INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

A novel prototype to secure network using malware detection framework against malware attack in wireless network

G. Jagadish
gjagadish.cse@anits.edu.in
Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh

L. Jaswanth
l.jaswanth0@gmail.com
Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh

K. Sowjanya
sowjanyakundu98@gmail.com
Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh

P. Sri Harsha
sriharsha.potnuru1070@gmail.com
Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh

M. Nikhil Kumar
nikhilmeruva19@gmail.com
Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh

ABSTRACT

A new and novel proposed algorithm based on malware detection has been used that overcomes the disadvantages of the existing algorithms and helps to eliminate viruses and worms from entrusted environment. In the wireless networks suffers from various spyware programs that prevents access to legitimate users who obtains services from target web server. In our proposed prototype helps to authenticate the sender to make the dynamic rule set to avoid the formations of unavailable networks which any user who obtain web services. In our proposal architecture diagnose malware whether malware based data has been really being sent to the valid user or is it being morphed by the attacker in the middle. The proposed algorithm has been tested against various existing algorithms to study how effectively the algorithm is working, and how effectively it is overcoming the drawbacks of the present malware detection algorithms. The algorithm is projected to serve the purpose of prevention of being used malware based programs to drop it by the user and also to identify that the non-infectious message is reaching only to the valid user.

Keywords— *Virus and worms, Malware detection framework, Client, server, Wireless LAN*

1. INTRODUCTION

Due to the increase in digitalization all over the world, security became one of the main issues to be considered. Now, the question arises that how to secure these computers. If a malicious content enters any of the systems in the network it may cause damage to the entire network and it will definitely lead to malfunction of the system. Within no time the entire network goes out of control from the users and gets destroyed thus losing all confidential data Because of this the efficiency of the system goes down. So much is the importance of establishing a security policy for the systems.

The main goal of the paper is that it should detect the worms and virus all they exist in any system in the network and immediately stop them from spreading all through the network. In this paper, we suggested that the required inputs are the existence of any worm or transfer of any infectious packets and the desired outputs are detected and deleted. If an infectious packet is found to be transferring over the wireless network, it will be discarded.

1.1 Malware

The incidence of security threats has increased dramatically in a few decades due to the direct connection of computers to the Internet. Malware is one of the important examples of smart design programs that can cause security threats and can be defined as programs, which replicate themselves and exploit various types of vulnerabilities in the network hosts. These characteristics mean that worms can spread within minutes to a large number of computers, leading to network congestion ranging from file detection to denial of system services.

The most effective method of detecting malware is by signature-based detection, which is also known as content-based filtering. This signature can be used to inform researchers about the particular characteristics of the malware, for containment of the malware infected files. This signature can be generated by use of either exploit-based signatures, which illustrate the characteristics of an individual or a number of exploits, or vulnerability-based signatures, which illustrate the properties of individual vulnerability along with detection of all possible exploits employing this vulnerability. However, Brumley et al. stated that the vulnerability-based signature is generally more efficient in making signatures if only the vulnerability-based is disclosed. On the other hand, Arce argued that both types of signatures have equal abilities for the detection of worms in various applications, especially in Intrusion Detection Systems (IDSs). If malicious network traffic is detected by IDSs, an alarm may be raised. An IDS mainly functions by detecting threats that obstruct the remainder of the offending traffic and then preventing future attempts from succeeding.

This paper investigates the characteristics of Malware and then explains the most common forms of pattern-based detection, such as Autograph, Polygraph and Simplified Regular Expression (SRE). In addition, we investigate the enhanced algorithm in terms of accuracy only. Autograph is the earliest system, which is used to automatically generate a signature for a single string based on matches with this string. Meanwhile, Polygraph is a token-based system that chooses a set of tokens which have a high exposure to the low false positive and the suspicious pool reaction to the ordinary traffic pool.

The SRE uses other automatic approaches, along with multiple sequence alignment to discover polymorphic worm signatures by utilizing the real polymorphic worm application level (as samples) and evaluating the accuracy of the signature arising from this approach.

1.1.1 Polymorphic Malware: Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, Trojans, or key loggers. Polymorphic techniques involve frequently changing identifiable characteristics like file names and types or encryption keys to make the malware unrecognizable to many detection techniques.

For example, a polymorphic virus will continue to spread and infect devices even if it's signature changes to avoid detection. By changing characteristics to generate a new signature, signature-based detection solutions will not recognize the file as malicious. Even if the new signature is identified and added to antivirus solutions' signature database, polymorphic malware can continue to change signatures and carry out attacks without being detected.

