WIDS Using Flow Based Approach

Dissertation

Submitted By

Rahul B. Adhao

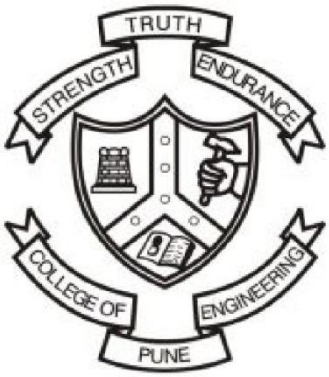
MIS No: 121222012

in partial fulfillment of the requirements
for the degree of

M. Tech Computer Engineering

Under the guidance of

Dr. V. K. Pachghare



DEPARTMENT OF COMPUTER ENGINEERING AND INFORMATION TECHNOLOGY

COLLEGE OF ENGINEERING PUNE-5

JUNE, 2014

DEPARTMENT OF COMPUTER ENGINEERING AND INFORMATION TECHNOLOGY, COLLEGE OF ENGINEERING PUNE

CERTIFICATE

This is to certify that the dissertation titled

WIDS Using Flow Based Approach

has been successfully completed

By

Rahul B Adhao

(121222012)

and is approved for the degree of

Master of Technology Computer Engineering

Dr. V K Pachghare
Project Guide,
Department of Computer Engineering
and Information Technology,
College of Engineering, Pune.
Shivajinagar, Pune-5.

Dr. J V Aghav
Head of Department
Department of Computer Engineering
and Information Technology,
College of Engineering, Pune.
Shivajinagar, Pune-5.

Date / /

"Guru Brahma Gurur Vishnu
Guru Devo Maheshwaraha
Guru Saakshat Para Brahma
Tasmai Sree Gurave Namaha"

Dedicated

To all my Gurus for their
guidance and

Constant
source of motivation for me.

Acknowledgments

I express my deepest gratitude towards my project guide **Dr. V. K. Pachghare** for his constant help and encouragement throughout the project work. I have been fortunate to have a guide who gave me the freedom to explore on my own and at the same time helped me to plan the project with timely reviews and constructive comments, suggestions wherever required.

I am also grateful **Dr. J V Aghav** (Head, Department of Computer Engineering and Information Technology, College of Engineering, Pune) for providing all resources for project work whenever needed. I also take this opportunity to thanks all teachers and staff who have constantly helped me grow, learn and mature both personally and professionally throughout the process.

A BIG thanks goes to my dearest classmates who made this journey so joyful and sporty without whom the journey wouldn't have been so interesting and memorable. They have always supported, guided me and have helped me stay sane throughout this and every other chapter of my life. I greatly value their friendship and deeply appreciate their belief in me.

Most importantly, I would like to express my heart-felt gratitude to my family.

Rahul B Adhao

Abstract

Wireless Technologies in the most straightforward sense empower one or more systems to communicate with each other, without using any physical medium like cables. That is the reason wireless network technology is the quickest developing portion of communication business sector. But unprotected wireless network essentially “Open the front door” of your network to intruder. Possibly he can access your shared devices and data, read your email, access websites and capture data for further analysis and takes as long as they need to crack rest of your system. Thus intrusion refers to an action done intentionally or unintentionally, which threaten the security, Integrity, Availability and Confidentiality of the network system.

In wireless network, specific protocol used, that challenge regular IDS to work properly in that network. So that’s why separate IDS are designed for wireless network, i.e. Wireless Intrusion Detection System (WIDS). But nowadays wireless network are very ubiquitous and protection of data in such network is very much important. Since last ten years, number of people using internet are increasing very rapidly. The research in network technology causes network speed to be increased and parallel the numbers of attacks also. So as internet is developing rapidly in size and complexity, complete understanding of network traffic also becoming difficult. In such cases, traditional packet based IDS could no longer useful. This is the reason that flow based approach is becoming popular. But at the same time it somewhere suffers by accuracy, when compare to traditional packet based approach.

The proposed Wireless Intrusion Detection System (WIDS) is designed by focusing mostly on flow along with packet based for certain circumstances. So our intrusion detection for wireless LANs can react to ever growing amount of data on network, also help to minimize resource consumption, seen in case of fully packet based system. It can detect attacks like DoS, Worm and Vulnerability Scan.

Contents

List of Figures

List of Tables

1. Introduction

The Internet and World Wide Web continues to rise in popularity. Social networking developed in the 21st century as a famous social communication, largely supplanting much of function of email, message board and instant messaging services. So the advantages of networking increasing, the number of Internet users also increasing very rapidly. According to Internet and Mobile Association of India (IMAI), India had crossed the 200 million in October 2013 report. They also estimated that it could be 243 million by June 2014, overtaking America and becoming world second biggest Internet base after China, as shown in below fig. 1.1 [1]. Along with this, technology like 3G, 4G are increasing speed of Internet access. Thus increased number of users (traffic) and ever increasing speed of network affect security of networks. As we know, nowadays Internet is being used not only for entertainment or educational purpose but also being used for commercial activities like online shopping and fund transfer. So by keeping all this things in mind, providing proper security to your network is very much important. But as already said, day by day network speed is increasing there is also need of equivalent faster security approach.

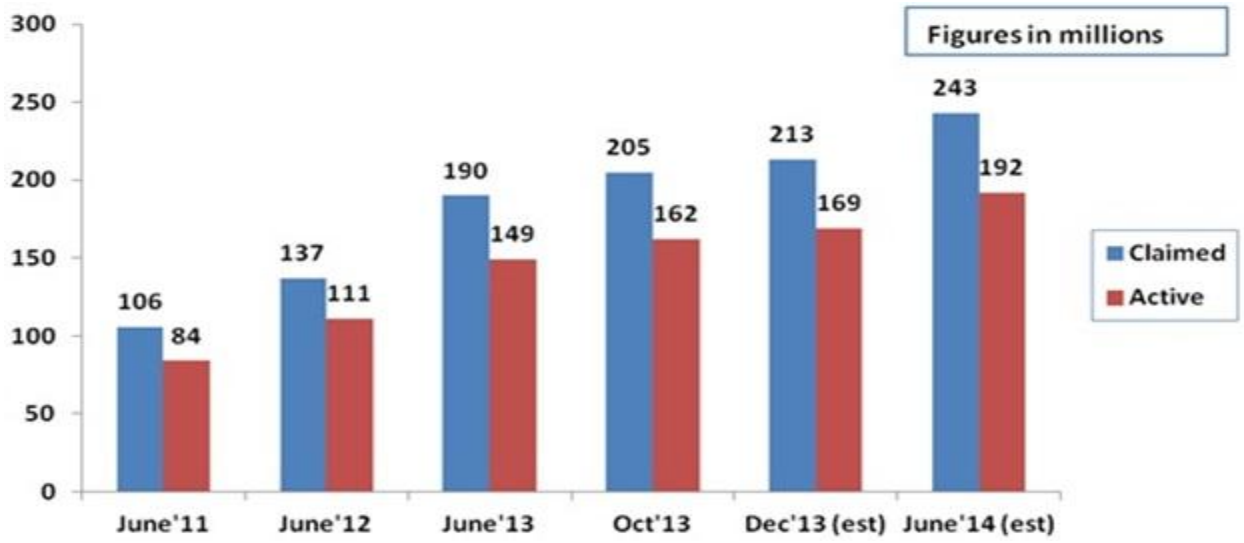


Figure 1.1: Total Number of Internet user in India

1.1 Network Security

Computer security is actually information security applied to computers and network. It covers all the processes and mechanisms by which computer based equipment, information and services are protected from unauthorized access. However complete preventions of security breaches are, at present, unrealistic. We can, however, try to detect this intrusion attempt so that action may be taken to repair damage later [2]. Intrusion Detection is a type of security management system for computers and network.

Wireless network are quick turning into the standard in the enterprises of all shapes and sizes. The easiness of deploying and simple administration made all these possible in comparison with the torment of deploying, administering and keeping up a wired network.

1.2 Wireless Networks

Wireless network`s security is much more complex than wired one. Wireless Technologies in the simplest sense enable one or more devices to communicate without physical connection – without requiring network or physical cabling. That's why wireless network technology is the fastest growing segment of communications market. But unprotected wireless network essentially "Open the front door" of your network to intruder that can access your shared devices and data, read your email, access websites and capture data for further analysis and takes as long as they need to crack rest of your system [3].But the benefit it is giving cause wireless network to be seen everywhere and day by day the speed with which it can be accessed getting increased because of ongoing research in this field [4]. Along with laptop and Desktop, you can access this network even with your hand held devices like PDAs, cell phones at same speed.

But introduction of such new hardware and technology along with new user friendly applications, resulting fluctuation of volume and the kind of traffic in the network. So though the network speed is increasing, the security of such networks continues as a thing of concern. To deal with such speedy network, packet based approach of Wireless Intrusion Detection System (WIDS) can never be suited. So there is need for faster security approach.

For WIDS to process packets coming at high frequency are very difficult. So instead of focusing on each packet, it can focus on flow of packets. In case of flow, the communication patterns within the network are analyzed, instead of content of individual packets [5]. But flow-based NIDS are still suffering from generating high false alarms. We could state a tradeoff between

accessibility of limited data of flow-based approach, which have negative impact on accuracy of NIDSs, and full data of packet-based which lead to a higher resources utilization. Therefore flow-based detection ought not to substitute the packet inspection approach [6].So both the methodologies are consolidated into a two stage discovery technique. At the first stage, flow based could be utilized to recognize certain attacks. At the second stage, packet based may be utilized additionally to protect critical server or selected system, for which the first stage has discovered suspicious activities [7].

1.3 Intrusion Detection System

An intrusion can be defined as the act of gaining unauthorized access to a system so as to cause loss or harm. So IDS are becoming integral part of network monitoring [8]. The rapid proliferation of computer network has changed the prospect of network security. Unfortunately the risk and chances of malicious intrusion still continues. According to Krugel et al; "intrusion detection is the process of identifying and responding to malicious activity targeted at computing and network resources" [5]. So IDS does not usually takes preventive measures when attack is detected, it is reactive rather than proactive agent. It plays role of informant, not of a police officer.

