control spoofing techniques and its countermeasures	18
2.7) IEEE 802.11 Anomaly-Based behavior analysis	18
2.8) Medium access control spoof detection and prevention algorithm for spoofing attacks in wlan	19
2.9) Wireless local area network (wlan) spoofing attack- A proposed detection method in victim silent case	20
2.10) Wireless Device positioning and finding intruder using rss	20
2.11) Tracking rogue device in wireless Network System	21
2.12) Detecting spoofing attacks in wireless network	21
2.13) Detection of SSH host spoofing in network control systems through network telemetry analysis	21
3) Present Work	22
3.1) Problem Formulation	22
3.2) Objectives of problem	23
3.3) Methodology	23
4) Result and discussions	28
5) Conclusions and Future scope	33

6) References	34
7) Appendix	36

LIST OF TABLES**PAGE NUMBER**

1) Table 2.5.1: Comparison between different Wireless network types

7

LIST OF FIGURES**PAGE NUMBER**

1) Fig 1.1: Infrastructure of wireless network	2
2) Fig 1.2: Ad-hoc mode	3
3) Fig 1.3: Wireless Local Area Networks	5
4) Fig 1.4: Wireless Personal Area Networks	5
5) Fig 1.5: Wireless Metropolitan Area Networks	6
6) Fig 1.6: Wireless Wide Area Networks	6
7) Fig 1.8: MAC Address	9
8) Fig 1.9: Identity Theft	13
9) Fig 1.10: Man in the Middle Attack	14
10) Fig 2.1: AV Mechanism	18
11) Fig 3.1: Proposed Methodology	27
12) Fig 3.2: Flow Chart	28
13) Fig 4.1: Home page	30
14) Fig 4.2: Reset Password	31
15) Fig 4.3: Register Page	31
16) Fig 4.4: Download Page	32
17) Fig 4.5: Window Application	33
18) Fig 4.6: Mac Capture	33
19) Fig 4.7: Login Page	33

CHAPTER 1

INTRODUCTION

1.1 Wireless network

Wireless network it is a network which is set up by using radio signal frequency to communicate between different computers and other network device. Sometimes it's also known as Wi-Fi network or WLAN. This network is becoming popular nowadays due to easy installation feature, less complexity and no cabling involved. We can connect to computers anywhere in our home or any place without using wires. Here is a simple example of how wireless network works, suppose we have two computers each equipped with wireless adapter and you have set upon a wireless router. Whenever the sender send out the data, it will be in binary form, and that binary data will be encoded to radio frequency and transmitted via wireless router to other devices. As the signal will reach the destination the data will again decoded to its original form by the destination computer.

A wireless network empowers individuals to convey and access applications and data without wires. This gives opportunity of development and the capacity to stretch out applications to distinctive parts of a building, city, or almost any place on the planet. Wireless networks permit individuals to associate with email or peruse the Web from an area that they lean toward. Numerous sorts of wireless communication frameworks exist, yet a recognizing characteristic of a wireless network is that communication happens between PC gadgets. These gadgets incorporate personal digital associates (PDAs), portable workstations, personal computers (PCs), servers, and printers. PC gadgets have processors, memory, and a method for interfacing with a specific kind of network. Customary PDAs don't fall inside the meaning of a PC gadget; nonetheless, fresher telephones and even sound headsets are starting to join processing power and network connectors. Inevitably, most gadgets will offer wireless network associations.

Likewise with networks in light of wire, or optical fiber, wireless networks pass on data between PC gadgets. The data can take the type of email messages, site pages, database records, gushing feature or voice. By and large, wireless networks exchange information, for example, email messages and documents, however progressions in the execution of wireless networks is empowering backing for feature and voice communications too.

1.2 Wireless operating mode

The IEEE 802.11 standards specify two operating modes for wireless network:

1.2.1 Infrastructure mode

Infrastructure mode in this mode we utilize access point to associate with wireless customers for transmission of information. PCs are associated with Access point through wireless system connectors, otherwise called wireless customers, to a current wired system with the assistance from wireless router or access point. It takes after customer server model foundation mode gives concentrated administration framework.

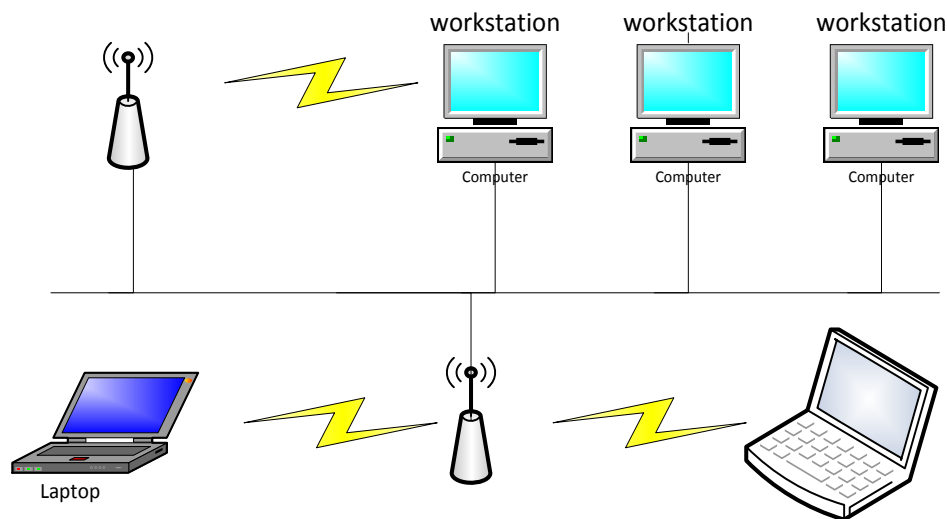


Fig 1.1: Infrastructure of wireless network

1.2.2 Ad hoc mode

Ad hoc mode it is utilized to straightforwardly associate with the wireless customers together, without the requirement for an entrance point or wireless router. In an impromptu system we can mean 9 wireless customers, which can send their information specifically to one another without utilizing any of these gadgets. It is a decentralized mode all hubs are self-arranging and nobody is better than other all offer equivalent status. An ad-hoc system has a tendency to highlight a little gathering of gadgets all in close nearness to one another. Execution endures as the quantity of gadgets develops, and a huge specially appointed system rapidly gets to be hard to oversee. Specially appointed systems can't extension to wired LANs or to the Internet without introducing an uncommon reason gateway.

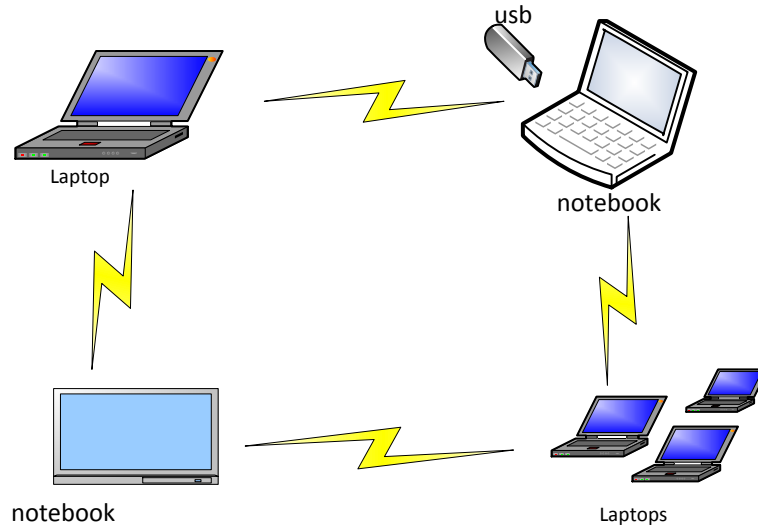


Fig 1.2: Ad-hoc mode

1.3 Advantages and disadvantages of wireless mode

Ad-hoc mode can be less demanding to set up in the event that you simply need to interface two gadgets to one another without obliging a centralized access point. For instance, how about we say's you have two tablets and you're sitting in an inn room without Wi-Fi. You can connect them straightforwardly with Ad-hoc mode to frame a provisional Wi-Fi system without requiring a switch. The new Wi-Fi Direct standard additionally expands on specially appointed mode, permitting gadgets to impart straightforwardly over Wi-Fi signals.

Infrastructure mode is ideal in case you're setting up a more changeless system. Wireless switches that capacity as access focuses for the most part have higher-power wireless radios and antennas so they can cover a more extensive range. In case you're utilizing a tablet to set up a wireless system, you'll be restricted by the force of the portable PC's wireless radio, which won't be as solid as a router's.

Ad-hoc mode likewise has different disadvantages. It requires more framework assets as the physical system format will change as gadgets move around, while an access point in foundation mode for the most part stays stationary. On the off chance that numerous gadgets are associated with the Ad-hoc system, there will be more wireless interference every PC needs to secure a direct association with one another PC instead of experiencing a solitary access point. On the off chance that a gadget is out of scope of another gadget it needs to interface with, it will go the information through different gadgets in transit. Going the information through a few PCs is only slower than going it through a solitary access point.

1.4 Benefits of wireless network

Remote LANs offer the accompanying efficiency, comfort, and expense preferences over wired systems:

1.4.1 Portability

Remote LAN frameworks can give LAN clients access to continuous data any place in their association. This portability bolsters profitability and administration opportunities unrealistic with wired systems. There are currently a great many colleges, inns and open spots with open remote association. These free you from must be at home or at work to get to the Web.

1.4.2 Establishment Rate and Effortlessness

Introducing a remote LAN framework can be quick and simple and can dispense with the need to draw link through dividers and roofs.

1.4.3 Diminished Expense of-Possession

While the introductory venture needed for remote LAN equipment can be higher than the expense of wired LAN equipment, general establishment costs and life-cycle expenses can be altogether lower. Long haul money saving advantages are most noteworthy in element situations obliging incessant moves and changes.

