EVALUATING THE EFFECTIVENESS OF WIRELESS IDPS AS A CRUCIAL LINE OF DEFENSE FOR MULTIPLE WIRELESS NETWORKS

Suksham Gupta[1] ,
Assistant Professor,
[1]Department of Computer Science and Engineering,
Lovely Professional University,Phagwara

Abstract—Nowadays ,The emergence of wireless technology plays an important role in public and personal communication. However, its growth of has confused the traditional boundaries between trusted and untrusted networks. Wireless networks are subject to numerous threats and attacks at present. An attacker having the ability to listen all the network traffic which is becoming a probable intrusion. Any kind of intrusion leads to a disordered condition. To overcome this issue, a security solution that includes an intrusion detection and prevention system need to be implemented. . In this paper, based upon the various wireless network flaws and various challenges and issues on current which will overcome those limitations and enhance its functionalities.

Keywords—intrusion detection, intrusion prevention, wireless networks, proactive protection,WIDPS,WIPS,WLAN,limitation issues,challenges.

I. INTRODUCTION

With the fast development of wireless network,the problems on wireless security have become more and more prominence.Technologies of firewall and intrusion detection cannot solve these problems satisfactorily. However,Wireless intrusion prevention systems which can prevent attacks for WLAN excellently have become the research hotspot. WIDPS (Wireless intrusion detection and prevention system)monitors the wireless network and analyses wireless network traffic to identify suspicious activity. Threats to our networks are faster, smarter, more prevalent, more targeted, and more elusive than ever before. At the same time, the number and types of operating systems, applications and services running on the network continue to grow. Gaining visibility into different user types – remote, mobile, third-parties, and by job function – and accommodating their unique requirements adds even greater complexity when it comes to protecting our IT infrastructure

A. Limitations of wireless network

- First, The Wireless Technology provides a easy way of connecting no of computers to network via radio waves, So there exist no border of defense resulting in attacks from all potential places. An attacker using its wireless card and numerous detection tools to find any access point around. For example, Tools like Netstumbler or Kismet provides detailed wireless information such as channel, encryption method etc .Using the gained information, the attacker is able to exploit the target.
- Second, the present 802.11 WLAN encryption methods including WEP, WPA and WPA2 are all weak and insufficient [Salman B Kamli 2011].
- Third, wireless networks are subject to DoS (Denial of Service) attack by authentication flood, deauthentication flood, association flood, disassociation flood and so on. These attacks are so effective that the wireless target network will be unable to serve its legitimate users.
- Last, Attackers can attack wireless networks via MITM (Man in the Middle). By introducing an unauthorized *(rogue)* Access Point (AP) into the wireless networks, the hacker is able to collect sensitive packets in the transmissionprocess thus resulting in a chaotic wireless network environment.
- Intrusion Detection and Prevention Systems are considered the most important solution to solve this problem.As the intrusion prevention system are evolving greatly in their role to defend networks against attacks .So there must be a strong IPS solutions for the vulnerability and not the exploit.

B.Intrusion Prevention System (IPS)

Intrusion prevention is also pronounced as IPS which is basically a current extension of intrusion detection system pronounced as IDS .So before focussing on IPS, let's have a look on what is "Intrusion detection ".Intrusion detection is the process in which the events that are occurring in the network or computer system are being monitored and analyzed for possible incident signs that are violating computer security policies, acceptable use policies, or standard security practices[K.Scarfone,P.Mell (2012)].

Now let us have a glance on both IDS and IPS

IDS

1.Violation of configuration is detected and alarm is activated

2.Auditing of files, system logs, and real time traffic is done [K.Scarfone,P.Mell (2012)]

IPS

#It is the extension of Intrusion Detection System (IDS).

#It can sense an intrusion, and also stop that intrusion by successfully attacking theorganization by means of an active response [K.Scarfone,P.Mell (2012)].

So basically instead of using abbreviation as IPS, the abbreviation in this will be used as IDPS(Intrusion Detection and Prevention System) as IPS not only detects an intrusion but prevent it by providing an active response.