There might be question how IDS differ from antivirus, firewall. As they all are related to computer security. Anti-virus prevents and gets rid of viruses, malware, Trojans. Antivirus is a program that prevents hurtful software from installing and harming your machine. Antivirus software secures the machine from contaminated files. Firewall keeps away hacker from being able to hack your machine from outer world. Firewall blocks unauthorized connections from other computers/hackers. Firewalls secure the systems network ports from unwanted software traffic. Therefore firewall limits the access between the networks in order to prevent intrusion and does not signal an attack from inside the network. An Intrusion detection system (IDS) is software and/or hardware intended to locate unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet [9]. It also watches for attack that originates from within a system. An IDS provides much the same purpose as burglar alarm system installed in house.

1.3.1 IDS Classification

IDS can be classified in various ways based on various parameters like types of data processing, the type of analysis or the source of the data. However we can classify IDS into two widely known classifications, signature versus anomaly-based and host versus network-based [10], as shown in below fig. 1.2.

Signature-based intrusion detection works by identifying specific pattern of events or behaviors that accompany an attack. Each such pattern is called a signature. A signature-based IDS maintains a database of known signatures. It attempts to obtain match between the currently observed behavior of the system and an entry in this database. A real world signature based IDS will have thousands of attack signatures against which to compare. An example of an attack signature is a specific bit sequence in a worm payload. Anomaly based IDS involves making a determination whether the behavior of the system is statistically significant departure from normal. The IDS will have to learn, over time, what constitute normal activity, usage and behavior. Moreover, the definition of what is normal may vary as a function of the time of the day or the day of week. What is normal may also vary from one host to another [2].

In Host based system, the IDS examines at the activity of on each individual computer or host. It is designed to run as software on host computer system. Its main job is to monitor the internal behavior of the host such as the sequence of system calls made, the file accessed etc. For this purpose, its make use of system log, application logs, and operating system audit trails to identify events related to an intrusion. In a network based system the individual packets flowing through a network are monitored and report on all network traffic. The NIDS can detect malicious packets that are designed to be firewall`s simplistic filtering rules [8].

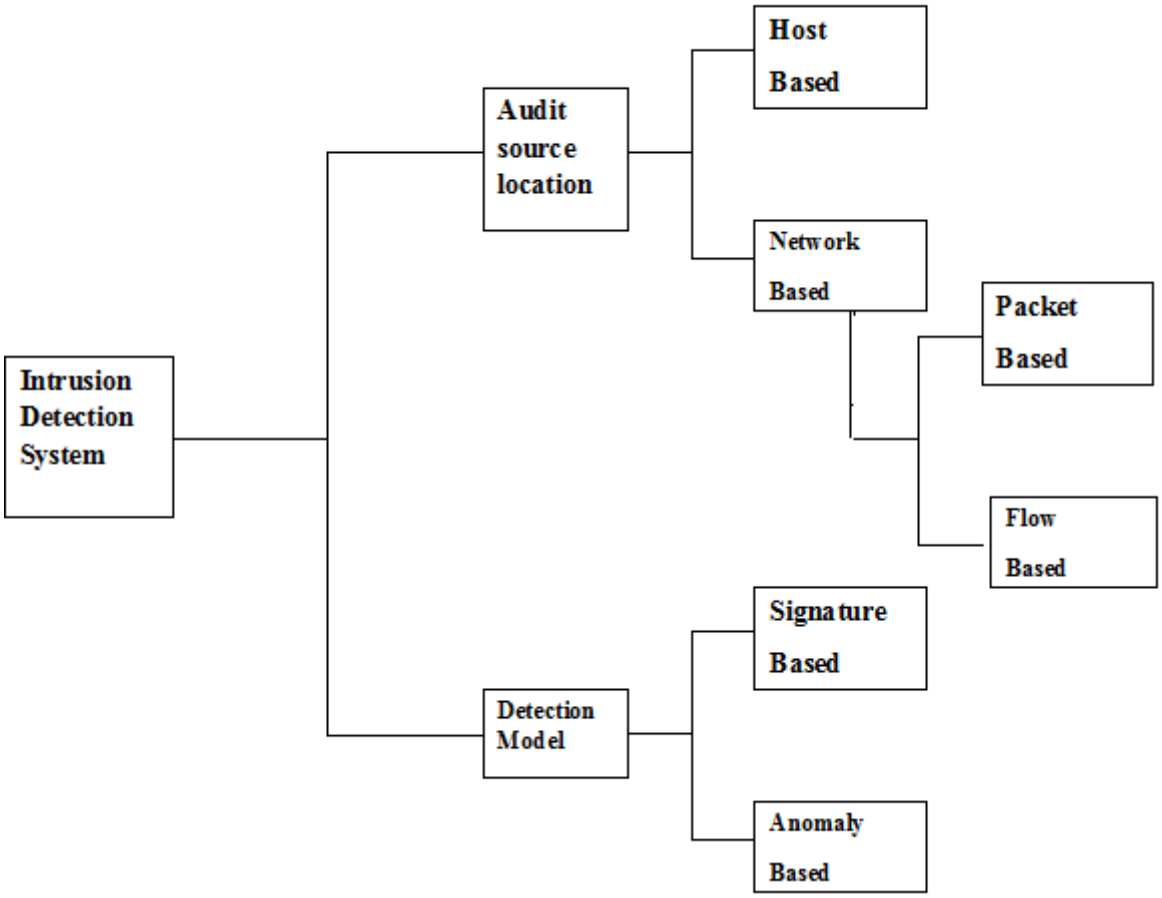


Figure 1.2: IDS Classification

NIDS can be further divided into two types on the basis of types of data to be analyzed in NIDSs: packet-based and flow-based. Packet-based has to look at the complete payload content along with headers. In case of flow-based NIDS, instead of looking at every packet passing through a network, it works on aggregated information of network traffic (Flow Record), so the amount of data to be analyzed is reduced [6].

1.3.2 Architecture of IDS

A WIDS could be centralized or decentralized. In case of first one, WIDS is typically a combination of individual sniffers which gather and send all wireless traffic data to a central system, where the wireless IDS data is stored and processed. Decentralized wireless intrusion

detection usually incorporates one or more devices that perform both the data gathering and processing/reporting functions of the IDS [10].

1.3.3 Desirable features of IDS

The two desirable features of IDS are Speed and Accuracy [8].Speed is especially important in fast spreading Internet worms, for example. Early worm detection and early response mechanism such as automated system shutdown can help in reducing the number of infected machines.IDS should be able to detect every instance of an intrusion. The two aspect of accuracy are sensitivity and selectivity- high sensitivity implies a low false negative rate, while high selectivity implies a low false positive.

Overview of Dissertation

This chapter frames the basic of security and intrusion detection system along with need and classification. Chapter 2, highlights the till date research on intrusion detection system from flow base point of view. It also includes details of flow base attack like DoS, Vulnerability Scan and Worm. Motivation and Objectives are discussed in chapter 3. Architecture and flow chart of proposed system is explained in chapter 4. It also details both the stages of the proposed system. Chapter 5 presents experimental analysis and result of the system. It talks about detection of flow based attack experimentally. At the end Conclusions and Future Scope conclude the thesis, with summary of proposed system and opportunity for future work.

2. Literature Survey

In Introduction chapter, we stated the situation of today`s and future Internet and also focused on need of fast and scalable security approach. In this chapter we discussed background information on Network Security, Intrusion Detection System, NetFlow and attack which play important role in this dissertation.

2.1 Network Security

Network Security compromises of the procurement and policies designed by a system administrator to avoid and monitor unauthorized access, abuse, alteration or denial of network services or resources [11]. While talking about network security, it must include the whole network. Means it should not be like security of only computers at the end of communication channel. The data flowing across communication channel should not be vulnerable to attack.

For development of secure network following things need to takes into accounts [12]:

- Access: Only legal users are allowed to use the network.
- Confidentiality: Privacy of Internet flowing through network.
- Authentication: Confirmation of legal user.
- Integrity: Message should not be modified in transit.
- Non-repudiation: User should not refuse that he has done that activity.

Network Security is domain of Information security. Because network security deals with prevention, detection and response to misuse of network infrastructure, which intern possess problem to confidentiality, integrity and availability [13]. For security of a network, network model and network monitoring plays important role.

2.1.1 Network Model

Internet can be defined as network of nodes, consist of sub-networks. Network topologies and traffic are the two important modeling concepts. With the good understanding of these two concepts, we can design a system that provides a good system that provides a good balance between accuracy and efficiency [14].

In case of wireless network, there are two network models, infrastructure and ad-hoc. Infrastructure mode is one where access point is needed for communication as shown in figure 2.1. Ad hoc model does not need any infrastructure. Each wireless node can communicate with other directly, no need of any access point, as shown in figure 2.2. The group of routers and other network devices which are controlled by one admin forms an Autonomous System (AS), and the gateway routers plays role of forwarding traffic to and from other autonomous system as show in figure 2.1 [28].