1.1.2 Storm Worm Email: The infamous spam email sent in 2007 with the subject "230 dead as storm batters Europe" was, at one point, responsible for as much as 8% of all global malware infections. When the message's attachment is opened, the malware installs wincom32 service and a trojan onto the recipient's computer, transforming it into a bot. One of the reasons the storm worm was so hard to detect with traditional antivirus software was the malicious code used morphed every 30 minutes or so.

1.1.3 Crypto Wall Ransomware: Crypto Wall is a polymorphic ransomware strain that encrypts files on the victim's computer and demands a ransom payment for their decryption. The polymorphic builder used in Crypto wall is used to develop what is essentially a new variant for every potential victim.

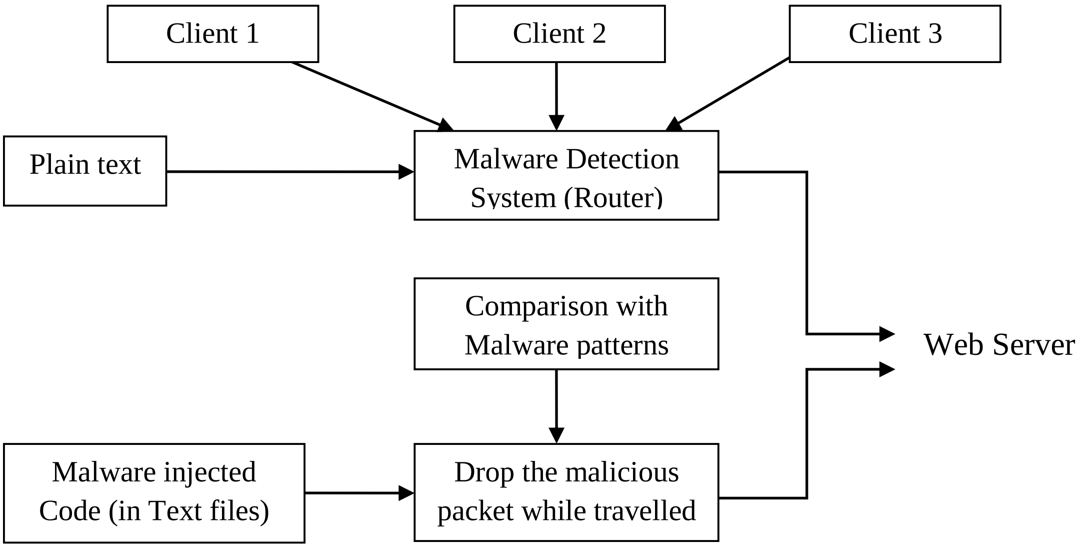
Client 1
Client 2
Client 3
Plain text
Malware Detection System (Router)
Comparison with Malware patterns
Web Server
Malware injected Code (in Text files)
Drop the malicious packet while travelled

Fig. 1: Malware detection system architecture

1.2 Related work

The main goal of the paper is that it should detect the worms or any malicious information if at all they exist in any system in the network and immediately stop them from spreading all through the network. The existing system ensures the detection of the malware in the network but at a great cost of discarding the entire network or removing of the particularly affected system using SNORT engine. Hence a new technique has been proposed to check the effect at a good level by discarding of the malicious traffic at the router itself using Java Swings. As most of the systems now being connected are through Wireless LAN, network traffic analysis plays a major role to encounter such deadly attacks.

2. LITERATURE SURVEY

2.1 Introduction to Malware detection approaches

Clients, when connected in a Local Area Network, are always prone to get affected by the dangerous worms and other malicious data. This is considered to be a very serious issue. Hence in our newly designed system, we maintain a database of all the worms existing today and if malware infected traffic enters into the network, the malware detection technique employed at the router identifies it and eliminate the data immediately. This means that the malware attack cannot make a system vulnerable to viruses and worms. Malicious codes (malware) – viruses, worms, and Trojan horses and so on - are one of the most destructive pieces of software that can attack a computer or network. This research mostly concentrates on viruses, worms and their behaviour.

2.1.1 Viruses: A computer virus is a program that performs unauthorized actions, without the knowledge of users. A program infected by a virus must meet two criteria:

- It must execute itself when the infected program is executed.
- It must often place its code in the path

2.1.2 Malware (Malicious software): A generic term increasingly being used to describe any form of malicious software like viruses, worms, Trojan horses, rootkits, spyware, malicious mobile code, backdoors, dialers, ransomware etc.…Some malware are actually combinations of more basic malware (e.g., a rootkit can be viewed as a Trojan horse backdoor tool) which are broadly classified according to:

- Infection technique: how does it propagate?
- Impact on target: what does it do?
- Type of exploited vulnerability: How (by violating which assumption) did it get in?