C. Need of IPS

- Firewall is the first shielding line, which prevents the network efficiently. But with a deadly defect-it only can prevent the intrusion from extranet. In other words, firewall can do nothing if an attacker attacks from intranet.

- Intrusion Detection System (IDS) provides a supplement to firewall by counter balancing the shortage of firewall efficiently. It has the ability of detecting improper intrusion and attack but lacks in preventing the attack.

- Intrusion Prevention System (IPS) merges the benefits of firewall and IDS. IPS enhances the performance of network security by detection and prevention of attack.

II. Problem Formulation

The main objective of Wireless IDPS is to monitor the wireless network and also to analyze wireless-specific traffic, including scanning of external users who are trying to connect to access point (AP), rogue APs, users outside the corporeal area of the company, along with WLAN IDPSs built into APs. The Scope of Wireless IDPS is to perform detection and prevention on a single wireless network .But as Wireless technologies popularity is rising to peaks due to increase in IT infrastructure and services and the distortion of borders between networks is occurring due to wireless communication, the vulnerabilities are also growing in wireless networks, and So does the possibility of attacks. For this reason, it was desired that a Wireless IDPS for multiple wireless networks should needs to be implemented, as Wireless Networks are of major concern today.The problem that lies with the WIDPS is that it is not effectual in the decryption of data flowing over the multiple wireless network, Hardly detect Unauthorized Clients, Less Accurate with high rate of false positives .Therefore, in this study the focus is to identify the capabilities of WIDPS and try to use it for the robust security level by using WIDPS this time as a defense tool by focussing on various security issues that have not been resolved by WIDPS till now and thereby enhancing the functionality of WIDPS for multiple wireless networks.

III. Objectives

The main objective of work is to define new methodology of WIDPS process on network. But this objective includes some key features.

1.To evaluate and analyse the possible tools.

2.To enhance the security of the established wireless network by knowing the importance of WIDPS.

3.To know about Challenges of WIDPS and try to overcome by developing an effective framework.

Defined a new methodology by using the concept of multithreading.

4.To conduct whole process of wireless IDPS in a successful and well organized manner on multiple networks

5.To develop the WIDPS which can analyze the encrypted and decrypted network..

To enhance the WIDPS by providing prevention by launching responsive actions in order to defend the system and/or the network. Research process has been conducted in different steps. Each phase is having its own importance. Figure 3.1 shows the research process flow diagram. On the basis of that research process overview has been given below.

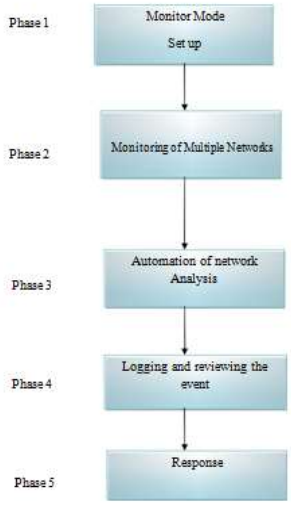


Figure 1 Research Process Flow

The WIDPS methodology consists of five phases, which are discussed below:

1. Monitor Mode Set up

Monitor mode is also called radio frequency monitoring mode .It will monitor all the traffic that is collected by the wireless network card .The benefit of setting up the monitor mode is that without associating with the access point we are able to capture all the network traffic.
In order to monitor different wireless network around us the following steps are performed:

A) The frequency of wireless card is set according to the channel frequency.

B) After this the wireless network card is set into promiscuous mode

C) After the above step is done, packet-capturing starts.

D) Analysis of wireless data packets is done.