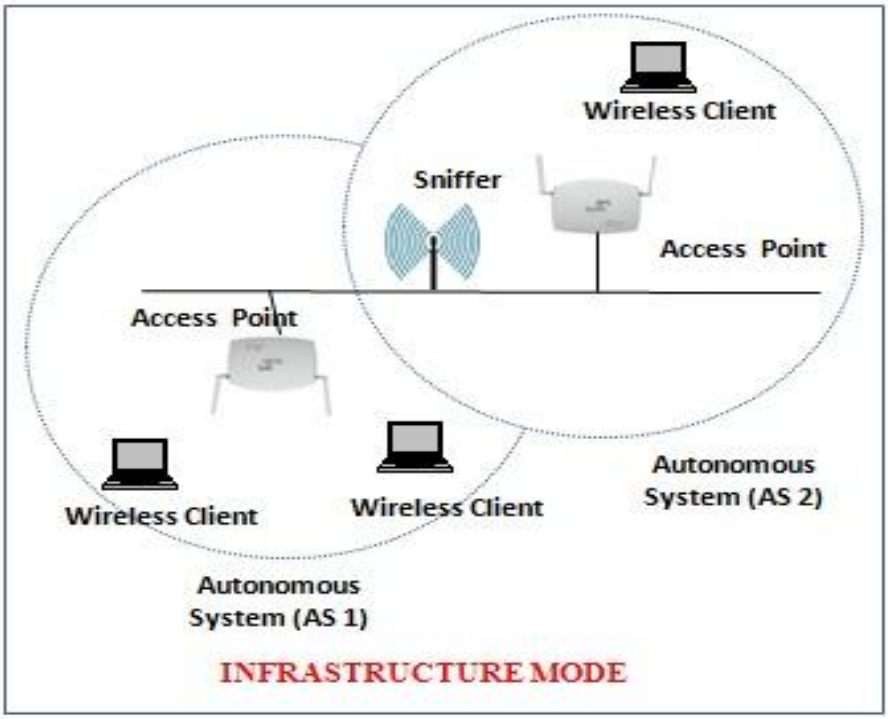


Figure2.1: Infrastructure Based wireless network

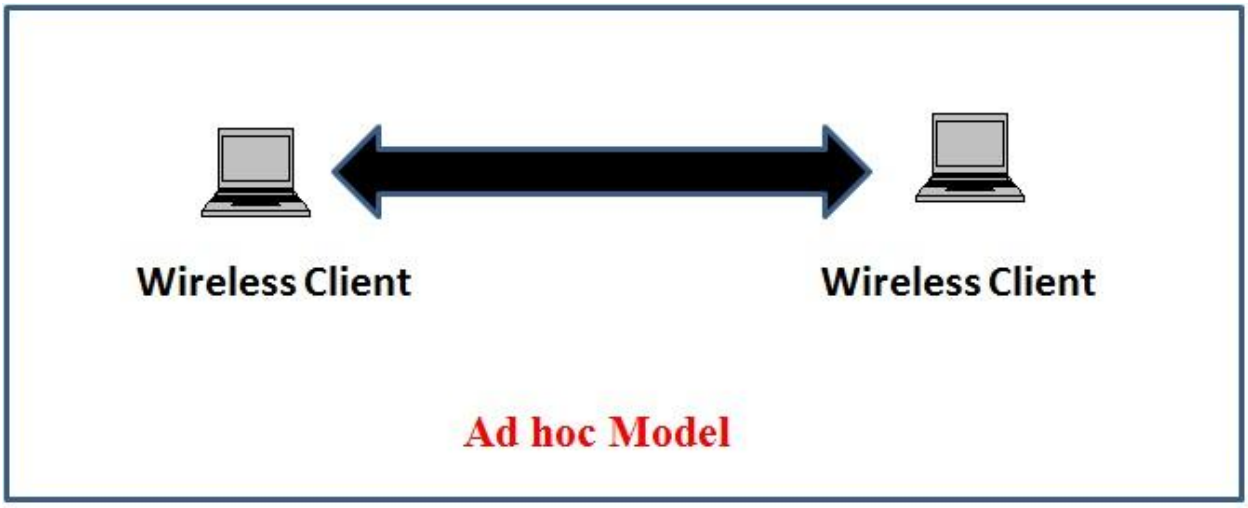


Figure 2.2: Ad hoc wireless network

2.1.2 Network Monitoring

Network security and network monitoring are closely related discipline, but members of this discipline have inadequate interactions. Network security focuses on security of important data and resources within network from harmful attack. Network monitoring deal with securing network services from attacks and accidents, when nodes in such networks are being penetrated and compromised [15].

2.2 Intrusion Detection System

An intrusion can be defined as the act of gaining unauthorized access to a system so as to cause harm or loss [16]. An Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. [17].

2.2.1 Evolution of IDS over the Time

Since the Intrusion Detection Technique introduced to network security world by James P Anderson in October 1980, a much of work has been done on it. Some of which are discussed below table 2.1 [21], giving author of paper and their contributions.

No	Author (Year)	Contribution
1	James Anderson (1980)	This paper indicated that audit files could be used to identify network threats and to recognize computer or network misuse. This is on the basis of that an intruder`s behavior will be observably not quite same as that of honest client.
2	Dr. Dorothy Denning (1985)	This was actually foundational work for Intrusion Detection Technology. It focused on tracing user activity using audit trails. In next paper he also focused on anomaly based intrusion detection.
3	Haystack (1988)	This paper presented a mixture of anomaly Detection and misuse detection IDS. Haystack used a different statistical anomaly detection algorithm.
4	Mukherjee B., Heberlein L., and Levitt K (1995)	This was a survey paper on host based and network based IDS. This paper talked on characteristics of host and network based IDS.
5	Axelsson (1998)	This paper described intrusion detection in local area network, connected to internet. Vulnerability in IDS was also discussed in this paper. The network security standards, general connectivity and compatibility requirements of IDS were also discussed.
6	Lee W. and Stolfo S. and Mok K (1999)	In This paper, adaptive intrusion detection system was designed.
7	Giovanni (2004)	Giovanni designed a tool which detects attack at the real time. Along with this vulnerability of mobile ad hoc network routing protocols were presented. Particularly some attacks against the routing and some threats to wireless ad hoc networks were discussed.
8	Jeyanthi Hall (2007)	This paper introduced an anomaly-based intrusion detection technique, using radio frequency fingerprinting (RFF) and Hotel ling's T 2, a multivariate statistical process control technique, for detecting this attack.
9	Magnus Almgren,	This paper introduced a way to use the alerts from many audit location to

	Ulf Lindqvist, and Erland Jonsson, (2008)	improve the accuracy of the intrusion detection system (IDS). A theoretical model was designed automatically for the reason about the alerts from the different sensors through concentrating on the web server attacks. It also provides a better understanding of possible attacks.
10	Anna Sperotto and Aiko Pras (2010)	This paper introduced flow based approach for intrusion detection in wired network. Using flow data, DoS, Worm, Scan and Botnets were detected.
11	David L. Hancock (2011)	This paper extended flow based approach by using reputation. David designed multi agent IDS.

Table 2.1: Evolution of Intrusion Detection System

2.2.2 Wireless Intrusion Detection System

Wireless network is more complex than wired one. Both the technologies faces different situation while dealing with security. That's why wired IDS could not be used in wireless environments.

In order to protect our wireless network we must know [18]:

- Locations of all Access Point Planted in your network
- Set of action to be taken for unauthorized access point detected within your network
- Total users accessing your wireless network
- Unencrypted information read or exchanged by such users

For getting above things, we need Wireless Intrusion Detection System within our network.

2.2.3 IDS Terminology

Important terminology for IDSs are as follows [19]:

- Alarm/ Alert: A signal suggesting that a system has been or is being attacked.
- True Positive: The number of actual intrusion detected by the system.
- False Positive: An event signaling IDS to produce an alarm when no attack has taken place.
- False Negative: A failure of IDS to detect an actual attack.

- True Negative: When no attack has taken place and no alarm is raised.
- Detection Rate: True Positive divided by the total number of intrusion instances present in the test set.
- Noise: Data or interference that can trigger a false positive.
- Confidence value: A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack.
- Attacker or Intruder: An entity who tries to find a way to gain unauthorized access to information, inflict harm or engage in other malicious activities.
- Masquerader: A user who does not have the authority to a system, but tries to access the information as an authorized user. They are generally outside users.
- Misfeasor: They are commonly internals who misuse their powers
- Clandestine user: A user who acts as a supervisor and tries to use his privileges so as to avoid being captured.

2.3 Flow / IP Flow / NetFlow

Catching IP flow has numerous profits, so most of the manufacturers give their routers that support Flow Statistics e.g. CISCO routers, Huawei routers, TP-LINK routers etc. IP Flow is caught and saved in flow records which could be utilized for flow traffic characterization [7]. It likewise helps IDS for faster intrusion detection which is we are talking about in this paper.

The definition of IP flow is given by IPFIX (IP Flow Information Export) is

“A flow is defined as a set of IP packets passing through an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties”.

As per IPFIX documentation, a flow is recognized by parameter like source address, destination address, source port number, destination port number, and IP Protocols:

source_ip
destination_ip
source_port
destination_port
Protocol

Table 2.2: Flow Keys or Flow Parameter

Using above parameter any problem with network can be detected hence these parameter are called as Flow keys or common properties [20] as shown in table 2.2.

2.3.1 Architecture of IP Flow

A Metering Process is responsible for collecting packets at an Observation Points, filtering them out (optionally) and aggregating information about these packets. An Exporter sends this information to a Collector using the IPFIX protocol as shown in following figure 2.1[21].

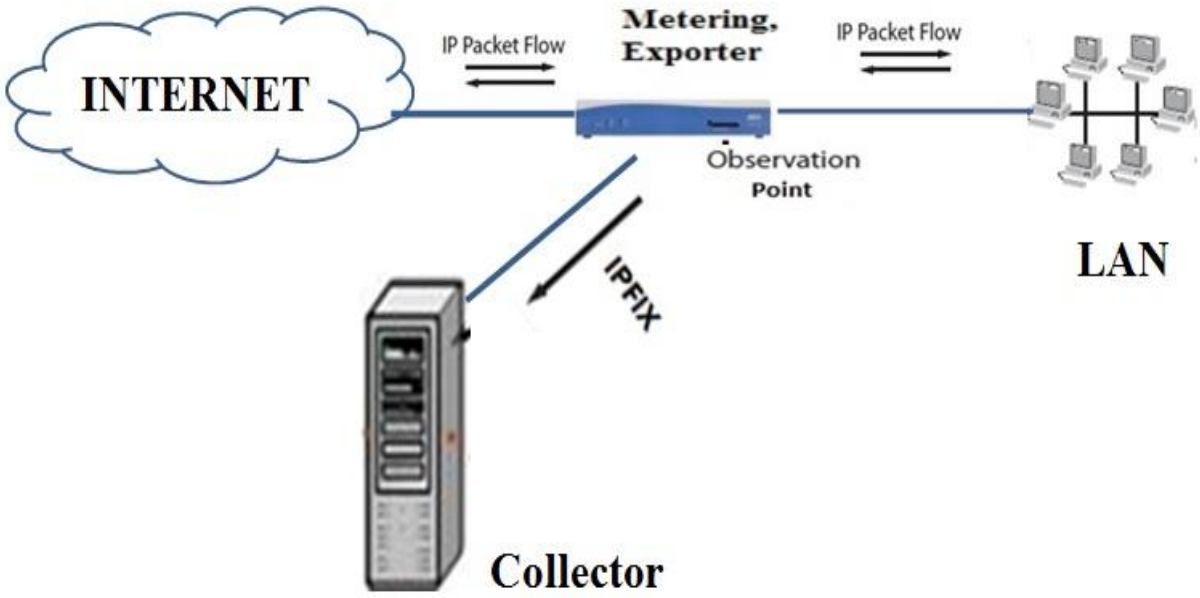


Figure 2.3: Architecture of IP Flow

2.3.2 Flow Based IDS

Flow offers aggregated view of network traffic by inspecting group of packets flowing in network. So drastically reduces amount of data need to compared. The flow monitoring process consists of two steps flow exporting and flow collection. After packet is captured by flow exporter it is given to flow collector. The information given from exporter to collector usually called as flow records [21]. It is duty of flow collector to get flow records from flow exporter and stored them in the form of suitable for analysis. Thus by aggregating packets of identical flow, we can inspect for abnormal traffic pattern observed in case of attacks [20].