1.4.4 Versatility

Remote LAN frameworks can be arranged in a mixed bag of topologies to address the issues of particular applications and establishments. Setups are effectively changed and range from peer-to-peer systems suitable for a little number of clients to full framework systems of a great many clients that empower wandering over a wide region.

1.5 Different types of wireless Systems

A wireless system empowers individuals to impart and access applications and data without wires. This gives opportunity of development and the capacity to stretch out applications to diverse parts of a building, city, or about anyplace on the planet. Wireless systems permit individuals to collaborate with email or peruse the Web from an area that they lean toward.

Numerous sorts of wireless correspondence frameworks exist, yet a recognizing characteristic of a wireless system is that correspondence happens between PC gadgets. These gadgets incorporate individual computerized partners (PDAs), portable PCs, (PCs), servers, and printers. PC gadgets have processors, memory, and a method for interfacing with a specific sort of

system. Customary cells don't fall inside the meaning of a PC gadget; on the other hand, fresher telephones and even sound headsets are starting to fuse figuring power and system connectors. In the end, most hardware will offer wireless system associations.

Similarly as with systems in light of wire, or optical fiber, wireless systems pass on data between PC gadgets. The data can take the manifestation of email messages, site pages, and database records, spilling feature or voice. As a rule, wireless systems exchange information, for example, email messages and documents, yet headways in the execution of wireless systems is empowering backing for feature and voice correspondences too.

1.5.1 WLANS: Wireless Local Area Networks

WLANS permit clients in a local area, as a college or library, to shape a system or obtain entrance to the internet. A temporary system can be shaped by a little number of clients without the need of an entrance point; given that they needn't bother with access to system assets. Each part that join with a WLAN is viewed as a station and can be categorized as one of two classes: access points (APs) and customers. APs transmit and get radio frequency signals with gadgets ready to get transmitted signals; they typically work as switches. Customers may incorporate a mixture of gadgets, for example, desktop PCs, workstations, PCs, telephones and other PDAs and Smartphones. All stations ready to speak with one another are called fundamental administration sets (BSSs), of which there are two sorts: free and infrastructure. Autonomous BSSs (IBSS) exist when two customers convey without utilizing APs, yet can't unite with some other BSS. Such WLANs are known as a distributed or an ad-hoc WLANs. The second BSS is called an infrastructure BSS. It may speak with different stations yet just in different BSSs and it must utilize APs.

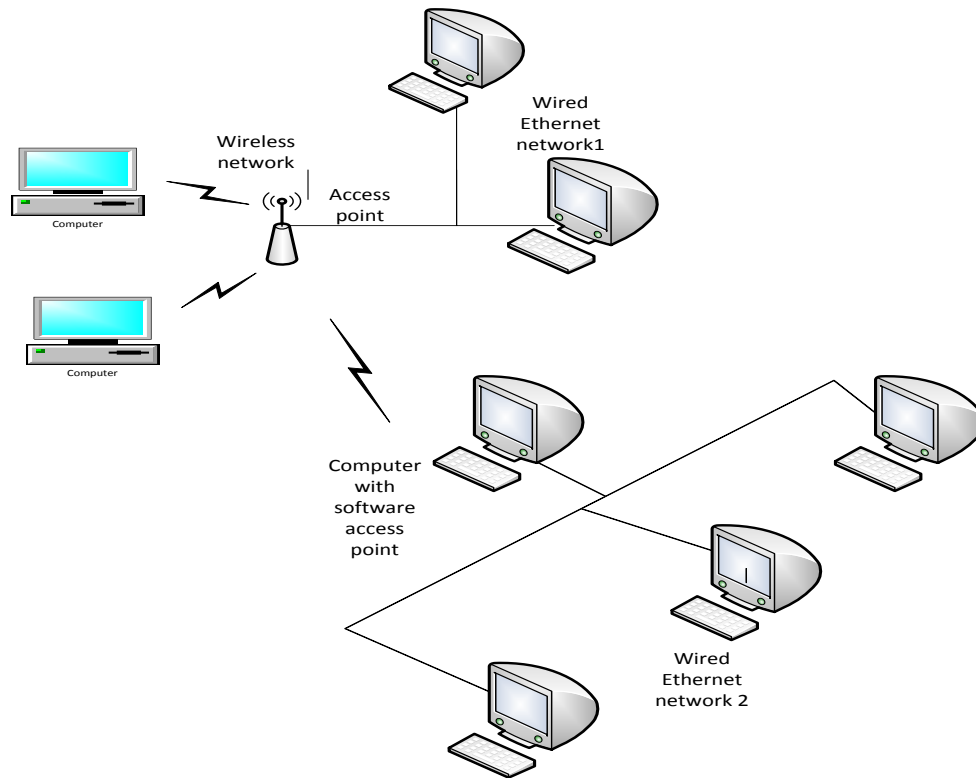


Fig 1.3: Wireless Local Area Networks

1.5.2 WPANS: Wireless Personal Area Networks

The two current advancements for wireless personal area networks are InfraRed (IR) and Bluetooth (IEEE 802.15). These will permit the integration of individual gadgets inside a zone of around 30 feet. Nonetheless, IR obliges a direct line of site and the reach is less.

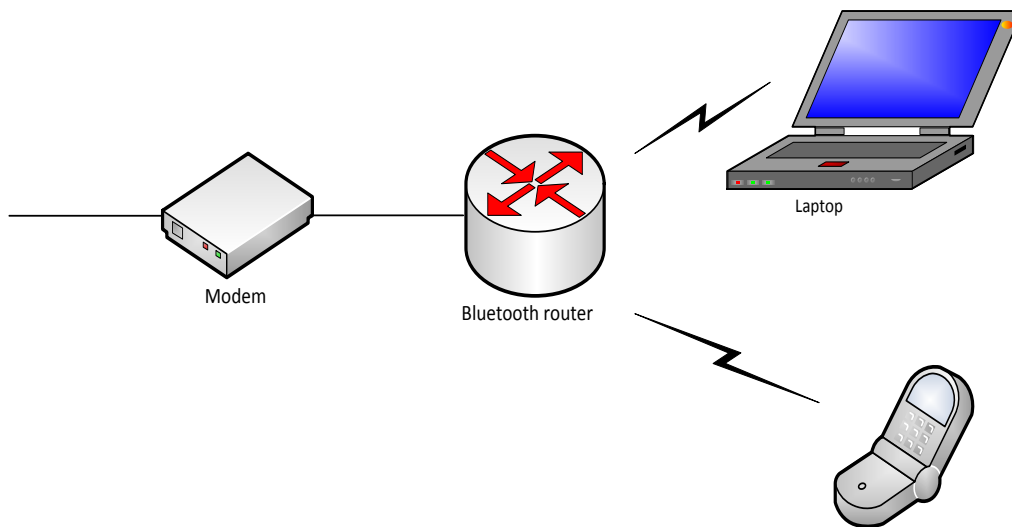


Fig 1.4: Wireless Personal Area Networks

1.5.3 WMANS: Wireless Metropolitan Area Networks

This innovation permits the association of various systems in a metropolitan territory, for example, diverse structures in a city, which can be an option or reinforcement to laying copper or fiber cabling.

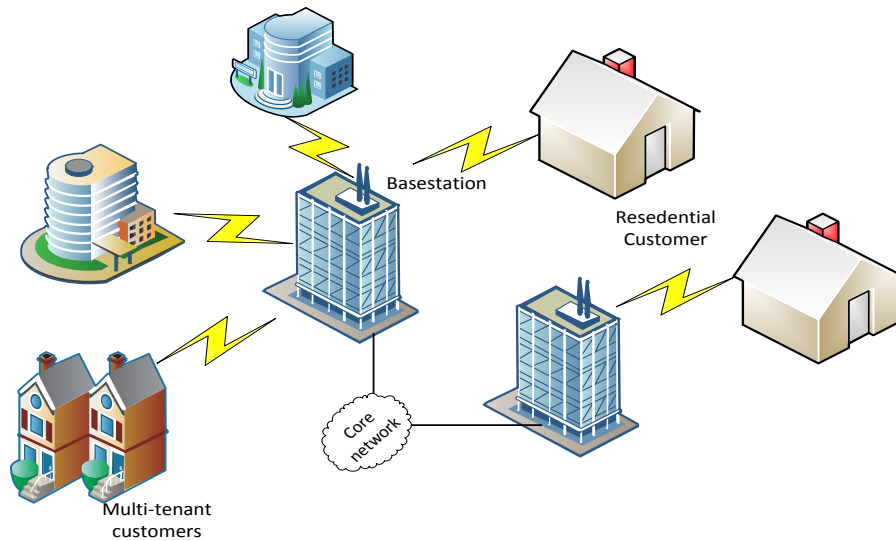


Fig 1.5: Wireless Metropolitan Area Networks

1.5.4 WWANS: Wireless Wide Area Networks

These sorts of systems can be kept up over huge territories, for example, urban communities or nations, by means of various satellite frameworks or reception apparatus locales cared for by an ISP. These sorts of frameworks are alluded to as 2G (2nd Generation) frameworks.