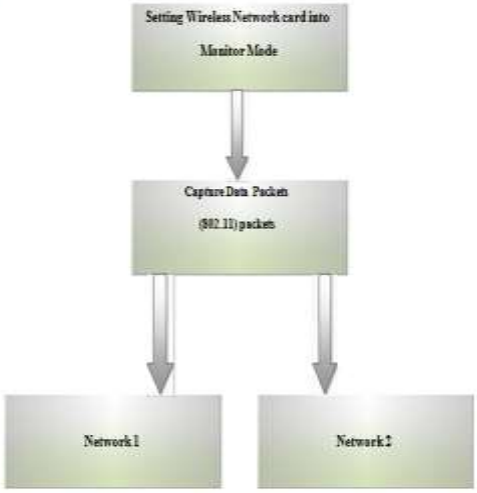


Figure 2: Steps of Monitoring network

2.Monitoring of Multiple Networks--After setting the wireless network card into monitor mode, it is now possible to monitor all the networks around. After getting information about different networks, the tool named Aircrack-ng from Linux is used for cracking out the network credentials

3.Automation Of Network Analysis--In this automated network analysis is done by using the framework designed in python. The conceptual framework designed for multiple networks analysis is done in parallel with multithreading .Here multithreading is a mechanism which will do parallel capturing of network networks and analysis of network together by keeping the captured files in .cap files .Theses files can be moved to separate storage for future analysis. When the traffic of unauthorized network is captured, it will be in encrypted form .Then it's monitoring of network is done. Decryption of data is performed by the usage of conceptual framework.

4.Logging and Reviewing the event--The capturing of data packets over the networks are stored in .cap file .Before starting for the monitoring the network again, the stored .cap is moved to some other storage for further analysis. So these files are used as the logs for providing the information about the network. It provides a means of analyzing the behavior of network at particular time

5.Response--This is the final phase of WIDPS for multiple wireless networks. In this phase, the unauthorized users will be prevented from accessing wireless network in the future by terminating the connection. Also capture and log packets prior, can be redirected to some spare system for detailed analysis which provide us the information about the traffic flowing over the network which can prevent intrusions over network by blocking the radio frequency or by blocking the switch port or by filtering.

IV. Results and Discussion

To set up the monitor mode on our system which will monitor all the around networks using linux utility tool .After that designed WIDPS framework with the new methodology of multithreading is used to monitor different networks and perform the functionality accordingly depending upon the type of network it is i.e. whether the network is authorized or whether it is unauthorized.

1.**Monitor Mode Setup--**Using the utility tool named airmon-ng of Linux, the system will be set up into **monitor mode.** The benefit of setting up the monitor mode is that without associating with the access point it is able to capture all the network traffic.

```
root@Apex:~# airmon-ng start wlan0


Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2485    NetworkManager
2741    wpa_supplicant
5898    dhclient
Process with PID 5898 (dhclient) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Broadcom        b43 - [phy0]
                                (monitor mode enabled on mon0)

root@Apex:~#
```

Figure 3: Monitor Mode set up

A. Architecture of Wireless IDPS Framework

The Architecture of Wireless IDPS framework is as follows-

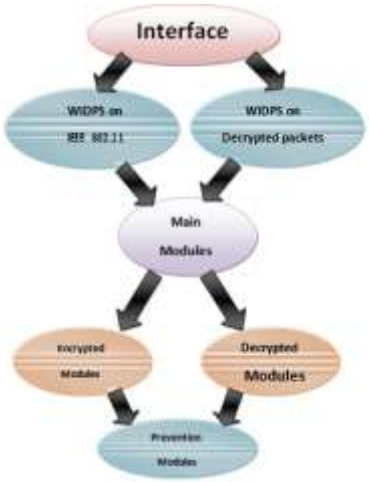


Figure 4: Architecture of WIDPS Framework

B. WIDPS Framework

The WIDPS framework is designed in python .It provides a new methodology, which facilitates the capturing of network traffic and analysis in multithreaded fashion. In this menu driven approach is provides the network monitoring and analysis with ease.I n this, we need to find out t he networks where this WIDPS framework can be deployed.The figure 5 below shows the interface of the WIDPS framework, which illustrates that WIDPS can be implemented on IEEE 802.11 packets or on the decrypted packets. In order to implement the WIDPS on the network, the BSSID is required.So when the designed framework is run, it runs in a multithreaded way invoking a sub process is invoked for finding out the networks around along with the information.