Table 1: Types of Malware and its characteristics

Virus	Self-replicating code that infects a host file. Usually requires human interaction to spread. Sometimes used as generic term for all malware.
Worms	Self-replicating code that spreads across a network. Usually does not require human interaction to spread.
Rabbit	Virus or worm that multiplies without bound.
Trojan Horse	Disguises itself as a useful program while masking hidden malicious purpose.
Backdoor/Trapdoor	Bypasses normal security controls to give attacker access.
User level Rootkit	Manipulates the OS kernel to hide and create backdoors
Spyware	Monitors and capture user keystrokes and collects information (e.g., via key logger)

2.1.3 Malware evolution: The AV-TEST Security Report 2017 /2018 published nowadays it is calling ransomware in figure 1, illustrates a marginal phenomenon, highlighting that only 0.94% of all malware deployed in 2016 was a blackmail trojan. There is no indication based on proliferation statistics that 2016 was the year of ransomware, said the team at AV-Test, an independent institute for testing the accuracy and efficiency of antivirus software. Ransomware accounted for less than 1% of all malware comprising not even 1% of the overall share of malware for Windows, the blackmail Trojans appear at first glance to be a marginal phenomenon," researchers said.

There are many valid reasons why ransomware got so much attention during the past year. For example, a user can be infected with a banking Trojan or a rootkit for years and not know about it. On the other side, once a user is infected with ransomware, he'll know about it the next second, because ransomware will change his desktop and lock his files.

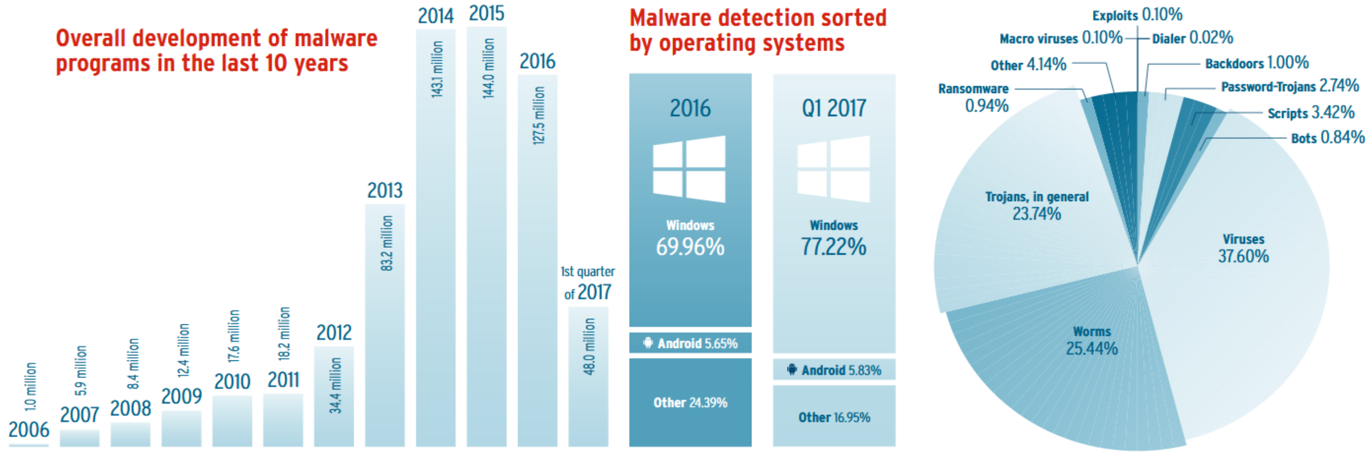

Fig. 2: Illustration of the evolution of malware

2.2 Virus Basics

Definition*:* A virus is a program that can infect other programs by modifying them to include a, possibly evolved, version of it.

- Virus: code that attaches itself to host programs and runs when host program executes. Running the host program usually requires user intervention.
- Self-replication: when the virus runs, it copies (a possibly mutated version of) itself to other host programs. The self-replicating mutating code is a cornerstone of artificial life research.

- A virus needs a target location method to find other hosts
- A running virus may also execute a payload = mischievous or malicious action.