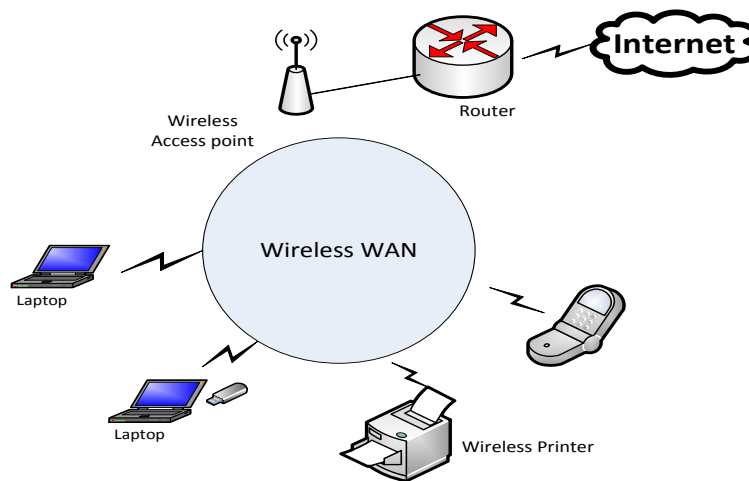


Fig 1.6: Wireless Wide Area Networks

Comparison between different wireless network types is shown in the following table:

TYPE	COVERAGE	PERFORMANCE	STANDARDS	APPLICATION
Wireless PAN	Inside span of an individual	Moderate	Within reach of a individual moderate Bluetooth, IEEE 802.15, and IrDa Link swap for peripherals	Link swap for peripherals
Wireless LAN	Inside a building or grounds	High	IEEE 802.11, Wi-Fi, and HiperLAN	Versatile expansion of wired systems
Wireless MAN	Inside a city	High	Exclusive, IEEE 802.16, and WIMAX	Settled remote in the middle of homes and organizations and the Web
Wireless WAN	Around the world	Low	CDPD and Cell 2G, 2.5G, and 3G	Versatile access to the Web from outside ranges

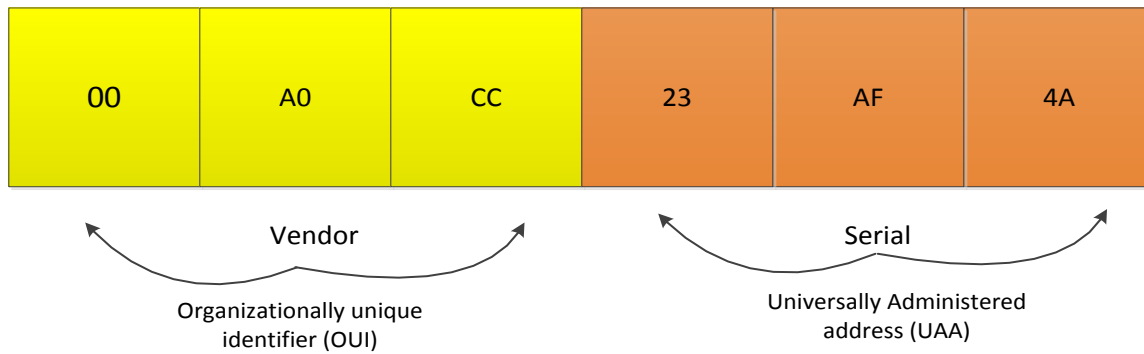
Table 1.1: Comparison between different Wireless network types

1.6 Mac Address

It is the physical location of a gadget through which it is perceived in the system. It is a special location gave to every gadget in the system. It is 48 bit address in Ipv4 and 64 bit in IPv6. It is communicated in a hexadecimal number.

E g 01-27-a1-e1-2f-38

These are the permanent addresses but can be changed easily.



Fig

1.8: MAC Address

Different type of mac address available

1.6.1 Universally administered address

It is the physical location of a device through which it is perceived in the system. It is a special location gave to every device in the system. It is 48 bit address in Ipv4 and 64 bit in IPv6. It is communicated in a hexadecimal number.

1.6.2 Locally administered address

It is the location that can change the mac location of system connector of gadget through which it associate with the system gadget and correspond with them. At whatever point LAA is changed then gadget take LAA as its mac address else it utilizes generally controlled address as its mac address.

1.7 Networking model

There are two different types of models that are used to interact between different types of devices

1.7.1 Client server model

It is a centralized model. In which one go about as server and other go about as client. All the client log into the system.

It comprise of

- Server: These are the framework which give administrations to different device.
- Router: These are the devices use to advise the course from source to destination.
- Clients: These are the gadgets which uses administrations from server.

1.7.2 Peer to peer

It is a decentralized model in which any gadget can go about as server or client all the while. Every hub having equivalent obligation and all are approach in status. All the client login in their local system.

1.8 Different wireless encryption protocol

Wireless system utilizes three distinct sorts of encryption conventions that are utilized to encode our information we send and get over the web so that no other can read it. So distinctive kind of encryption conventions are:

1.8.1 WEP (Wired Equivalent Privacy)

This was the first encryption convention use in wireless system as its name recommend it was create to give same or equivalent level of security as wired system yet its no more suggested in light of the fact that when we empower the WEP encryption convention we need to choose a key which is utilized to scramble the messages send and get over the system yet these days it is generally simple to break.

1.8.2 WPA (Wi-Fi Protected Access)

Due to the shortcomings of WEP encryption convention WPA was produced to conquer its impediment and to give more secure correspondence over the net. It was utilized with 802.1X standard and give distinctive keys to diverse clients normally alluded as WPA Enterprise. It utilizes the idea of PSK (Pre –shared key) basically known as WPA Personal and TKIP (Temporal Key Integrity Protocol). It verifies that the key utilized for encryption has not be adjusted so that no unapproved client can get to the system.

1.8.3 WPA2 (Wi-Fi Protected Access 2)

It is the improved form of WPA. The most critical improvement was the utilization of AES (Advanced Encryption Standard) system for encryption of message over the system and the utilization of CCMP (Counter Cipher Mode with Block Chaining Messages) in substitution of TKIP.

1.9 Steps for implementing security in wireless network

Security is the most important aspects of the wireless network and implementing security to the medium can be challenging task to resolve wireless security issues and to make the medium secure following measures can be adopted:

1.9.1 First change the default username and password of router

For better security of your wireless router one must change its default setting of router. At whatever point you begin designing your router than the default username and secret key must be changed on the grounds that those username and watchword can be known from the router's model number and these passwords are known openly on the grounds that seller use same username and passwords for every comparable router, so don't abandon it as default setting.

A few illustrations of default username and watchword of router are:

- Linksys router username: (blank) password: admin
- Netgear router username: admin password: password
- Dlink router username: admin password: (blank)

1.9.2 Change default SSID of router

One must change the default SSID of wireless router on the grounds that it would be simple for other's to know the default SSID settings despite the fact that you have debilitated your SSID. They just need the data about your wireless router model. Along these lines, dependably dole out SSID in such a way which is not simple to figure for others, and never utilize your name, or your own place of residence as SSID.

A few samples of default SSID of wireless router from diverse sellers:

- Linksys router SSID: Linksys
- Netgear router SSID: Netgear
- Dlink router SSID: default

1.9.3 Change the default ip address of the router

One must change the default ip location of the router as seller uses the comparative ip addresses for all the comparable gadgets and it can be effectively accessible from the merchant's site. Set up a security key for getting to the system for making your framework more secure system key must be doled out to control the entrance of client so that just approved client can get to it.

1.9.4 Applying firewall

A firewall is a product or equipment that manages the approaching and active system movement and shield your gadget from noxious programming or programmers.

1.9.5 Disable router SSID broadcast

Of course wireless router will dependably telecast its SSID to all the gadgets in its range. So anybody can see your SSID and can go into your system without your insight. So one must

handicap its SSID show setting yet in the event that still you need to telecast your SSID then one must empower the WPA2 encryption and mac location sifting so that just approved individual can get to the system and no other can exploit it.

1.9.6 Enable wpa2 encryption and limit the access of user by applying mac address filtering

For better wireless security one must encode its system with WPA2 convention as it is the best encryption calculation yet one can likewise utilize WEP, WPA encryption procedures if this one is not upheld by the router. You can likewise empower mac location sifting to permit just the approved PC to utilize the wireless system. By empowering separating you can stop the unapproved access of any PC.

1.10 Attacks on wireless network

Wireless medium is an open medium which is not secure intruder can attack a network easily. Following attacks can be done in the wireless network.

1.10.1 Identity theft

It is a crime in which the criminal masquerades itself with the identity of some other user for doing malicious activity for his personal use or benefit and all this record is stored in original user log so for any harmful activity the original user will be blamed for that. Intruder can use your identity for financial gain for doing transaction.

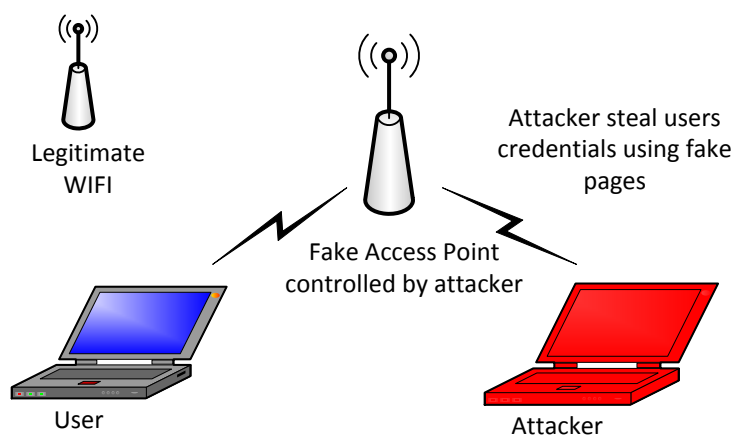


Fig 1.9: Identity Theft

1.10.2 Mac Spoofing

In this type of attack, to gain the access in a network where filtering is done according to mac address the intruder spoof its mac address to the authorized user and impersonate as original user

and break into the network and can access the resources which are available for only authorized users.

1.10.3 Man-in-the-middle-attack

As the name suggest there is a man that is an intruder in between the legitimate client and the server who is silently listening to the conversation and monitoring the packets without the knowledge of user and the server. This is a passive attack as both user and the server are unaware of the third person but this attack can be converted into active attack i.e. dos attack after receiving enough information to break into the wireless network. In which the intruder deny the availability of the services for the authenticated user and the user is devoid from getting resources.