In this case we are getting speed but questions is does the flow provide enough information i.e. reduction in information should not result in negligence of any single attack. Thus accuracy is in question, as we stated above speed and accuracy are the desirable feature of IDS. As flow is aggregated form of information it cannot provide accuracy like packet based inspection.

2.3.3 Comparisons of Flow and Packet Based IDS

Packet based IDS or Traditional IDS are no longer useful for today high speed network, flow based IDS can substitute packet based one. But they lack in accuracy. Following table 2.3 shows comparison of both approaches [6].

Flow Based Intrusion Detection	**Packet Based Intrusion Detection**
It uses data up to 4^{th} layer of OSI model, mainly network (IP) and transport layer (TCP/UDP)	It uses data up to application layer, as it requires both header and payload
Due to scarcity of data accuracy affected	As all data available here, gives good accuracy over flow based
This gives a reduced alert confidence and more false alarm	This gives a higher alert confidence and less false alarm
Flow based has to work on aggregated data, so more complex than packet based one	Packet based work on each packet, so simpler than flow based one.
NIDS has to wait till complete flow record given to it	Packet based approach has to wait for a single packet

Encrypted payload does not influence this NIDS	Encrypted payload affect this NIDS
It has to process low data. So low resource consumption	It has to process more data. So more resource consumption.
No privacy issue, as it does not deal with payload data	Work on full payload, so privacy issue is there.

Table 2.3: Comparison of Flow and Packet Based IDS

2.4 Network Attacks

The network associated with internet is always at risk, albeit whatever security you are providing. To secure your network from malicious activity is possible by reducing the network connectivity. In complex case completely disconnecting network but this approach is not practical on as we are more dependent on internet nowadays. The attack which can be detected using network data or traffic statics can be called as network level attack.

The Network Attack can be categorized in three classes [7]:

- Attack that devour network resources, denying their utilization for genuine purposes.
- Strike that invade system, permitting attacker's unapproved access to network assets, including delicate information, information storage, privileged associations with different system, and network connectivity.
- Unapproved vulnerability scan, giving attackers essential surveillance in planning network penetrations..

Generally data belonging to Transport (TCP) and Network (IP) layer termed as network data. By using this following type of attack can be detected.

2.4.1 Denial of Service (DOS) Attack

A denial of service attack is a strategy defined to prevent valid traffic from using the target of the attack. The main target of DOS attack are Web Server, Application Server and Communication links [23]**.** Brute force attack or flood attack is a type of DoS attack. In case of brute force attack, attackers send a large volume of traffic to victim system. The victim system bandwidth is congested by such IP traffic. Eventually slowing down or crashing victim system and thus

preventing legitimate user from accessing victim system [24]. This attack can be performed using User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) packets.

2.4.2 Vulnerability Scan

A vulnerability scan is an attack which sends a request to a target system with intend of finding range of available port on that system. After choosing one of the active ports, vulnerability of the service will be then exploited [25]. The result of vulnerability scan on a port is generally summed up into one of three classes:

- Open: A service is listening on the port.
- Closed: The connection to the port is denied.
- Filtered: There is no reply from the host.

2.4.3 Worm

Early detection of worm is of vital importance. Within a brief period of time worms might spread over the entire Internet a small span of time, making the normal recognition time critical. A typical approach to catch worms is to place sensors in a network for analyzing the network traffic [26].

On the basis of vector of propagation Worms are classified. The main categories include:

- Internet scanning worms
- Web worms
- Email worms
- P2P worms
- Mobile Worms

Over the decades, worm scholars have brought numerous bright procedures to worm design. Some of which are listed in table 2.4 [27].

Worm Name	**Year**	**Vector of Propagation**	**Claim to Fame**
Code Red	2001	Internet	First worm that spread rapidly causing billions of dollar in damage

Nimda	2001	Email, HTTP, File sharing	First worm to use multiple vector of propagation
Slammer	2003	Internet	First internet scanning worm to spread through UDP only. Much faster.
Sobig	2003	Email	First worm to update itself at specific point in time
Witty	2004	Internet	First worm which carry destructive payload
Cabir	2004	Bluetooth	First worm to target cell phones
Santy	2005	Web	First warm to use web search engine to locate new target
Commwar	2005	Bluetooth, MMS	First worm using two vector of propagation
Samy	2005	Web	Within 24 hours, affected ! million user`s using MYSpace- a social networking site
Storm	2007	Email, USB driver	Multiple infection stages
Conficker	2009	USB drives, network files system, Scan	Dynamically generated URLs for code update
Stuxnet	2010	USB drives, link files	Designed to attack PLC (Programmable Logic Controller).
W32netsky	2010	Email, Drives	Send a mail to address find during drives scanning
Camouflaging	2011	Internet	(C-worm) Capable of manipulating its scan traffic volume over the time intelligently.
Flame	2012	LAN, USB	Attack computer running windows operating system.

Table 2.4: Selected Worm with their innovative features

2.5 Challenges Discovered

From its inception, much of work has been done on Intrusion Detection System. But still it has some limitations because of much reason. Some of which are [1] [3] [5]:

- Dealing with increased network speed
- Handling ever increasing network traffic
- Limited accuracy of Flow Based Approach
- Slow packet based approach
- Increasing alert confidence
- Reducing resource consumption
- Detection Rough access point in wireless network
- Detection illegal user accessing your wireless network

Summary

For designing a security system for a network, understanding of network model and network monitoring is important. In case of wireless network, wired IDS is not much useful. Also to speed up wireless network monitoring, a group of packet having common properties (Flow) should be analyzed at a time. With such approach attacks like DoS, Scan and Worm can be detected.

3. Problem Definition

3.1 Motivation

The introduction of technology like 3G, 4G in recent years prepared a way to a new, high speed internet. This technology caused expansion in bandwidth of communication as shown in figure 3.1. So handling a large traffic with high speed is no easier with existing security system.

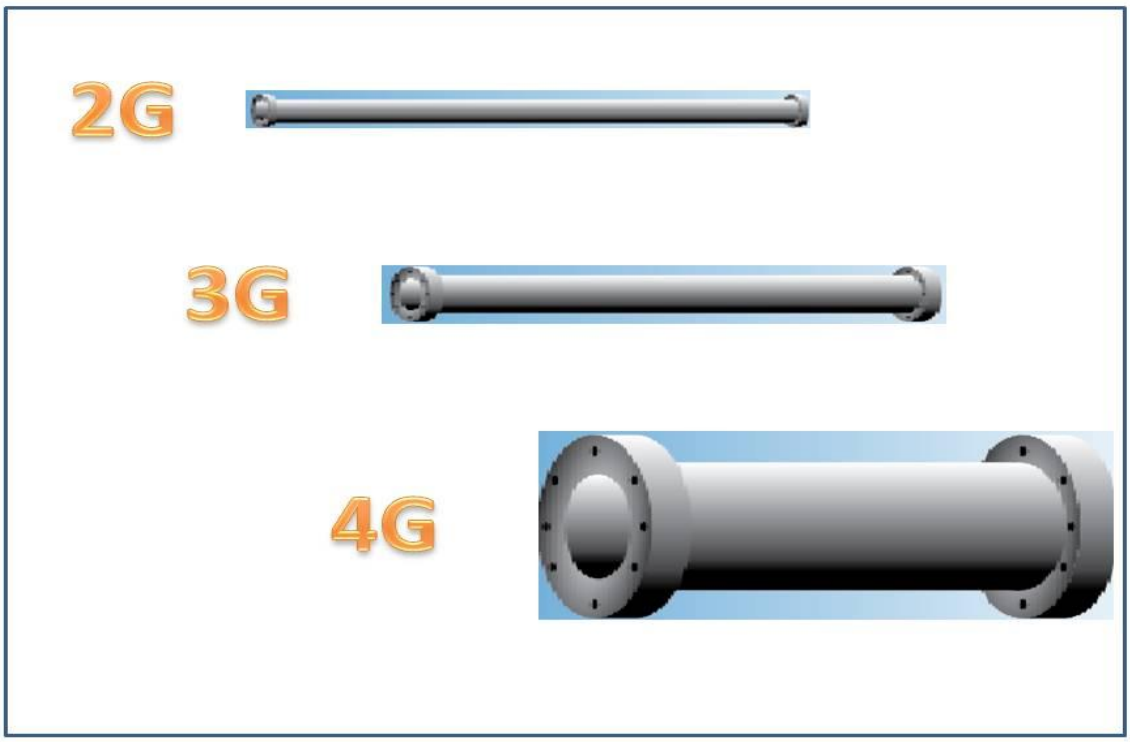


Figure 3.1: Bandwidth increasing with new technology

Nowadays we rely on upon the Internet in our everyday life for basic things, for example, checking messages or emails, along with this also for overseeing private and budgetary data. On the other hand, entrusting such data to the Internet additionally implies that the system has ended up a charming spot for attackers. Attacks are getting more and more profitable every day. To this risk, the network security group has replied with an expanded enthusiasm toward intrusion identification.