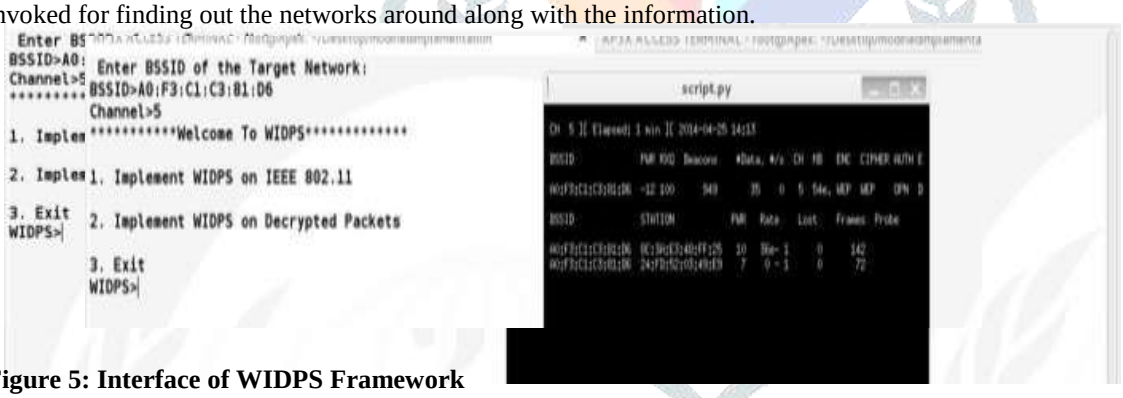


Figure 5: Interface of WIDPS Framework

The sub process that invokes from the framework of WIDPS,It displays the information of the network which is shown in the figure 6

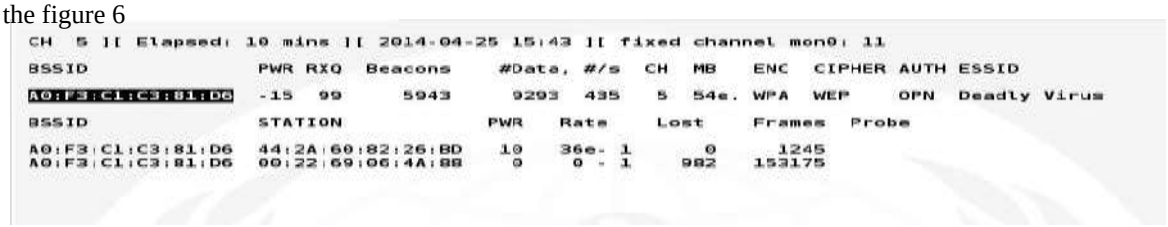


Figure 6: A Sub process showing different networks

When the WIDPS Frame work is executed without BSSID and channel, it display out an error message like syntax error or remove hash tags etc.When the network information is monitored from the sub process executed in multithreaded fashion, it displays the information given below in figure 7.

- The first number provides the information about the last data rate from access point (BSSID) to the client that is STATION. It is mainly 36 megabits per seconds.
- The second numb er provides the information about the last data rate from client that is STATION to access point (BSSID) to the. It is mainly 24 megabits per seconds.

- These rates may possibly vary on each transmission of data packets along with the last speed.



Figure 7: Entering BSSID and channel of Target network in the WIDPS Framework

As the framework is designed for implementing WIDPS on multiple wireless networks enhances the functionality of WIDPS scope to multiple networks. It provides us with numerous commands along with its usage information.General commands for WIDPS Framework includes:

- Implement on IEEE 802.11 network packets
- Implement on Decrypted Packets.
- Sub processes included in the IEEE 802.11 network packets for the WIDPS Framework are :

The figure 8 shows implementation of WIDPS framework on IEEE 802.11.In this when some clien t is requesting for authentication over th e network and the network provides the encrypted data packets over the network. T he WIDPS usage provides the authentication information even when the packets are encrypted along with the addresses of clients performing authentication and display to which network the authentication is being done.