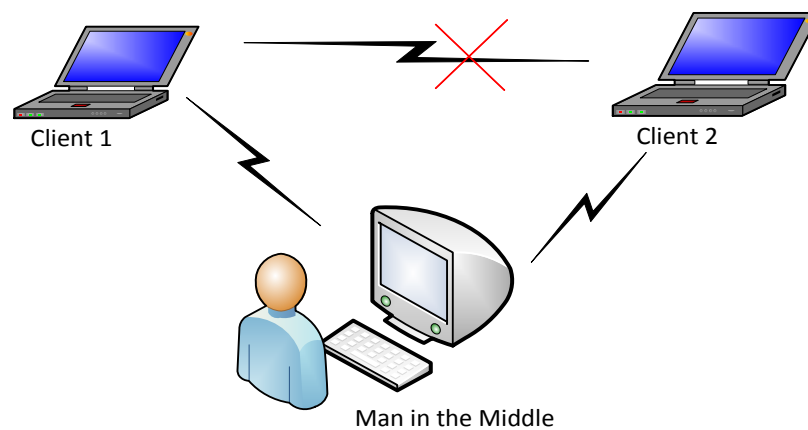


Fig1.0: Man in the Middle Attack

1.11 Disadvantages of wireless network

System specialists and clients extoll the advantages of Wi-Fi, saying its quick, helpful and adaptable. Be that as it may, remote systems administration has a few genuine weaknesses when contrasted with customary Ethernet.

1.11.1 Speed

While 802.11ac hypothetically bolsters an Ethernet-identical rate of one gigabit every second, or the considerably more famous 802.11n standard backings a most extreme pace of 600Mbps some more than a large portion of the velocity of 802.11ac. The issue gets to be significantly more intense in the event that you have an occupied system or if your sign quality is weaker than ideal.

1.11.2 Dependability

Remote systems administration uses radios to transmit systems administration signals. Pretty much as with physical or satellite radio, remote systems have a predetermined number of stations and, if each station is full, associations will back off or neglect to work.

1.11.3 Security

A wired system association must be caught by somebody who has grafted into the wire. But since remote associations experience the air, all that an individual keen on taking your data needs is a Wi-Fi collector, programming, persistence, and a work environment where he can get your sign.

1.11.4 Diminished Administration Control

Opening up your organization's system diminishes your control in two ways. The primary is that it makes it less demanding for your workers to interface their own particular non-sanctioned gadgets, similar to individual tablets or PDAs, to your system, devouring your data transfer capacity.

1.12 Organization of thesis

Our thesis work is organized as follows.

Chapter 2 is devoted to the writing survey that has helped in choosing the target. We broke down the security of the remote system and how to enhance its security. We will attempt to make the security instrument more secure and proficient. We will consider a few current answers for tackle the present issues and adding more strategy to relieve the issues and the impediments.

Chapter 3 clarifies the present or present work which we are performing in the remote network. In issue definition we have talked about the issues which depicts the issues which we are presently confronting. It is trailed by the goal of the issue in which we have examined our objectives which we will accomplish by our examination. It is trailed by the examination approach in which we have examined the method which we have received to finish our exploration.

Chapter 4 will contain the outcomes and execution of the proposed approach including the preview of every steps.

Chapter 5 we will total up our proposal by the conclusion and future extent of the performed work.

CHAPTER 2

LITERATURE REVIEW

Recently, there have been several proposed solution to solve the spoofed attack in wireless network by using more secure protocols or using encryption techniques to prevent/detect spoofed attacks. However most of them have some major drawbacks. They are described below in compact form

2.1 Lightweight detection of spoofing attacks in wireless network.

Qing li and Wade trappe [1], proposed a method based on the behavior of the sequence number of the packets coming from a specific destination to detect spoofing in the network rather than working on two consecutive frame differences it calculated n no of frames together and note their differences. It consist of a window which contains the n consecutive sequence number of frames and the detector calculate the n-1 sequence number differences from this it determines that if the value is greater than the threshold($T=3$) i.e. the probability of false alarm and missed detection then it is an intruder and generate a false alarm.

2.2 An improved method of detecting spoofed attack in wireless LAN.

Shikha and Sudesh [2], proposed an improved model of FRR (Forge Resistance Method) with rate analysis. It calculates the sequence number differences 'n-1' on window of packet size 'n' as FRR method does but for reducing the rate of false positive and false negative it also consider the transmission rate of frame with sequence number. Transmission rate reduces the rate of false positive by considering the chances of packet loss. Transmission rate can be calculated by taking difference of sequence numbers of consecutive frames with modulo 4095

$$\text{Transmission rate} = (S_{(i)} - S_{(i-1)}) / (T_{(i)} - T_{(i-1)})$$

Where $S_{(i)}$ and $S_{(i-1)}$ is sequence number and $T_{(i)}$ and $T_{(i-1)}$ represents the arrival time of i^{th} and $(i-1)^{\text{th}}$ frame.

Retransmission and frame coming out of order will decrease or equal the current sequence number to the last sequence number of the received packet.

If FRR verifies the packet as a spoofed one then before declaring it spoofed packet and without raising any alarm the content of that spoofed packet is matched with the copy of the packet generated by the monitor node which is used to analyze the traffic flow. If content is matched

then the packet is declared as original one but if content not match then we do the transmission rate of both the packets if first one fails then second is the genuine one but if second one fails then first one is the original packet and the spoofed packet will be dropped.

2.3 Using constant traffic to specific ip destinations for detecting spoofed MAC addresses in Local area networks.

E.C.Sasu et al. [3] this paper focuses on the behavior of legitimate user .In this mechanism admin maintain profiles for different user. First the server monitors the activity of its legitimate user by checking the ip addresses with whom the user is communicating, which sites are mostly visited by the user and note down the time duration of that communication session between the user and the destination ip address up to what time the connection was there and after creating the list of destination ip addresses with whom the legitimate user contact it checks the addresses where there was a constant traffic (i.e. to whom the user communicate regularly) and then from that list the server will evaluate the percentage of presence and absence of user on that specific destination and creates a fingerprint of it. And if any deviation is noticed it detect that the user address has been spoofed. It is a time consuming process because admin has to notice the activity of user for a long period of time to determine the normal behavior and it may also increase the false positive rate as behavior of user cannot be static it need to be updated time to time and any deviation from the normal behavior can raise the alarm. So we need a dynamic profile for this by using that profile we can stop the spoofed attacks as the profile will be updated automatically and the new behaviors of user will also be added on that one.

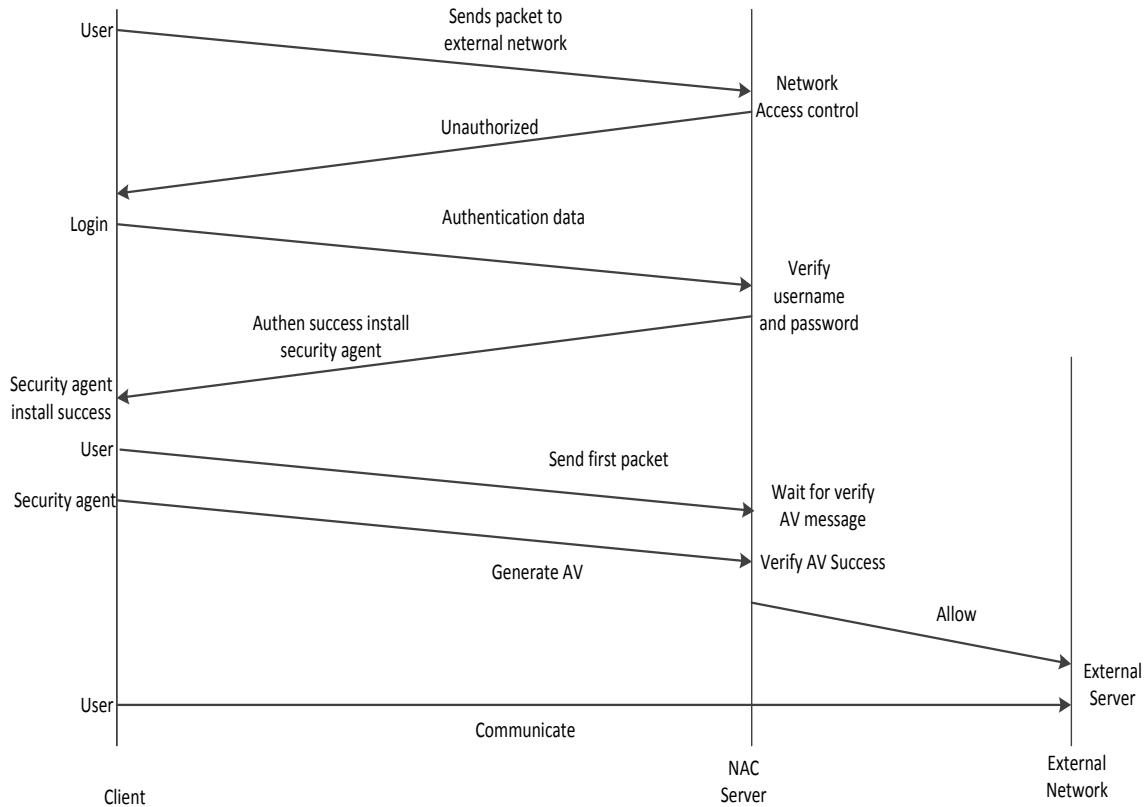
2.4 Using constant traffic to specific ip destinations for detecting spoofed MAC addresses in Local area networks.