3.2 Scope of Project

This project is designed for Infrastructure based wireless network (shown in figure 2.1). It can be used in high speed heavy traffic wireless network. In first stage, it will focus on flow level attack detection. This attack will be detected by using flow keys (table 2.2) i.e. source IP address, destination IP address, source port number, destination port number and protocol used. So accuracy won't be like traditional packet based IDS, but attack like DoS, worm scan can be detected at high speed in bulk traffic also. So traffic for information sensitive nodes like web server, file server etc. can be passed through second stage, packet based approach.

3.3 Objectives

1. To design two stages monitoring NIDS for Wireless network, first stage will be flow based intrusion detection. Second stage is packet based intrusion detection for important node in network.
2. Perform various attacks like DoS, vulnerability scan and worm (Experimentation).
3. Detection of above attack successfully by system (Evolution).

Summary

Technologies like 3G and 4G are increased bandwidth of network. Application of network in day to day life is also increased so the traffic. For protecting valuable data and protecting network devices in such condition there is need of faster intrusion detection system.

4. System Design

The system is designed to work in two stages. At the first stage, flow based approaches can be used to detect certain attacks. At the second stage, packet inspection can be used additionally to protect critical server or selected system.

4.1 Flow Based Stage

Flow offers aggregated view of network traffic by inspecting group of packets flowing in network. So drastically reduces amount of data need to compared. The flow monitoring process consists of two steps flow exporting and flow collection. After packet is captured by flow exporter it is given to flow collector. The information given from exporter to collector usually called as flow records (explained in section 2.3.1). It is duty of flow collector to get flow records from flow exporter and stored them in the form of suitable for analysis. Thus by aggregating packets of identical flow, we can inspect for abnormal traffic pattern observed in case of attacks, as shown in figure 4.1.

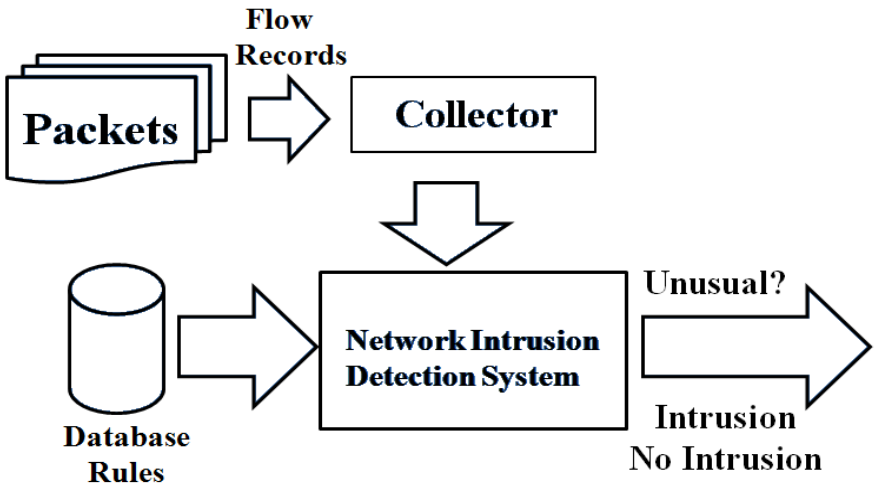


Figure 4.1: Flow Based Detection

4.2 Packet Based Stage

In the second stage, traditional packet based approach is used for information sensitive server of the system. The main advantage of packet-based approach is that all common kinds of known attacks and intrusions practically can be detected if the data source deliver entire network packet for analysis.

4.3 Architecture

In this system, one node (admin) is put in promiscuous mode, which sniffs all the data (packets) in the air as shown in figure 4.2. In promiscuous mode, there is no IP address associated with the NIC card, so all network traffic will be routed to it. The admin is also provided with WIDS setup and also having flow record to place captured packets. After capturing packets in the air, the packets will be placed in their corresponding flow records; if flow record is not present for given IP then new one is created. Now from this flow records are analyzed to extract information out of it i.e. flow keys. This information is compared with flow based dataset, to detect intrusion. If for a packet in flow any suspicious activities are discovered and is destined for information sensitive node (IS node), then packet based approach can be used to detect intrusion accurately. For packet based IDS, the captured packets are stored .pcap (Packet Capture Format used to store data of network packets).

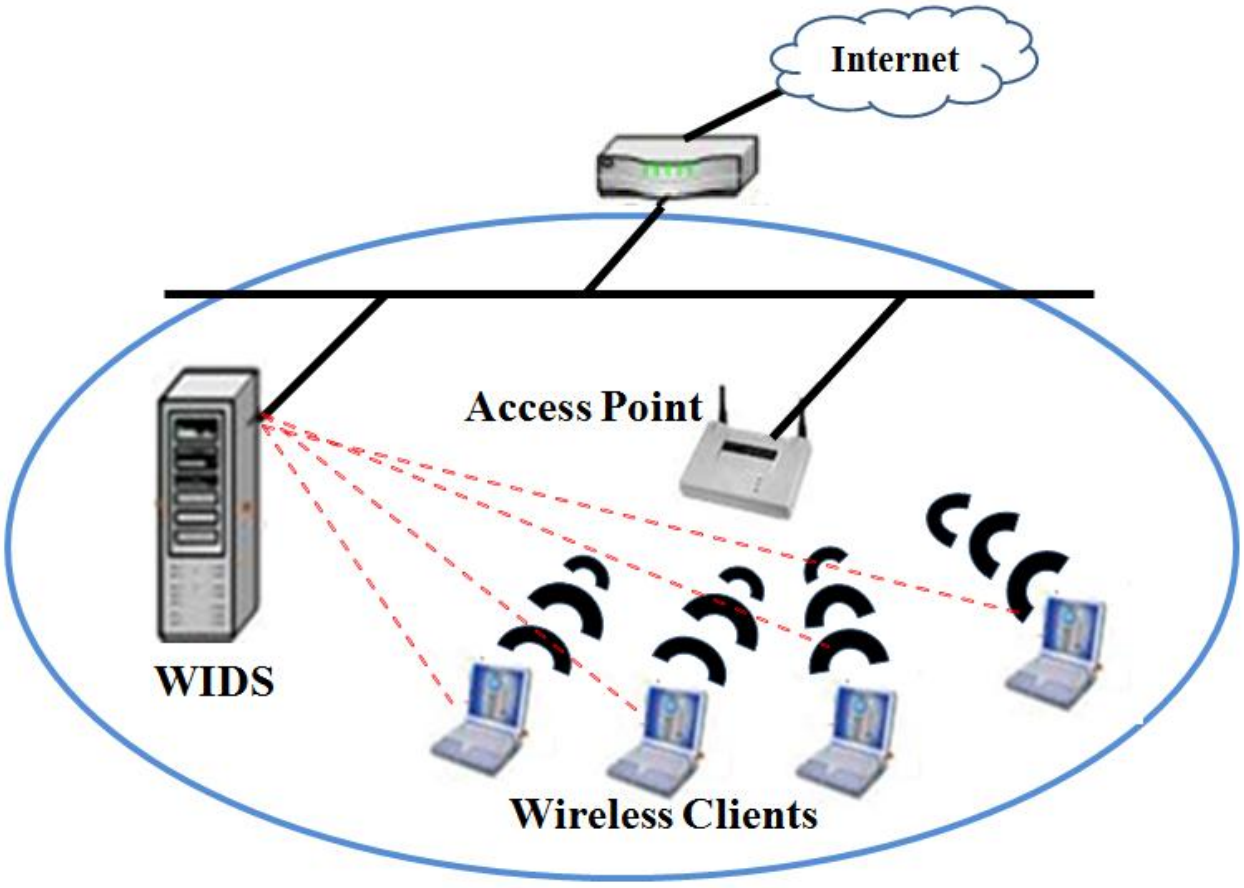


Figure 4.2: System Prototype

4.4 Flowchart

The following figure 4.3, depict the algorithm for the proposed system. Each incoming packet is first checked with existing flow records. If flow record for that packet is not present new flow record is created and packets are placed in that flow. These flow records are then checked for flow based attack pattern. If it contain IP address of any Information Sensitive (IS) node or any suspicious flow it can be given to packet based IDS.