Figure 8:Implementation of WIDPS framework on IEEE 802.11

As the framework is designed for implementing WIDPS on multiple wireless networks, thereby enhancing the functionality of WIDPS scope to multiple networks.It provides us with numerous commands along with its usage information.In order to provide the scope of WIDPS Framework to multiple networks where we may encounter number of networks in two cases:

1) The network where complete information is provided along with necessary credentials

2) The network where no information is provided .In order to provide this WIPDS Framework, The decryption needs to be performed which requires two tools.

->First to perform packet gathering

->Second for packet analysis and formative the key.

C.Decryption of Data

This phase involves decryption of encrypted data. The question is how the data can be decrypted for various APs in a particular region? The answer to this question is by using the AP's wireless authentication key. But in case an analyst is in a car which is lying near to the suspect's house, he carried out the investigation but he need to decrypt the data, the question is how he can decrypt the data without knowing the actual key used for authentication? The answer is by simulating an attack over the target network and finding out the key. As soon as the analyst gets the key, he can use utilities like AirDecap which will actually decrypt entirely encrypted 802.11 data into the normal Ethernet data.**Aircrack tool kit**-----Aircrack-ng is a software suite for the network which comprises of detector ,sniffer of packet ,WEP/WPA crack etc.It works with wireless network interface of any type which can support monitoring mode can sniff any data traffic of 802.11 network.First airodump is started to gather the packets;Then, AirCrack is started, the file just created by airodump is access ed, a 0 needs to be entered and the program determines the key.To crack the wifi password using aircrack toolkit is performed step by step First of all it is required to find out the network whose information need to be found.Information of different network is shown in the figure 9..

- Then putting the network interface card in monitor mode.

- Then the packet analysis is done for particular chosen network's BSSI D

- Packet analyzer performs the capturing of each packet information in a file named .cap file.

Then the key of the network is found by the captured HASH.

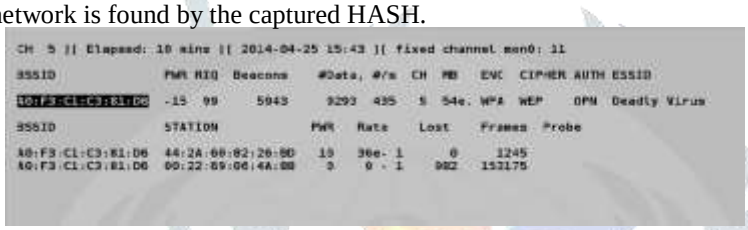


Figure 9: Information of different networks

After getting the information about the network using tool named Aircrack-ng Suite in order to find out the network credentials. Then the key of the network is found by the captured Hash shown in figure 10

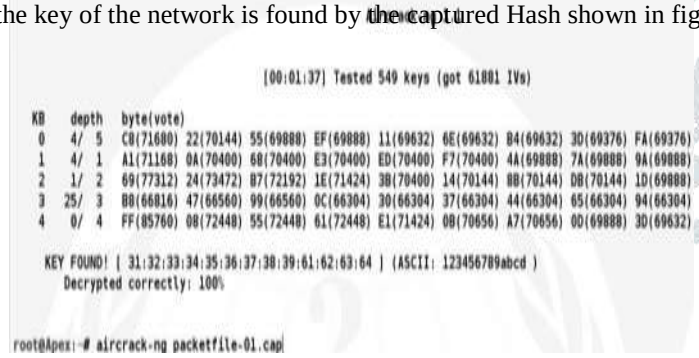


Figure 10: Cracking Key of the network

Now the focus is how the WIDPS Framework will be used on decrypted networks packets.After getting the necessary credentials of the network the WIDP S framework will provide the information of Hexadecimal value of the cracked key .It will provide us with the information which includes:

- **Total number of packets read** –It will provide the network information of how many packets that were sent over the network were read .

- **Total number of WEP data packets** – It will provide the information about what number of packets are of WEP type from the total number of packets being collected.