2.3 Viruses infection techniques

- Compression virus: automatically compress files to save space (but there's a time/space tradeoff).
- Maintenance virus: install system updates, clean up undeleted temporary files, reset incorrect protection bits, defragment the disk, etc.
- Distributed database virus: make copies of information across multiple machines and modify old copies to be consistent with recent changes.
- Overwriting
    - Overwrite host program, changing behaviour (easy to discover)
    - Typically overwrite beginning, but can overwrite later (in which case virus may not be executed).

2.4 Basic Anti-Virus (AV) Techniques

2.4.1 Anomaly-based detection: Anomaly-based IDS typically work by taking a baseline of the normal traffic and activity taking place on the network. They can measure the present state of traffic on the network against this baseline in order to detect patterns that are not present in the traffic normally. Such methods can work very well when we are looking to detect new attacks or attacks that have been deliberately assembled to avoid IDS. On the other hand, we may also see larger numbers of false positives from anomaly-based IDS than we might from signature-based IDS. If the traffic on the network changes from what was present when we took our baseline, the IDS may see this as indicative of an attack and likewise for legitimate activity that causes unusual traffic patterns or spikes in traffic.

2.4.2 Signature-based detection: Signature-based IDS maintain a database of the signatures that might signal a particular type of attack and compare incoming traffic to those signatures. In general, this method works well, except when we encounter an attack that is new or has been specifically constructed in order to not match existing attack signatures. One of the large drawbacks to this method is that many signature-based systems rely solely on their signature database in order to detect attacks. If we do not have a signature for the attack, we may not see it at all. In addition to this, the attacker crafting the traffic may have access to the same IDS tools we are using and may be able to test the attack against them in order to specifically avoid our security measures.

2.5 Constraints of malware behaviour

Worms use a compromised machine to spread through instant messaging, emails, sharing etc. It discloses private or sensitive information to the hacker or displays it all over the internet. It changes your settings, wallpapers etc. It deletes files and folders of your hard drive without the administrator knowing about it. It causes software instability making the software showing errors whenever opened, hanging of software or closing down without any reason. Your computer becomes really slow making processing really hard. Some of the characteristics of different types of worms are:

2.5.1. Autorun..xfd.1-worm

Virus: Worm/Autorun.xfd.1
Date Discovered: 09/02/2009
Type: Worm
In the wild: Yes
Reported Infections: Low to medium
Distribution Potential: Low to medium
Damage Potential: Low to medium
Static file: Yes
File size: 106.295 Bytes
MD5 checksum: 8cec5723623ef9fb5be5ff26a2d1c338
IVDF version: 7.01.01.248 - Mon, 09 Feb 2009 17:48

2.5.2. AutoIt.X – Worm

Virus: Worm/AutoIt.X
Date discovered: 10/04/2008
Type: Worm
In the wild: Yes
Reported Infections: Medium
Distribution Potential: Medium
Damage Potential: Medium
Static file: Yes
File size: 617.473 Bytes
MD5 checksum: 3adfe5101e736d996b27b5d547909477
IVDF version:
7.00.03.144 - Thu, 10 Apr 2008 11:00 (GMT+1)

Side effects:
• Downloads malicious files
• Drops malicious files

- Lowers security settings
- Registry modification

Files copies itself to the following locations:
- %WINDIR%\regsvr.exe
- %SYSDIR%\svchost .exe
- %SYSDIR%\regsvr.exe
- %drive%\regsvr.exe

The following files are created:
– %SYSDIR%\setup.ini
– %drive%\autorun.inf.This is a non malicious text file with the following content:
• %code that runs malware%
– %SYSDIR%\28463\svchost.exe Further investigation pointed out that this file is malware, too.

Detected as: TR/Spy.Ardamax.J
– %WINDIR%\Tasks\At1.job
– %SYSDIR%\28463\svchost.001

3. EXISTING ALGORITHM

This method is the simplest method that involves clients and server connected in a wired local network. A malware detection algorithm is run in all the systems to check for the malicious content in the network.

If any worm or virus has been detected in the network, the system either the server or the clients are removed from the LAN using SNORT rule. After the system has been removed, the network has to be re-established for the communication to happen normally. This takes much time and the malware detection algorithm should again run to detect any threat and this process should be repeated until the total network is free from malicious attacks.

Disadvantages: This algorithm ensures the removal of harmful content to infect the systems at the great cost of losing performance efficiency. Also, the physical elimination of the system in the network is not much suitable to meet the increased demands in security threats.