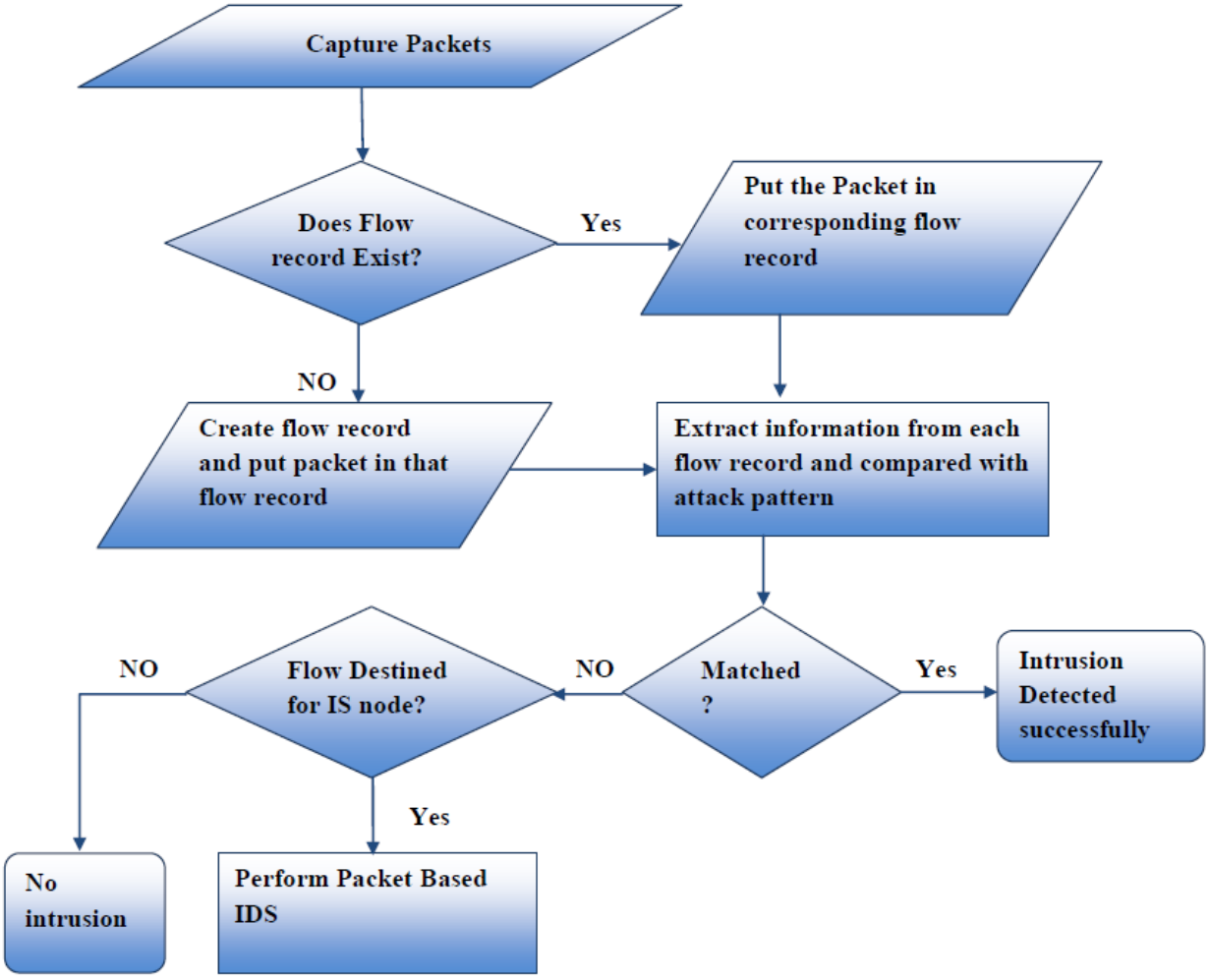


Figure 4.3: Flowchart for the Proposed System

Summary:

With the advancement of network technology, along with increased speed network are becoming very bulky.To deal with such higher speed bulk traffic, flow based attack detection can be used for faster attack detection.For increasing accuracy of flow based approach, it can be backed up by packet based approach. The working of the proposed system is explained by the above flowchart.

5. Experimentations and Results

5.1 Detecting Unauthorized AP and Malicious User

In case of wireless network, generally attacks are performed using unauthorized access point and malicious user. So detection of such major source of attack is very much basic thing, to secure your network. For detection of such access point is done by capturing beacon frames by sniffer. The other possible source of attack is illegal user within your network. So detection of such user is also important. Such user can be detected by just sniffing packets from such user`s system. Figure 5.1 shows detection of unauthorized AP and malicious user detection by our system (underlined with red color).

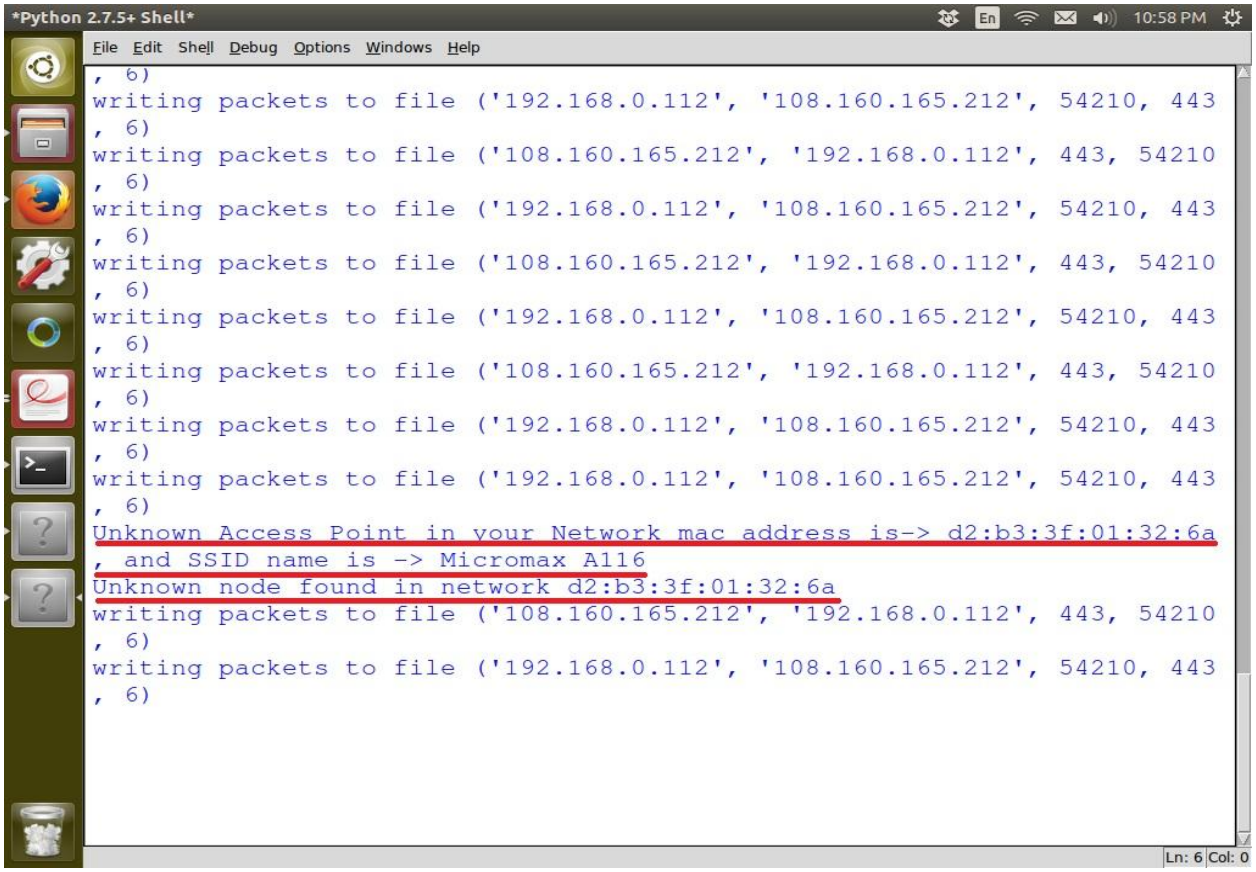


Figure 5.1: Detection of Unauthorized AP and Malicious User

5.2 Flow Based Attack

Flow based attack are those attacks that can be detected using flow keys or flow parameters. This include both IP address and Port Number and protocol (discussed in 2.3), it can also use number of packets in each flows, size of each packets etc.

5.2.1 Denial of Service (DoS)

A DoS attack is a strategy defined to prevent valid traffic from using the target of the attack. The main targets of DoS attack are Web Server, Application Server and Communication links. There are various forms of this attack, but intention of all form is one i.e. to overwork the target.

One of DoS attack is SYN Flooding attack. This attack is performed by misuse of "three way handshake" technique of TCP protocol. In normal case for establishing a connection using TCP, a client needs to send TCP SYN packet first to server. Then server replies this with SYN ACK packet. Again, the client sends ACK packet (or RST to reset connection). Thus connection is established. But while performing attack, the client i.e. attacker does not send last ACK or RST packet. The target remains in SYN_RECV state waiting for reply from client. Thus the connection is half open. Attacker creates number of such half open connection, busing target in wait condition. Thus legitimate client could not communicate with that server. The attack scenario is depicted in figure 5.2.

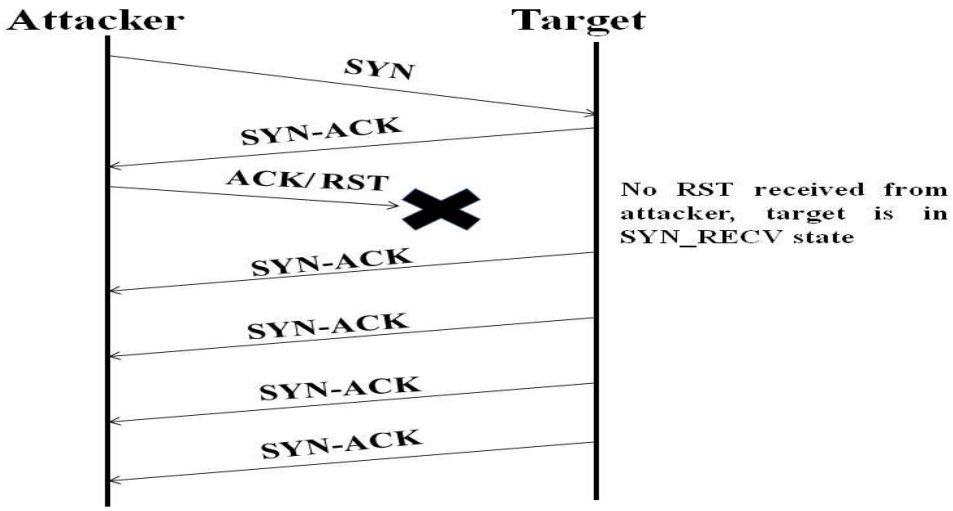


Figure 5.2: TCP-SYN Flooding DoS Attack Scenario

Using flow based approach, if we monitor each IP address attempts we can prevent this attack. Each IP address is allowed to send limited number of TCP SYN packets. If up to crossing the limit, that IP does not send ACK or RST packet then block that IP address. Figure 5.3 and 5.4 show, attacker attacking the target and result after blocking such attacker. In the figures SA stands for SYN ACK and RA stand for RST ACK.