- **Total number of WPA data packets** – It will provide the information about what number of packets are of WPA type from the total number of packets being collected

 Total number of Plaintext data packets – It will provide the information about what number of packets are in the form of plaintext from the total number of packets being collected

 Total number of decrypted WEP data packets – It will provide the information about what number of packets are of WEP type and are in the decrypted form from the total number being collected

 Total number of corrupted WEP data packets – It will provide the information about what number of packets are of WEP type and are in corrupted form from the total number being collected

 Total number of decrypted WPA data packets– It will provide the information about what number of packets are of WPA type and are in the decrypted form from the total number being collected

 Total number of corrupted WPA data packets - It will provide the information about what number of packets are of WPA type and are in the corrupted form from the total number being collected

 Total number of encrypted data packets – It will provide the information about what number of packets are in the encrypted form from the total number of packets being collected

 Total number of packets –It will provide the network information of how many total number of packets that were sent over the network.

In order to illustrate the framework view for decrypted packets option 2 is selected which is shown in figure 11.it requires the need to enter the key of the network which is cracked using the tool of Linux.After choosing the option it provide the information about number of packets read,number of WEP packets,number of WPA packets,number of corrupted packets etc.Then WIDPS Framework designed will ask for which kind of decrypted information to be viewed. Select http filter for retrieving out http protocol information .Then Framework provides with the decrypted information about all HTTP protocol.

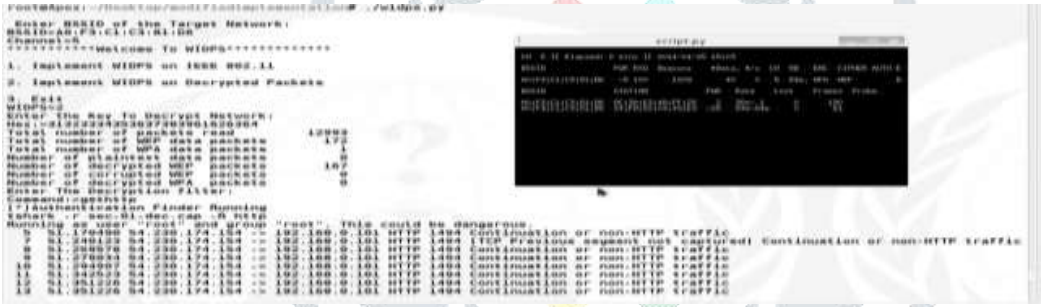


Figure 11: Framework View of decrypted Packet

D. Detection of Unauthorized Clients over the network

While performing the functionality of WIDPS, we may require the need to find out the clients who all are illegally using the network services. Using this framework, It is very easy to find out fake clients over the network .It lists out the complete information which includes all sources with the Fake MAC and all the destination devices are with the Fake MAC .It includes the details about the vendor along with its addresses .

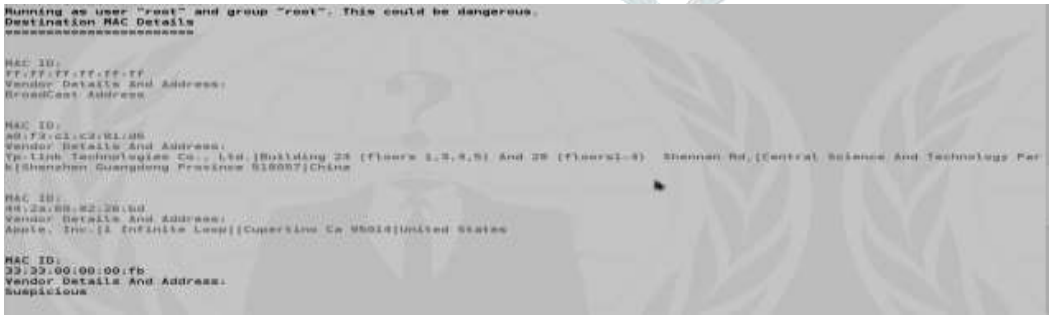


Figure 12: Detection of Unauthorized clients over the network.