4. PROPOSED ALGORITHM IN MALWARE DETECTION

The proposed algorithm is contained 3 modules:

4.1 Communication module

For any two or more clients to communicate with each other or when the client requests a service from the server, it is necessary that they should be connected in a network. Here the clients act as nodes to the router which acts as a server. The nodes are first established and connected to the router using the star topology. Once all the nodes are connected to the router, every node is specified with all the paths available to reach another node. There may be one or more paths to reach the desired destination. Before initiating the file transfer, the clients must be logged in. A client then transfers the files by providing the destination client info. In our proposed algorithm, we restricted the files to .txt and .java extensions. Once the transfer starts, information regarding the number of packets, the path of transfer can be viewed. When all the packets are transferred, the process at source client terminates. At the destination client, the file data received can be seen if everything goes well.

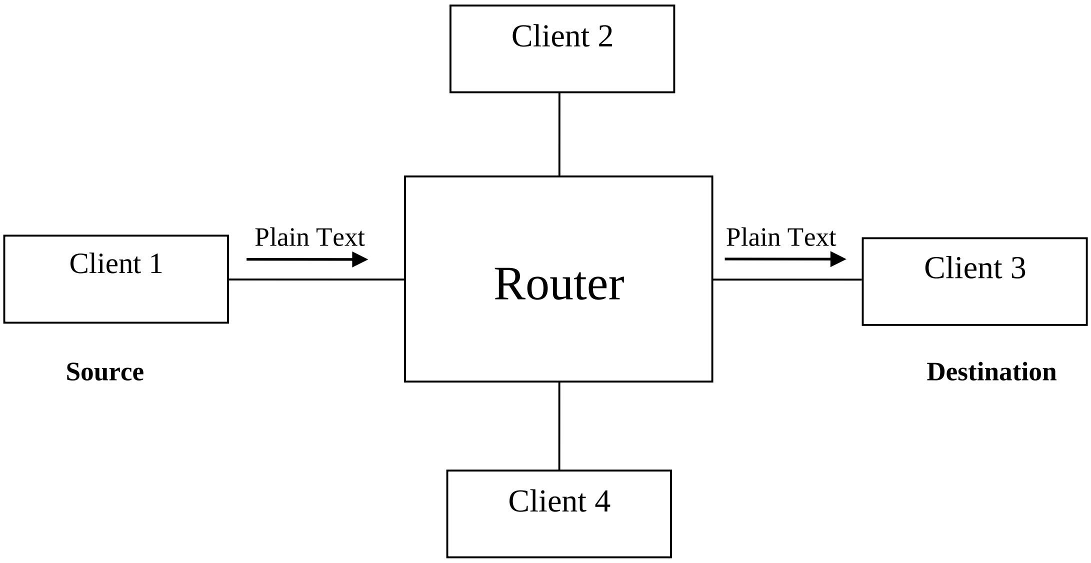

Fig. 3: Communication module architecture

4.2 Detection module

Once the communication of file transfer works smooth between two nodes, the file needs to get tested for malicious traffic. For this to happen, a malware detection technique must be deployed at the router. When the infected file reaches the router to enter the destined path, the malware detection techniques have to scan the file for malicious traffic by checking it against the database which contains the characteristics of the viruses and worms. If the infected program matches that of the virus or worm characteristics, the file is discarded. Also, the destination will be notified of this elimination of data as it is vicious.