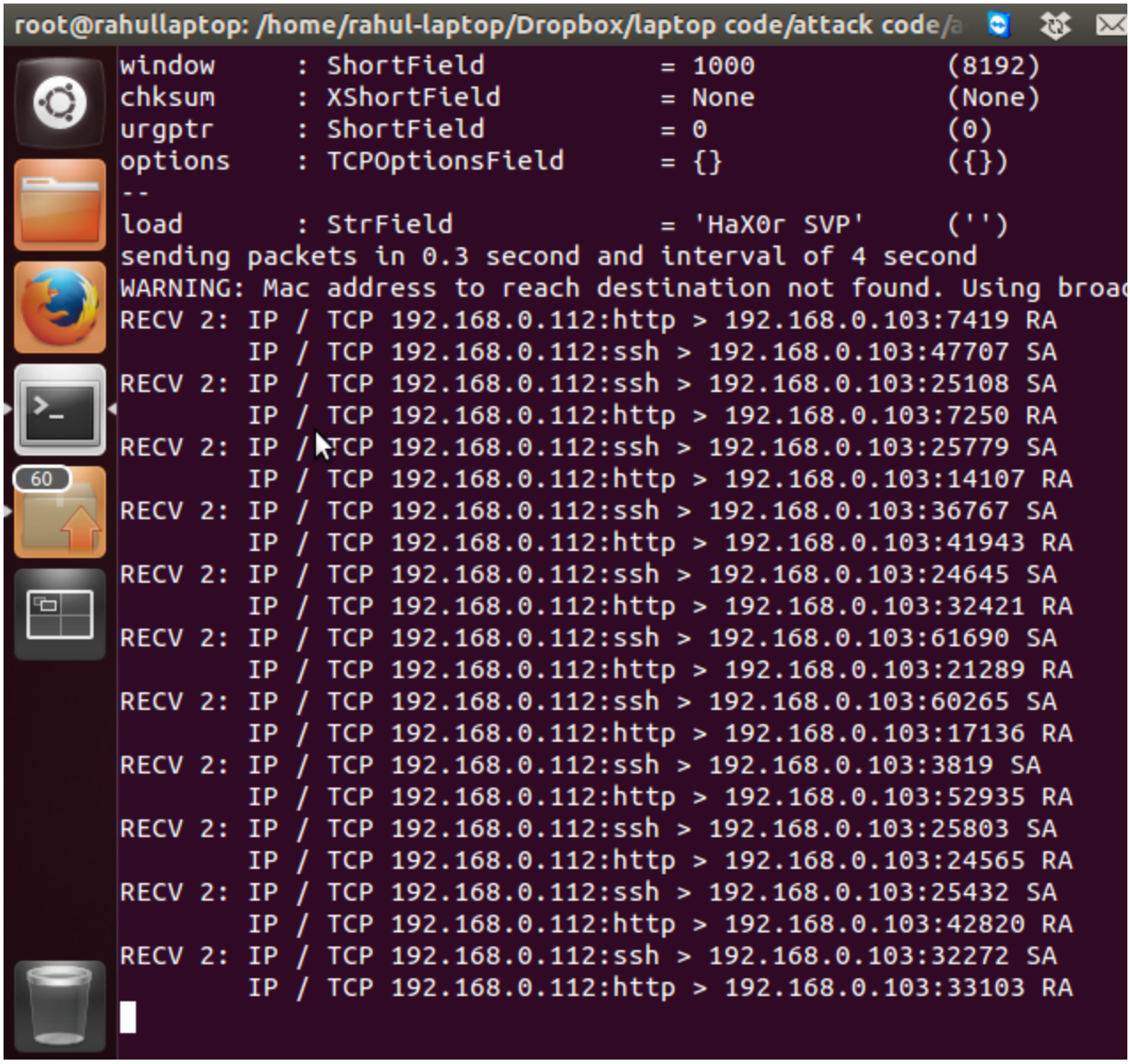


Figure 5.3: Attacker attacking Target

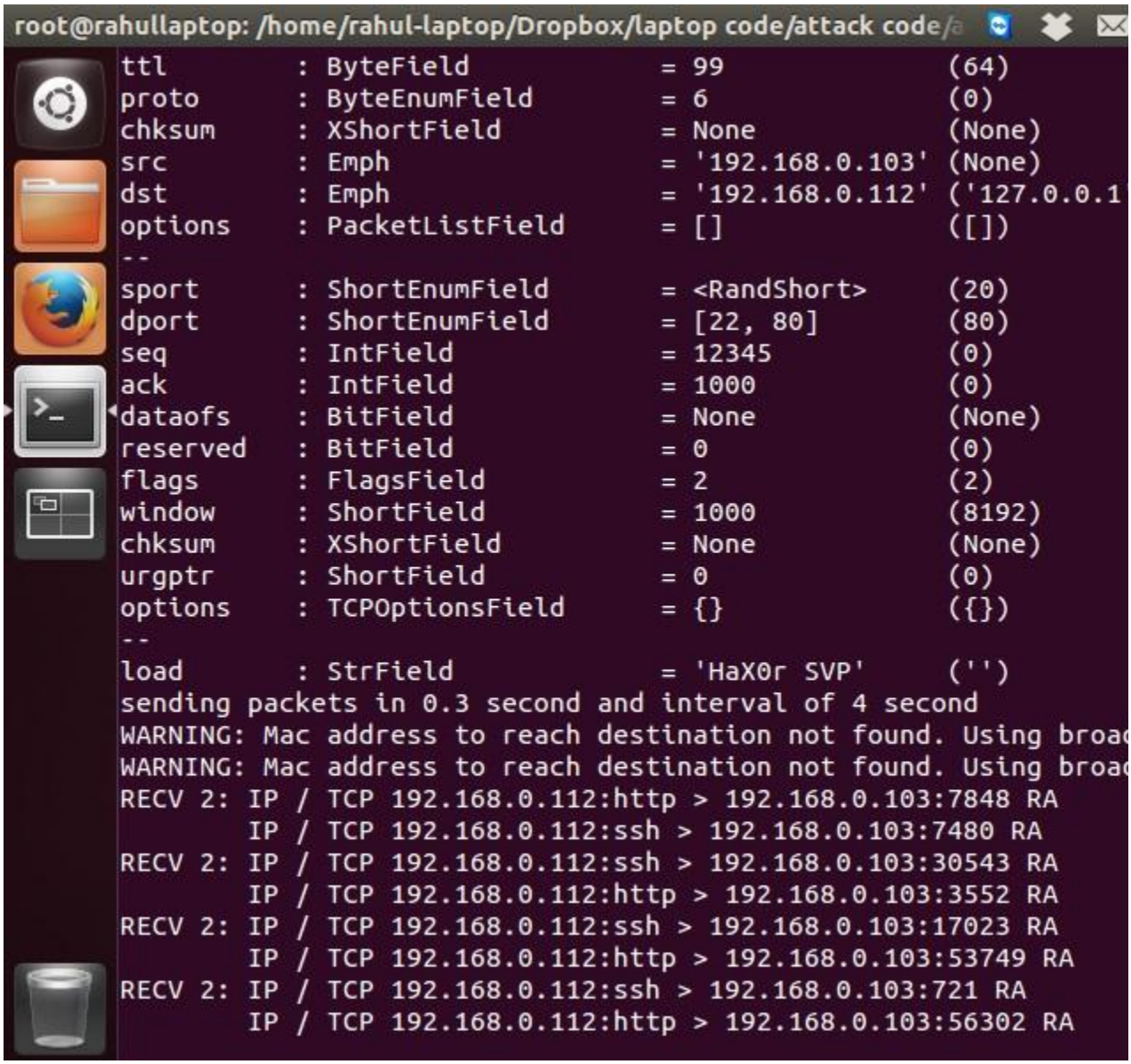


Figure 5.4: Result after blocking attacker

5.2.2 Vulnerability Scan

In case of vulnerability scan, the attacker searches for entry point i.e. available port on network to launch the attack. There are various forms for this attack. But they mainly classified as vertical scan and horizontal scan. For vertical scan, attacker searches several destination ports on a single system in the network. A horizontal scan targets only one port across several systems in the network. For this, attacker is aware of particular vulnerability and looking for susceptible machines.

Such scan attack is detected by our system using table method shown in table 5.1, where C0, C1 etc. represent count associated with the triplet (SIP, DIP and DPort).Using sniffer, we are keeping watch on every communication happening in the network and recording all such information in the table. In normal communication, any clients ask for very limited number of ports on a system. But in case of vertical attack, attacker generally attacker has to ask check many ports. So by setting the limit we can find out such request.

DPort/IP	**Port 1**	**Port 2**	**Port 3**	**Port 4**	**…….**	**Port N**
SIP,DIP	C1	C2	C0	C0	C6	C2
SIP,DIP	C3	C0	C1	C4	C4	C0
SIP,DIP	C0	C3	C1	C0	C1	C2

Table 5.1: Table for Counting Communications pattern

Same case is with horizontal scan, any normal communication needs limited number of systems with same port. But for performing horizontal scan, attacker has to check most of the system. So by using above approach we can detect horizontal attack also. We have checked this approach with standard flow based dataset i.e. "Labeled Flow Based Dataset for Intrusion Detection" by Anna Sperotto and colleague [29]. The accuracy came for the horizontal approach is 70 percent, shown in table 5.2.

Total Number of Records	Nor of Horizontal Attack	Nor of attack Detected
500000	10	7

Table 5.2: Accuracy of Table Horizontal scan Detection

5.2.3 Worm

A worm is actually a standalone computer program. It spreads through computer network to exploits network resources like bandwidth and also can cause any hardware malfunctioning. Unlike viruses worm does not require any existing program to attach itself.