Ahmad hassan and Xiaowen Zhang [4], give different kind of scenario through which an intruder can bypass the security and provided different solutions how we can manage the wlan security. As DHCP (Dynamic Host configuration Protocol) is not secured for web based authentication network as it broadcast the frames which can be seen by anyone even if we are not an authenticated client and this will benefit the intruder by monitoring the traffic intruder can get the detail of all the devices that are connected to the network or by using tcpdump or wireshark to capture these frames and can use this information for his personal benefits. So an authentication is required before connecting to the network as most of the network authorized

user based on mac address only so we can also provide unique username to user to validate legitimate user from the unauthenticated one. So before entering into the network user has to authenticate itself first and administrator must use strong protocol for security and user must register their mac address to admin by web portal or manually. Instead of using logout button to logout from network a pop up window should be used and authentication software should not leak any identifiable information. by using this technique intruder can be detected from the original ones and hence we can the spoofed attacks in the network.

2.5 A design of egress NAC using an authentication visa checking mechanism to protect against MAC against spoofing attacks.

Somnuk and Atthapol [5], propose a solution for protection against the mac spoofing. As intruder can easily enter into the network by just spoofing its mac address In this they implemented a NAC (Network Access Control) server which is connected to a gateway which is connected to the internet the client and attacker will also be connected through this gateway. So they generate an authentication visa (AV) which will be provided to the any user whenever they will try to connect to the internet. This Authentication Visa mechanism will be used during the web based login. In this authentication visa user has to provide its username and secret password which will be known to him only other than server and this key will be provided to him during the first authentication time and at that time a agent will be installed automatically in user device which will send messages to the server after the user enter its password and enter login when the server will receive the messages it will come to know that it is the authenticated client and the messages are generated from the agent only but if server will not able to find messages from the security agent then hence the admin will be able to identify the spoofed mac address and then spoofed mac will not able to enter the network. It is a good solution but it also has some drawbacks as if the file is deleted or corrupted by the user then user will not able to access the internet as no alternate is provided for this but tis method provide a good method to stop spoofed attacks in the network.



Fig

2.5.1: AV Mechanism

2.6 Media access control spoofing techniques and its countermeasures.

Archana et al. [6], proposed some solution to prevent mac spoofing in the network. As its being common nowadays to spoof the mac address of legitimate user and the intruder show itself as authenticated one and can get access to the network without the knowledge of server. As mac address is not encrypted during transmission of data. So intruder can easily spoofed the mac address and can take wrong benefit from it. So it is necessary to follow some step during connecting to the server for security purpose. Whenever a arp request comes that request must retrieve the mac address from LAN card by itself rather than checking for it and delete the entry once the mac address has been verified or if it doesn't find that mac address from its cache and we can lock our mac address in the router by using mac filtering and encrypt the communication between the router and the client.

2.7 IEEE 802.11 Anomaly-Based behavior analysis.

Hamid Alipour [7], et al. proposed a solution using an anomaly based technique for IEEE 802.11 network based on tempo-spatial data analysis to detect any variation from the normal

profile. As there are management and control frames that are not protected and can be easily exploit by the intruder for do any kind of attack. There are many DoS attack which can take advantage of this. So, they use a n-gram patterns which are extracted during online protocol behavior analysis as the protocol is observed in specific observation time window so the state transitions are validated for some specific interval of time and the protocol transition state are model through machine learning algorithms. The n-gram is a sequential behavior analysis method. A sliding window of fixed size is used to extract n-length subsequences which is known as n-gram.

$$n(\mathbf{n}\text{-gram}_i) = \min(\text{count}(\mathbf{n}\text{-gram}_i), \text{moc}(\mathbf{n}\text{-gram}_i))$$

$$np(\text{flow}) = \sum \mathbf{n}\text{-gram}_i \in \text{flow } n(\mathbf{n}\text{-gram}_i)$$

$$\text{allp}(\text{flow}) = \sum \mathbf{n}\text{-gram}_i \in \text{flow } \text{count}(\mathbf{n}\text{-gram}_i)$$

$$a_score(\text{flow}) = [1 - np(\text{flow}) / \text{allp}(\text{flow})] \times 100$$

where $\text{count}(\mathbf{n}\text{-gram}_i)$ represent frequency of $\mathbf{n}\text{-gram}_i$ in flow and $\text{moc}(\mathbf{n}\text{-gram}_i)$ represent maximum observed count for $(\mathbf{n}\text{-gram}_i)$ which is stored in normal transition model during training. $\text{allp}(\text{flow})$ means no. of all observed patterns in tat flow and $np(\text{flow})$ no. of normal ngram patterns. a_score is anomaly score if its exceeds the specified threshold then flow is considered abnormal. In protocol behavior analysis the frequency of sequence of protocol transitions over the observation time window is calculate to verify whether the device is behaving normally or not.

2.8 Medium access control spoof detection and prevention algorithm for spoofing attacks in wlan.

L.Arockiam and B.Vani [8], proposed an algorithm to prevent and detect the mac spoofing dos attack with a use of passkey value. This passkey is given to user at the time of authentication and a sequence number is provided to user which will be used by the user for transferring the data Whenever a user authenticate or disassociate itself from the network the passkey value was used which was generated randomly for a single session. A counter was maintained which is used for the authentication and disassociation messages and a threshold value was stored for authentication and disassociation of connection for the legitimate user. If frame value is 0 and its sub frame value is 12 then it was identified as disassociation frame or if it exceeds the threshold limit it will be identified as dos attack.

2.9 Wireless lan (wlan) spoofing attack- A proposed detection method in victim silent case.

Shikha goel [9], proposed a solution to detect an intruder in victim silent mode. As if the victim is in silent mode it is difficult for server to detect the intruder so a regular presence of legitimate user is needed in the network to show its presence so that intruder can't take its place. To detect the intruder in this mode firstly it is required that it must show its presence in the network after some regular interval. Second, monitor node can send an arp request periodically to the server. Then the ARP response field will be used to detect the intruder in the network as it will be synchronized with the last received sequence number of the packet. Therefore arp response sequence number will detect whether the packet is from legitimate user or intruder.

```
StringnameContains("<SSID>")ssidname=Between (Stringname, "<SSID>", "</SSID>");
```

2.10 Wireless Device positioning and finding intruder using rss.

Alex Joseph A. [10], proposed a solution to detect the intruder in the network by using RSS (Received Signal Strength). As we know if an intruder attack then it is difficult to determine from where the intruder is attacking so it's an important issue to locate that device from which the attack was done and to capture the intruder who has done it so RSS was proposed to locate the device using the signal strength of that device. Therefore the identity of client are noticed like longitude, latitude, mac address , time and date when it was first logged in that network in a XML based log file and converted into the RDBMS file for user recognition. To get the value of SSID name of the network from the log file we can use following query and can implement into the table.

2.11 Tracking rogue device in wireless Network System.

Amolkumar N. Jadhav et al. [11], proposed a solution to detect the rogue devices in the organization. Rogue devices are also termed as unauthorized device. It can be used to do the man in the middle attack or can be used to cause any kind of harm to the organization. So these rogue devices can be detected by first comparing the network SSID and mac address of wireless client as the authorized device information will be stored before. Now, 3 case can be formed from this first if the information is completely matched then there can be 2 possibilities it can be valid user or an intruder with spoofed information so to identify the real user from intruder they used timestamp information within beacon even if intruder has spoofed all the data but it will be difficult for intruder to synchronize. Second if information is partially correct now the device can

be rogue or misconfigured device so verifying the configuration of all the device will solve this problem and we will be able to detect the intruder. Third case if completely unmatched information then it would be either neighborhood device or internal employee rogue device. If device connects to the external network, we can assume that it is Neighborhood device or if the device connects to the internal network, it is Employee rogue device so through internally checking the device we can easily identify the intruder.

2.12 Detecting spoofing attacks in wireless network.

Khusboo Surin et al. [12], proposed a model to detect and prevent these attacks. This method was based on physical data like ip address, signal strength and mac address value of the device. This information is used to find the device location from anywhere. This data is does not rely on cryptographic techniques. If it is found that data is coming from two nodes having the same identity and both are claiming that they are the real one then the server detect the spoof and find the device location using the signal strength as the malicious node is identified then a response is send to the genuine user.

2.13 Detection of SSH host spoofing in control systems through network telemetry analysis.

Stainslav et al. [13], propose a method as it is very difficult to identify that's why their team proposed a solution for that uses meta-data that is not directly transmitted in the packet but comes into role when the data packet is send as these factors (throughput, response time, delay etc.) are associated with the transmitted packet. So they proposed a method with inter delay between the packets. As there will be always a time difference between the intruders transmitted packet and legitimate user transmitted packet which intruder can't be spoofed. The time of arrival of these captured packet of legitimate user is graphed including the deviation that can come in between and the server will create a node fingerprint so if any other deviation is observed then the packet will be identified as spoofed one. This method is little bit complex and needs extra computation power for calculating the difference between the user and the intruder and this technique may not give good result for mobile devices. It's also difficult for detecting the intruder if both devices are near to each other.

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

Due to open nature of wireless system it is easy for intruders to crack the system. Many techniques are available through which we can increase the security of our system but no one provides the full security. Even if we hide or stop the broadcasting SSID of our network still it doesn't make our system a secure one because SSID is broadcasted in response to client SSID query and many tools or commands are also available through which we can still see the hidden network SSID. So this method doesn't provide full security of our system. We can also do mac filtering in our network as it is more secure than the previous method. Mac address is the address which is used for identifying a device/system as it is the unique number assigned to each device but still it is easy for intruder to crack the system as mac addresses are not encrypted during transmission so an intruder can easily get the mac address of the legitimate user and can access the network using the mac address of the legitimate user by spoofing its own mac address to the authenticated one. Which is being a problem from starting because it's always difficult to find which one is the original node as both node claims to be the original one. So identity theft or masquerading attack is always being a problem for wireless network as the intruder can use the stolen identity for crime purpose or for accessing a secure network which is dangerous because for any malicious activity the legitimate user will be blamed. This problem arises because of the open availability of mac address as during the transmission of frames mac addresses are not encrypted. So our main focus is on securing the identity of the user.