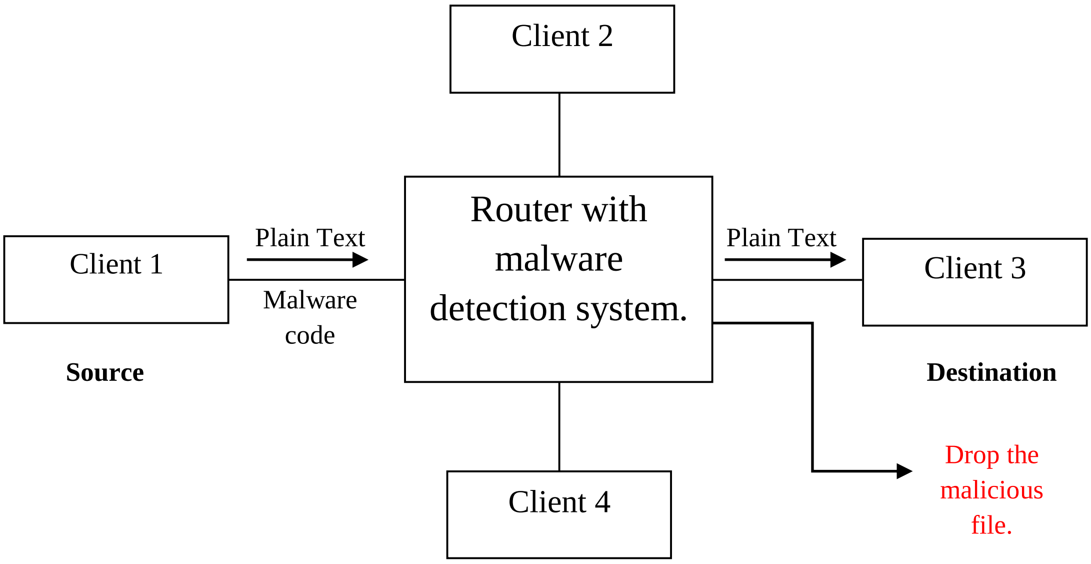

Fig. 3: Detection Module Architecture

4.3 Prevention module

Prevention is a very important step to be taken as detection alone is not sufficient to ensure the safety of the destination. The infected module has to be dropped at the router and the destination node must be acknowledged of the action done.

5. EXPERIMENTATION AND RESULTS

Table 2: Sample test cases

S. no	Condition	Input	Expected output	Obtained output	Results
1	Malware injected file transmitted through the wireless network.	Run detection code with some malware patterns database	A malicious content file detected and is dropped by the router.	A malicious content file detected and is dropped by the router.	Success
2.	Normal file transmitted through the wireless network.	Run detection code with some malware patterns database.	The file is transmitted successfully	The file is transmitted successfully.	Success
3	Both Malware file and normal file transmitted across wireless network0	Run Detection code with some malware patterns database.	The file is transmitted successfully after isolated the malicious content file and then discard it.	A malicious content file detected and is dropped by the router and accept the normal file to transmit.	May allow good traffic.

6. CONCLUSION AND FUTURE WORK

The main motto behind our paper is to protect systems that are connected through wireless LAN’s and the mobile environment from getting affected by malware. It is necessary to detect the worms and viruses before it enters the network, thereby ensuring protection to other systems by stopping their migration to other systems. In the first phase, we maintained the malware information in an Access Database and successfully deleted that malware whose information is present in the Database. Also, the database can be updated so that we yield better results. Since many people are having individual wireless connections and as security for the systems is the biggest concern today, we wish that our work would definitely help them to the maximum extent.

In our paper, we successfully deleted the malware (worms and viruses) stored in the database and detected the infectious packets flowing through the network. This work can be extended for all types of malware, spyware and ransomware thus providing total security to the systems. The database can be updated as and when new locations of these harmful content are known so that better security is assured. If any better Intrusion Detection system is introduced, that can be employed in this paper which would yield better results.

7. ACKNOWLEDGEMENT

We owe our tributes to Dr.R.Sivaranjani, Head of Department, ANITS for all his support in technical aspects and for his guidance. And also we are thankful to Mr G.Jagadish, Sr. Assistant Professor, ANITS for his support.

8. REFERENCES

[1] ‘A Novel Approach to Troubleshoot Security Attacks in Local Area Networks’ by Y V Srinivasa Murthy, G Jagadish, K. Mrunalini Dept of CSE, Anits in IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.9, September 2011

[2] ‘Investigations of automatic methods for detecting the polymorphic worms signatures’ by Shadi A.Aljawarneh, Raja A.Moftah, Abdelsalam M.Maatuk in Future Generation computer systems 60(2016)67-77.

[3] ‘An Intrusion-Detection Model’ by DOROTHY E. DENNING in IEEE transactions on software engineering, VOL. SE-13, NO. 2, February 1987, 222-232.

[4] Fredrik Linell, Dabid Mellqvist ‘Viruses and worms’ TDDC03 Information security Linkoping Institute of Technology May 10, 2004.

[5] ‘Detection of malicious Traffic on Backbone Links via Packet Header Analysis’ by Wolfgang John and Tomas Olovsson Department of Computer Science and Engineering, Chalmers University of Technology, Göteborg, SE e-mail: {wolfgang.john, tomas.olovsson}@chalmers.se.

[6] Thomas Chen, Jean-Marc Robert (2004). "The Evolution of Viruses and Worms". Retrieved 2009-02-16.Northcutt, S. (2002) Network Intrusion Detection, New Riders Publishers.