E. Prevention in WIDPS Framework

While performing the functionality of WIDPS, we may require the need to find out the clients who all are illegally using the network services and violating the normal functioning of the wireless network.The Framework will lists out the

complete information which includes all unauthorized clients with the details about the vendor along with its addresses.When the information about the unauthorized client is available ,the deauthentication to that client is being performed in order to forcefully disconnect the client from the network.With this the false positive rate of WIDPS Framework will be less because network is prevented from the illegal activities by only stopping or blocking the client who is conducting the suspicious activity rather than the blocking the entire traffic.A subprocess is invoked upon the suspicious activity over the network which using utility named aireplay –ng .It intentionally disconnect the suspicious client from the network.

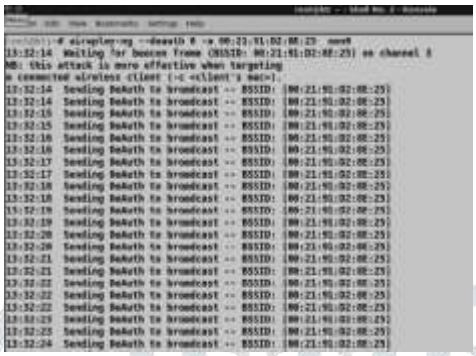


Figure 12:Blocking of unauthorized client performing illegal activities over the network

V. Conclusion

During research, the main aim is to define the best efficient method for implementing WIDPS Framework for the multiple wireless networks. Wireless networks threats are emerging at a rapid rate. The need of portable and flexible WIDPS is crucial and should be implemented widely. Lack of mechanism and approaches used as WIDPS are limited. The designed Framework extends the functionality and scope of WIDPS to multiple networks. The invent of the designed framework will sort out every type of challenges which are faced nowadays

VI. Future scope

The proposed Framework system will be very cost effective, reliable and flexible in the future directions, as it deals with multiple levels of detection and prevention.Future of wireless IDPS framework is under upgrading and is managing to add all the latest possible attacks in the network. The essential component of the security infrastructure is the prevention function that will overpass the gap between prevention and detection mechanisms. Therefore, the Wireless IDPS framework will be upgrading more ways of preventions

VII. References

Amardeep Singh, Gurjeet Singh(2010),” Vulnerabilities and Intrusion Detection in Wireless Networks”.China Internet Network Information Center(2010), "25th Statistical Survey Report on the Internet Development in China"
George Lawton(2010),”Fighting Intrusions into Wireless Networks”, TECHNOLOGY NEWS.
Guanlin Chen, Hui Yao, Zebing Wang(2010),”An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition”, 2010 Second International Conference on Future Networks.
Hiba M Yusuf (2011) ,”Wireless IDS” ,scbaghdad.edu.iq,College of Science, Baghdad University
Hugh J. M (2001) , "Intrusion and Intrusion Detection", Springer
Jack TIMOFTE(2008),”Wireless Intrusion Prevention Systems” Revista Informatica Economics
Jeff Dixon (2008),”Wireless Intrusion Detection Systems”.
John Bellardo, S. S. (n.d.). “802.11 Denial-of-Service Attacks:Real Vulnerabilities and Practical Solutions”.
Manish Kumar*, Dr. M. Hanumanthappa**, Dr. T. V. Suresh Kumar(2012),” Intrusion Detection Systems Challenges for Wireless Network”, International Journal of Engineering Research and Applications (IJERA) .
M.Salman,B.Budiardjo,K.Kamli(2011),”key-issues-and-challenges-of-intrusion-detection-and-prevention-system-developing-proactive-protection-in-wireless-network-environment.
Nilotpal Chakraborty (2013),” Intrusion Detection System And Intrusion Prevention System: A Comparative Study”.
Partha Dasgupta and Tom Boyd (2010),”Wireless Network Security”, Dept. of Computer Science and Engineering.
Pushpa,Yashpal Singh & S. Niranjan (2013),” Implementation Of Honeypot As An Intrusion Detection System For Wireless NETWORK” International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR).
The Government of the Hong Kong Special Administrative Region (2010),”Wireless Networking Security”.
Yaqing Zhang,Srinivas Sampalli(2010),” Client-based Intrusion Prevention System for 802.11 Wireless LANs”, 2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing. Networking and Communication