Authentication is also one of the techniques which provide better security if we implement it with the mac filtering so that only authorized person can access the network but it is also vulnerable to some attack. Many techniques are present but still we are not getting a full secure environment .So, first main motive is to save the identity of user so that no one can spoof it and use it for their personal use. Second motive is to make the access of authenticated user secure so that no other then legitimate user can enter it .So, the main purpose is to provide a secure system for authenticated user without the fear of identity stolen and restricting the access of unauthorized user.

3.2 Objectives of Problem

As security is the main matter of concern so the main objective is to provide a secure environment for legitimate user so that they can communicate with other users in the network without losing the privacy. As security is the main concern nowadays and there are so many people out there who just want to steal the data of others and want to do wrong things by hiding their real identity so they use masquerading attack that is using the identity of someone else or impersonating as others so that they can't be caught for their misdeeds. So it is necessary that no one can steal the identity of others so we have to implement some security level for that to stop these type of things. In wireless network this attack is done by using masquerading attack also known as identity theft i.e. using the identity of someone else. In this intruder just spoof its mac address by using the mac address of someone else. mac address is the hardware address of a device i.e. assign uniquely to each device for its identification. So open availability of it make it insecure. So our main purpose is to hide the identity of genuine user so that no one else can use it except the real user.

So main objectives are -:

- 1) The first main motive is to save the unique identity of the user so that no intruder can access it and use it for its personal purpose.
- 2) The second motive is to increase the wireless security for authenticated user so that only authorized person can access it and no unauthorized person can take advantage of that.

3.3 Methodology

Main motive of this research is to provide a secure access to the legitimate user whenever connecting to the network so that the privacy should not loose and to stop the unauthorized access of the intruder. This method is a web based authentication system which will provide access to the authorized user only and stop the unauthorized access These are the following steps needed to maintain the privacy of the user -:

- When the new user will enter into the organization it will be provided with unique username and password which will be used when it will connect to the Wi-Fi services.
- User first has to register itself online so firstly, user will go to the homepage from there user has to select an option.

- If user is new to the network then it has to choose new user and then it will be redirected to registration page else it can choose cannot access the network option that is for the existing user.
- Now new user will enter its detail in the registration form along with its unique username and password.
- If details are verified then a zip file will automatically start downloading in user device else a message will be shown to user that invalid details.
- After successful download of zip folder user has to extract the files from the zip folder.
- Zip folder will contain one window application and a file that will be used during accessing the net.
- Now if user want to access the net it has to run that window application.
- As the user will run the application that application will secretly check for that other file that we have already stored in user device with that application.
- If file found then the user will be redirected to the login page where user will enter its unique username and password and click on login button.
- If details are verified then user can access the network but if not then it will be asked to verify it details.
- If user forget its password then it can also opt for forget password option which will redirect it to OTP page.
- A message will be send in user mobile or mail.
- User has to enter that one time password
- If it is verified then user will be redirected to reset password page where it can change its password and can access the network else if the OTP is wrong then a counter value will be incremented and if $\text{counter_value} > 3$ then user access will be blocked for 24 hours.
- If legitimate user is not able to access the network due to reason that file or application has been deleted or lost then then user can go to the homepage again and can select cant access the network option.
- This option will redirect the user to the OTP Page where user will be asked to enter the one time password.
- If password is correct then user will be redirected to the page from where it can again download the zip folder but if OTP is not correct then the connection will be terminated.

Algorithm

BEGIN:

User will enter all details with its unique Id and password then we will verify

- 1) *if*(user_type=new), then
Start downloading the Application in user device.
- 2) *else if*(user_type=existing), then
User already exist
- 3) *else*
Invalid user goto 14
- 4) //Now user has to run that application to access the internet and that application will //check for the secret file.
if(file_exists), then
redirect to login page
- 5) // But if file is deleted or lost by user then
else
Redirect to OTP page and send a password to user mobile or mail.
- 6) *if*(otp_attempt=3 times), then
Block access for 24 hrs.
- 7) *else*
Start downloading the application again in user device
- 8) Verify login credentials
- 9) *if*(user_credentials =true), then
Connection established
- 10) *else*
Wrong username and password
- 11) *if*(forgot_password), then
Redirect to OTP page and a send a password in user mobile or mail.
- 12) *If*(otp_password =true), then
Reset password
- 13) *else*
Disconnected

14) END:

This figure shows our proposed methodology that how client and the server will interact with each other and after all this procedure how user will be able to gain access to the internet. So to provide better security to user we have proposed this methodology this method will provide better security than any previous method. In this first a file will be downloaded on user device. User first has to extract those files. It consist of a secret file and a window application and by using that application user will be able to access the internet. If the request will not be generated from the application then user will not able to access the internet and the request will be disconnected.