As already said, a worm is standalone computer program. Means after its execution it is going to show same behavior every time. So by characterizing worm, its detection can be possible. To show this, for our system, we take Win32/Netsky.c. It is a mass mailing worm which utilize its own SMTP engine to send itself to the email addresses it discovers when checking hard drives

and mapped drives. The characteristic of this worm is that it sends packets to some hard coded IP address using destination port 53 (DNS) and UDP protocol. So we can check all out going packets from our network, if any packet is destined for that hard coded IP address then that worm could detected. By looking at corresponding source IP address, the infected system within network can be easily find out. Following figure 5.5 shows this

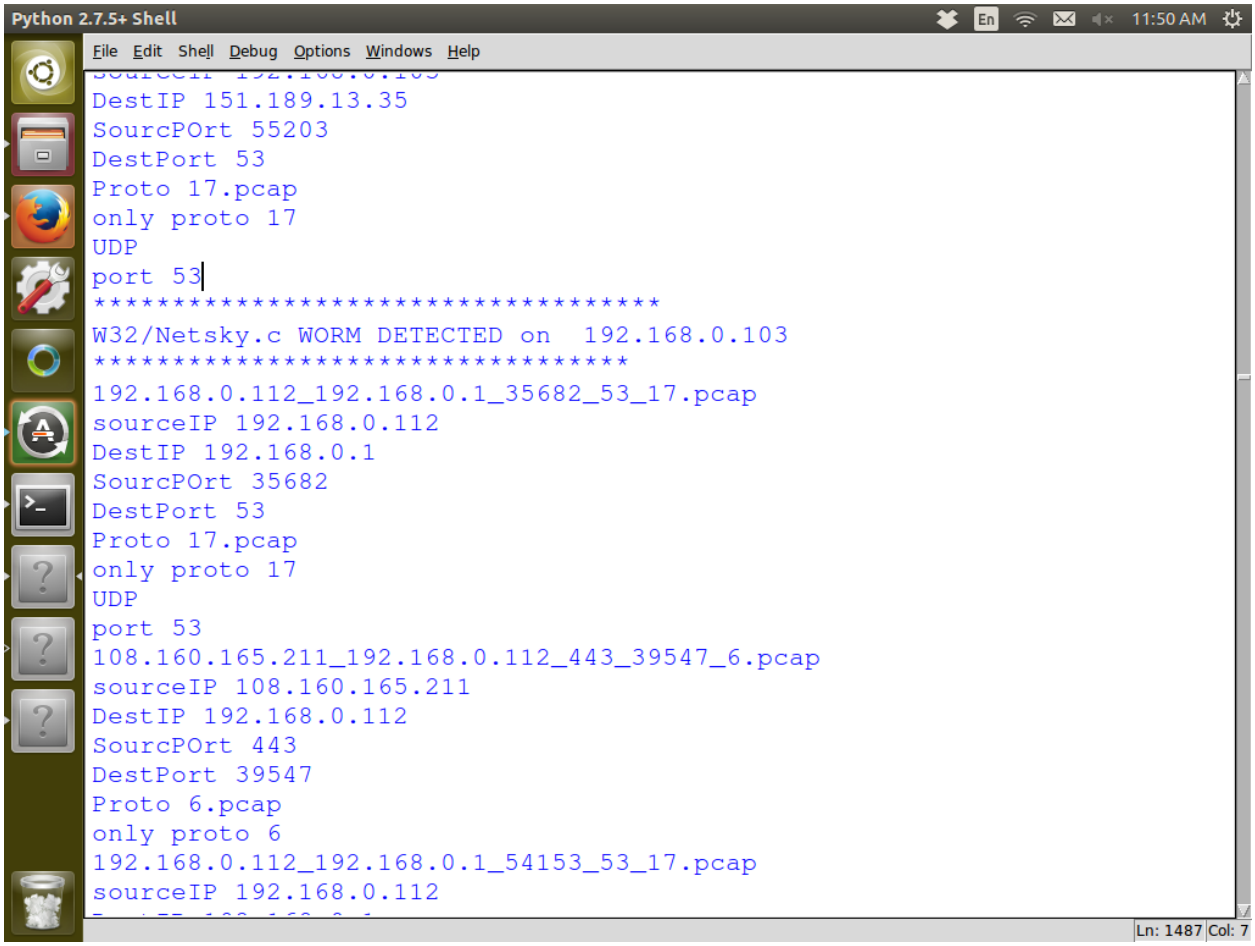


Figure 5.5: Detection of W32/Netsky.c on 192.168.0.103

Summary

For any wireless security system detecting unauthorized AP and malicious user very much important. The proposed system detecting flow based attack like DoS, Vulnerability Scan and Worm. It detects DoS attack by counting request coming from each destination IP address. For detection of scan it uses triplet of SIP, DIP and DPort. Worm detection is possible by using its characterization.

Conclusions and Future Scope

Conclusions

Nowadays wireless network are very ubiquitous, places like coffee shops, airports, educational institutes, hotel are the common one. All this is because of the research happening in the network field. With the technological advancement the speed is also increasing. Most of devices like Xerox machine, printer, mobile phone coming with Wi-Fi technology. The use of network is not limited to only file transfer; nowadays it has been used for commercial activities also. So securing such network is very much important, that to be in a faster way.

We have presented flow based approach for Wireless network. In this system, we are grouping packets on the basis of flow only which avoids the need of payload checking of each and every packet. Even it will not be possible with such high speed network with bulky traffic. Some packets may be dropped at monitoring point of network. That is not acceptable for security point of view. So it is good to focus on group of packet having same properties.

With this approach we have detected attack like Denial of Service (DoS), Vulnerability Scan and Worm like attack. All these attacks are detected using flow keys. There is no need to check entire packets of all the system in a network. It is done only for information sensitive node like file server. All the communication intended for such node has to go through both approaches. Means first it is checked for flow based attack detection and then for packet based attack detection. This is good approach to deal with speedy and bulky network traffic in wireless network.

Future Scope

Day by day the awareness about internet application and its importance is increasing, so the internet users. That's why every institute, companies and hotels providing internet facility to their student, clients and customers respectively. As in case of wireless network there is no need of physical cabling like things. Also it is easy to maintain, connect and flexible. The devices like PDA, Mobiles, Xerox and printer also coming with the Wi-Fi facility. It is very much clear that in future wireless technology will be more preferable than wired one.

So securing such network and devices will also important. Though presently, our system needed knowledge about the nature of traffic for underlying network. But with use of machine learning approaches it can be tune for automatic detection of intrusion. Also using such approach it can deal with IP spoofing like things, with the help of packet based approach in back end. For securing large local area network having regular clients, reputation like concept can be used for faster and accurate intrusion detection.

Publications

[1] Rahul B. Adhao, Avinash R. Kshirsagar, Dr. V. K. Pachghare, "NIDS Designed Using Two Stages Monitoring", International Journal of Computer Science and Information Technology (IJCSIT) , Vol-5 (1), pp 256-259 (2014).

[2] Rahul B. Adhao, Avinash R. Kshirsagar, Dr. V. K. Pachghare, "Reputation Based Fast Intrusion Detection", International Conference on Information Technology, Computer Science & Management (ICITCSM), 10th May Goa. (Best Paper Award)

Bibliography

[1] Internet and Mobile Association of India (IAMAI), "Internet in India 2013", Inter-Research Journal (Nov. 2013).

[2] Dr. V K Pachghare, "Cryptography and Information Security", PHI publication.

[3] Uday Banerjee, "Wireless Security: Considerations, Intrusion Detection System, Tools and More", SANS Conference 2004, Virginia Beach (2004).

[4] International Telecommunications Union, "IctvStatistics", http://www.itu.in/ITU-D/icteye/ (Jan 2010).

[5] Anna Sperotto and Aiko Pras, "Flow Based Intrusion Detection System", 12th IFIP/IEEE 2011: Dissertation Digest (2011).

[6] Hashem Mohammed Alaidaros, Massudi Mahmuddin, Ali Al Mazari, "From Packet-Based Towards Hybrid Packet-based and Flow-based Monitoring for efficient Intrusion Detection: An Overview", Second International Conference on Communication and Information Technology (2012).

[7] Anna Sperotto, Georor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller, " An Overview of IP Flow- Based Intrusion Detection", IEEE communication survey & Tutorial, Vol. 12, No. 3 (2010).

[8] Bernard Menezes, "Network Security and Cryptography", Cengage Learning.

[9] Scott Hogg and Eric Vyncke, "IPv6 Security", Cisco Press (2008).

[10] F. Sabahi and A. Movaghar, "Intrusion Detection: Survey", the Third International Conference on System and Network Communications (2008).

[11] Simmonds A, Sandilands, P van Ekert, "An Ontology for Network Security Attacks", Lecture Notes in Computer Science, pp. 317-323 (2004).

[12] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28 (1998).

[13] D. Denning, "An Intrusion Detection Model," IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222-232 (1987).

[14] Kurose, J. and K. Ross. Computer Networking: A top-down approach. Pearson Addison-Wesley, fifth edition (2009).

[15] D. Firesmith, “Common Concepts Underlying Safety, Security, and Survivability Engineering,” Carnegie Mellon Software Engineering Institute, Technical Report (2003).

[16] Rahul B Adhao, Avinash R Kshirsagar, Dr. V K Pachghare “ NIDS Design using Two Stage Monitoring” , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , pp. 256-259 (2014).

[17] “Intrusion Detection Systems; Definition, Need & Challenges”, SANS Institute InfoSec Reading Room, GIAC Security Essentials (2001).

[18] Ken Hutchison, “Wireless Intrusion Detection Systems”, SANS Institute InfoSec Reading Room, GIAC Security Essentials, London (2004).

[19] Whiteman, Michael E. and Herber J. Mattord, “Principles of Information Security”, Course Technology (2011).

[20] Myung S., Hunk K., Seung C., James H. “A Flow Based Method for Abnormal Network Traffic Detection”, IEEE/IFIP Network Operations and Management Symposium, pp. 599-612 (2004).

[21] G. Sadasivan, N. Brownlee, B. Claise, “Network Working Group” RFC 5470, http://www.ietf.org/rfc/rfc5470.txt (2009).

[22] Singh, Jatinder. "Study of the enhancements in intrusion detection techniques for wireless local area network (WLAN)", Punjab University college of Engineering (2012).

[23] Alfred Basta, Wolf Halton, “Computer Security: Concept, Issues, and Implementation”, Cengage Learning publication (2007).

[24] Specht, Ruby B., Stephen M. and Lee. “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". Proceedings of the 17th In- ternational Conference on Parallel and Distributed Computing Systems, pp. 543 -550 (2004).

[25] Shirey, R., “Internet Security Glossary, Version 2" (2007).

[26] Chen, Z., L. Gao, and K. Kwiat, “Modeling the spread of active worms", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3 (2003).

[27] N. Weaver, V. Paxson, S. Staniford and R Cunningham, “A Taxonomy of Computer Worms”, ACM Workshop Rapid Mallcode, pp. 11-18 (2010).

[28] Jochen Schiller, "Mobile Communication", Second Edition, Pearson Education publication (2006).

[29] A. Sperotto, R. Sadre, D. F. Van Vliet and A. Pras, "Labeled Data Set For Flow Based Intrusion Detection", Proceeding of the 9th IEEE International Workshop on IP operation and Management Venice Italy, pp. 39-50 (2009).