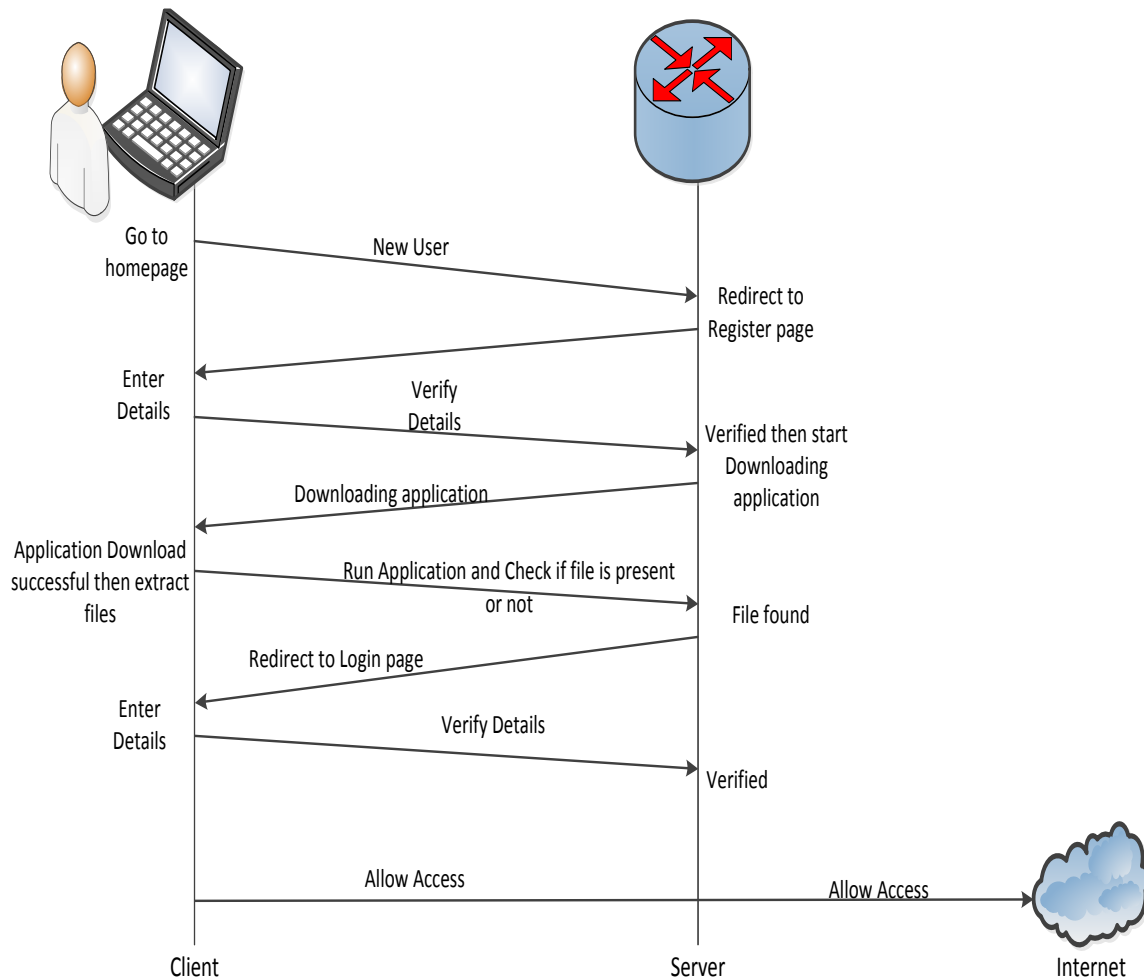


Fig 3.1: Proposed Methodology

Flow Chart

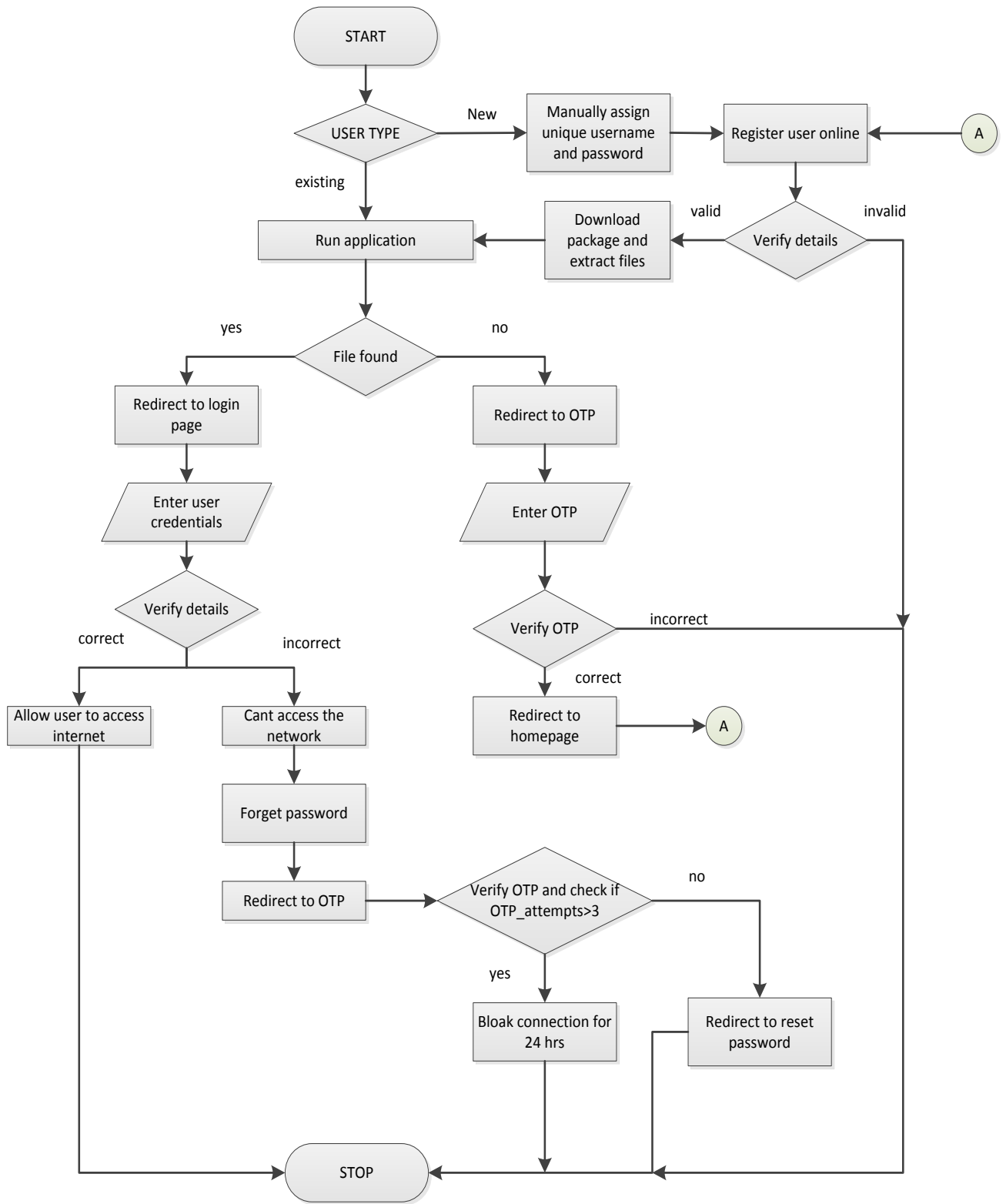


Fig 3.2: Flow Chart

CHAPTER 4

RESULT AND DISCUSSIONS

This methodology will give better results than the other previous techniques used in past. as we have stored a file in the user device which will help the server to recognize the legitimate client from the unauthenticated one. If the user is a legitimate one than his request will come from the application which can be identified by the server but if some request is made by some unauthenticated device then he will not be able to access the network because it is necessary for him to have that application to access the internet services no other request will be entertained by server only. This method also provides alternate option if user has lost his file or application he can still access the network by going to the homepage. There user is provided with the option cant access the network. If user will opt for that then the application package will be downloaded again in user device and he will be able to access the network again. In this server will able to recognize its client better than other older techniques even if there are two nodes claiming to be original one because the legitimate client will use that application to access the network. This method will provide a better recognition of clients to its server without any hindrance. So this method will provide improved security in wireless networks.

Experimental setup

The experimental environmental for demonstration of this algorithm is developed in visual studio 2013 windows application and web form. It is an integrated development environment (IDE) from Microsoft. It is utilized to create PC programs for Microsoft Windows, and in addition sites, web applications and web administrations. It is used to create both local code and manageable code. We use C#.net as the language for developing the application. For the storage of data we use SQL Server 2012 as the backend database.

Snapshots

1) Home page



Fig 4.1: Home page

Homepage is mainly design for the new user who have to register themselves for the first time when they will enter into the network for accessing the internet and for the existing user who are not able to access the network.

New user

After provided with the username and password by admin new user has to open the homepage website for downloading that application package through which it will be able to access the network. So new user has to opt for the new user button which will redirect user to the registration page where user has to enter its basic details.

Existing user

If existing user are not able to access the network because of some issues (like the file is deleted or if application is lost) then he can choose the cant access the network option. This option will redirect user to OTP page which will provide a alternate option to user to access the internet services.

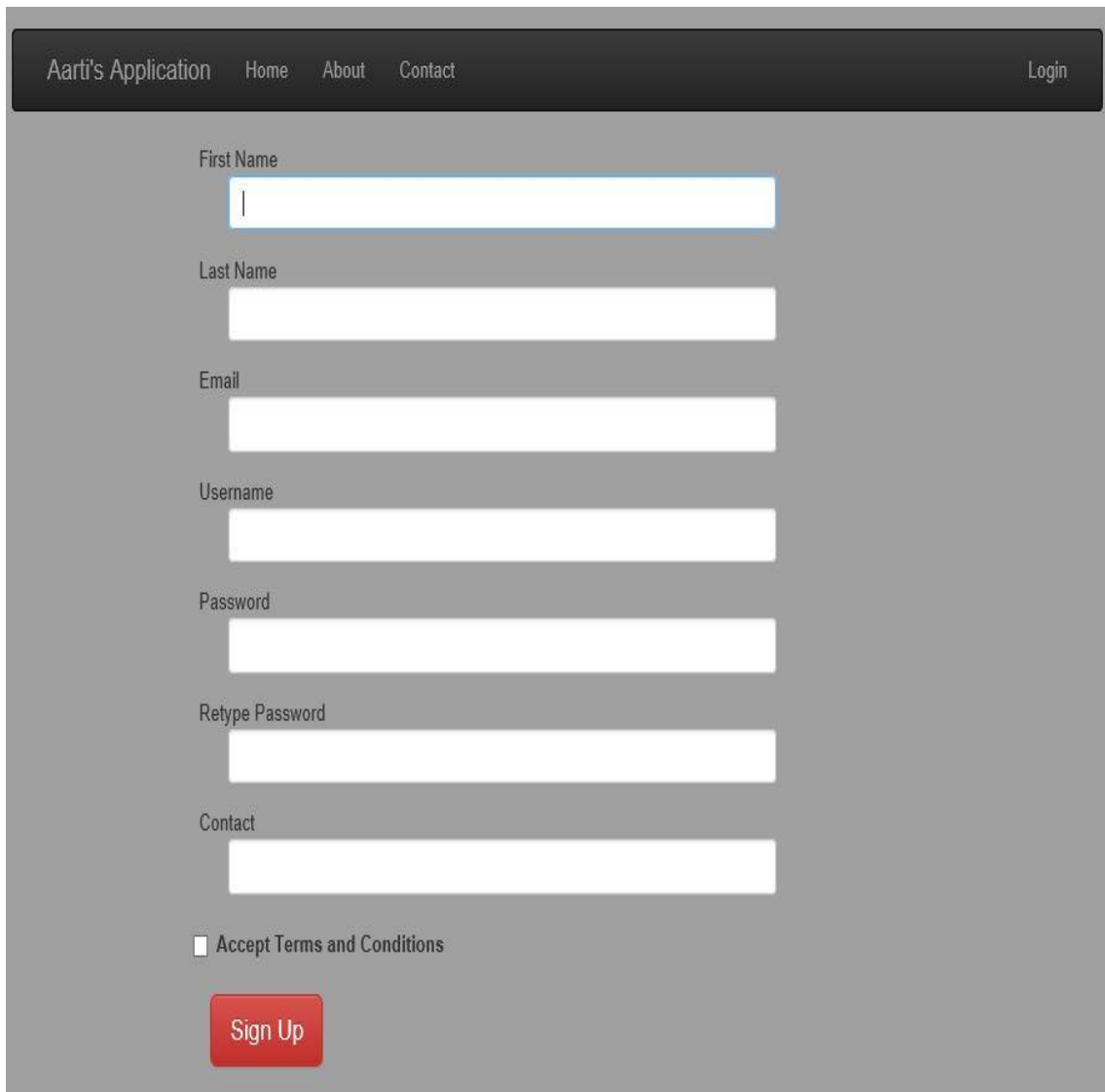
2) Reset Password

A screenshot of a web form titled "Reset Password". It contains three input fields: "Username", "New Password", and "Re-Type password". Below these fields is a "Submit" button.

Fig 4.2: Reset Password

If the OTP is correct then the user will be redirected to reset password page where user can change its password and after clicking on submit button the password will be changed.

3) Register page



The image shows a registration form for 'Aarfi's Application'. The form is set against a dark grey background. At the top, there is a navigation bar with the text 'Aarfi's Application' on the left and 'Home', 'About', 'Contact', and 'Login' on the right. The registration fields are arranged vertically and include: 'First Name' with a text input field containing a vertical cursor; 'Last Name' with an empty text input field; 'Email' with an empty text input field; 'Username' with an empty text input field; 'Password' with an empty text input field; 'Retype Password' with an empty text input field; and 'Contact' with an empty text input field. Below these fields is a checkbox labeled 'Accept Terms and Conditions' which is currently unchecked. At the bottom of the form is a red button with the text 'Sign Up' in white.

Fig 4.3: Register Page

When the user will click that new user button then he will be redirected to register page in which user has to enter its basic details. After filling all the details user has to accept the terms and conditions and as the user will click on sign up. The username will be verified with the admin database to check if the user is valid or not if it is not then it will be asked to verify its details but if it is a genuine user then a pop up will come asking for downloading the file.

4) Download application

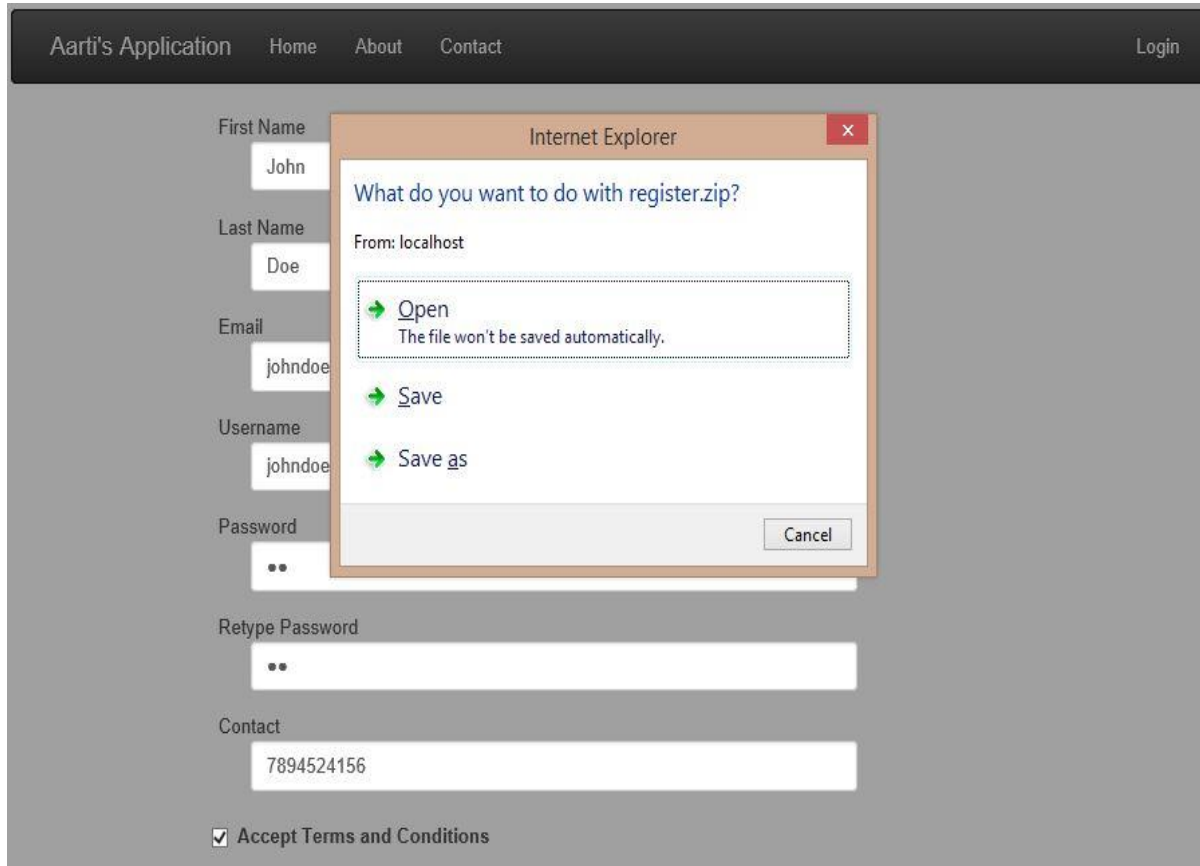


Fig 4.4: Download Page

When the pop up will appear user has to download that file. That downloaded file will contain an zip folder which consist of a window application and one other file. User first has to extract the files from the folder to use it.

Now from the next time whenever user want to access the internet services he has to use that window application. As the user will click on that window application it will secretly start looking for that other file that we have saved with the window application. If file found then user will be redirected to login page but if not then it will redirect user to the OTP page.

5) Window Application

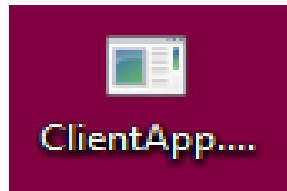


Fig 4.5: Window Application

This is the application that will be stored in the client device. That is used by the user to access the internet services.

6) Mac Capture

	firstname	lastname	email	username	upassword	contact	macaddress1	macaddress2
▶	John	Doe	johndoe1@gm...	johndoe_D	jd	7894524156	1C659D316C9F	
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Fig 4.6: Mac Capture

As user will click the sign up button in register page it's all data is sent to the database and it will automatically read the mac address of the user.

7) Login Page



Sign In

Username

Password

[Forget Password](#)

Fig 4.7: Login Page

As the user will run that window application and if the file is found then user will be redirected to the web page for login. After entering its credentials as the user will click the login button its details are verified with the database if credentials are correct then user will be allowed to access the internet but if not then user will not be able to access the network. But if user forget his password he is also provided with the option that forgot password. As the user will click this button he will be redirected to forget password page.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

As wireless security is being a big issue due to its open nature anyone can crack it easily. So our method will provide better result for protection of wireless network against the intruder. It will provide more security to user than any other techniques as we are storing a file in user device which will help us to identify the intruder from the authenticated client and it provide better recognition of clients to its server. So that the server can know its client even if intruder tries to spoof its mac address to enter into the network. Future work can be done on hiding the mac address of the client within the network and whenever he will leave the network his mac address will be reset again to the original one and this mac address will be valid within that network only. If we can hide the mac address of client and provide a fake address to the client which will be used to connect to the network then we will be able to provide user more confidentiality. Suppose if our client mac address are not hidden and intruder find out the mac address of legitimate client than not only intruder can do malicious inside the network but can also use the mac address of the client to do some attack in outside network and all blame will go to the innocent client. So, if we are able to hide the mac address of the client within network than we can save client from outside attackers.

REFERENCES

Research Papers

- [1] Qing Li and Wade Trappe, "Lightweight detection of spoofing attacks in wireless network", *MAHSS*, 2006, IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, IEEE International Conference on Mobile Adhoc and Sensor Systems Conference 2006, pp. 845-851, doi:10.1109/MOBHOC.2006.278663.
- [2] Shikha and Sudesh, "An improved method of detecting spoofed attack in wireless LAN", *NETCOM*, 2009, Networks & Communications, International Conference on, Networks & Communications, International Conference on 2009, pp. 104-108, doi:10.1109/NetCoM.2009.75.
- [3] E.C. Sasu and Prosteau, "Using constant traffic to specific ip destinations for detecting spoofed MAC addresses in Local area networks", *Applied Computational Intelligence and Informatics (SACI)*, 2012 7th IEEE International Symposium on; 01/2012.
- [4] Ahmed Hassan and Zhang, "Bypassing web-based wireless authentication systems", 01/2011; DOI: 10.1109/LISAT.2011.5784246 2011.
- [5] Somnuk and Suwannasa, "A design of egress NAC using an authentication visa checking mechanism to protect against MAC against spoofing attacks", *Computer & Information Science (ICCIS)*, 2012 International Conference on; 01/2012.
- [6] Hatkar Archana et al, "Media access control spoofing techniques and its countermeasures", *International Journal of Scientific & Engineering Research*, Volume 2, Issue 6, June-2012 1 ISSN 2229-5518.
- [7] Hamid Alipour et al., "IEEE 802.11 Anomaly-Based behavior analysis", *Computing, Networking and Communications (ICNC)*, 2013 International Conference on ,vol.,no.,pp.369,373,28-31Jan.2013doi: 10.1109/ICCNC.2013.65041112013.
- [8] L. Arockian and B. Vani, "Medium access control spoof detection and prevention algorithm for spoofing attacks in wlan", *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, ISSN: 2249-9555Vol. 3, No.2, April 2013.
- [9] Shikha goel, "Wireless lan (wlan) spoofing attack- A proposed detection method in victim silent case", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 2, Issue 11, November 2013.

- [10] Franklin Alex Joseph. A, “Wireless Device positioning and finding intruder using rss”, IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014.
- [11] N. Jadhav et al., “Tracking rogue device in wireless Network System”, International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 10, Issue 7 (July 2014), PP.81-84 2014.
- [12] Stainslav et al, “Detection of SSH host spoofing in control systems through network telemetry analysis”, 2014.
- [13] Sudha Khusboo Surin et al, “Detecting spoofing attacks in wireless network”, IPASJ International Journal of Computer Science (IJCS) ISSN 2321-5992 2014.
- [14] <http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html>
- [15] <http://www.infocellar.com/networks/ip/Images/mac-address.gif>
- [16] http://classic.www.axis.com/products/print_servers/applications/img/infrastr.gif
- [17] http://etutorials.org/shared/images/tutorials/tutorial_154/04fig06.gif
- [18] <http://petronellait.com/wp-content/uploads/2012/03/wan-diagram.gif>
- [19] <http://technews365.info/wp-content/uploads/2013/11/wirelessman.png>
- [20] http://t1.gstatic.com/images?q=tbn:ANd9GcRkiE8IZw9C0xGVIBcduC7RG4Q3kK5vgx_MSfgQ4OEJq_B23slYb
- [21] <http://www.vicomsoft.com/images/learning-center/wireless-networking/twolans.gif>

List of Abbreviations

A

AP Access Point

B

BSS Basic Service Set

BSSID Basic Service Set Identifier

D

DHCP Dynamic Host Configuration Protocol

F

FRR Forge Resistance Relationship

FRR-RA Forge Resistance Relationship - Rate Analysis

I

IEEE Institute of Electrical and Electronics Engineering

IR InfraRed

L

LAA Locally Administered Address

LAN Local Area Network

M

MAC Media Access Control

O

OUI Organizationally Unique Identifier

P

PC Personal Computer

PDA Personal Digital Accessories

R

RSS Received Signal Strength

S

SSID Service Set Identifier

W

WEP

Wired Equivalent Privacy

WLAN

Wireless Local Area Network

WMAN

Wireless Metropolitan Area Network

WPAN

Wireless Personal Area Network

WPA

Wi-Fi Protected Access

WPA2

Wi-Fi Protected Access 2