Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Efficient Approach to Identify the Information Loss with Snort in Wireless Technology

[1]R. China Appala Naidu, [2]A. Prakash, [3]Vinod P.K, [4]Sreenivasa Rao.T

[1, 2] Associate Professor, CSE Department, St. Martins Engg College, Dhullapally, Secundrabad, Telengana, India

[3]Sr Software Design Engineer, Verifone India Technology Pvt.Ltd Cyber Park, Electronic City Phase-1, Karnataka, India

[4] Post Graduate Teacher Kendriya Vidyalayam, CRPF Avadi, Chennai, Tamil Nadu, India

Abstract: The performance of Snort is analyzed and tested in Wireless Technology for Packet Loss. The Total system is implemented on Linux Platform. It is observed that there is increase packet loss when the traffic speed is increased. Similarly when the packet size is increased the packet loss was decreased.

Keywords: Snort, Wireless Technology, Packet Loss

I. INTRODUCTION

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network [6]. Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified. Of course A crisp, exact distinction between an attack by an intruder and the normal use of resources by an authorized user cannot be expected [2].IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect threads based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect threads based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat.

NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS.

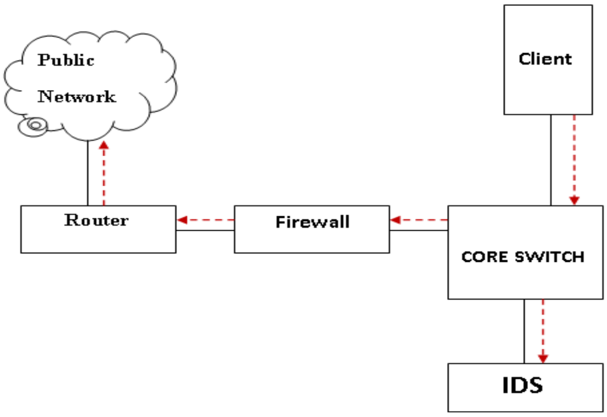

Fig. 1: Basic Intrusion Detection System

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

II. RESEARCH METHODOLOGY

A wireless network consists of several components that support communications using radio or light waves propagating through an air medium. Some of these elements overlap with those of wired networks, but special consideration is necessary for all of these components when deploying a wireless network. Figure 2 illustrates these primary components.

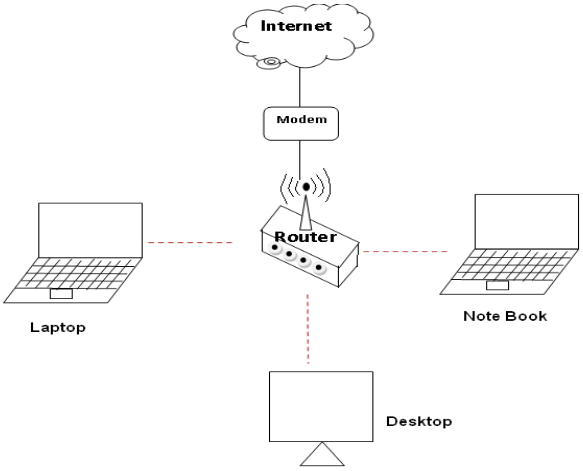

Fig. 2: Wireless Network Architecture

A user can be anything that directly utilizes the wireless network [9]. One of the most common types of user is a person. For example, a business traveler accessing the Internet from a public wireless LAN at an airport is a user. In some cases, however, the user might not be human. A robot, for example, might receive instructions over a wireless network from a central computer that controls a manufacturing process. Because the wireless network exists to serve the user, the user is the component that receives the benefits of a wireless network. As a result, users are an important part of the wireless network. The user initiates and terminates use of a wireless network, making the term end-user appropriate. Typically, a user operates a computer device, which often performs a variety of application-specific functions in addition to offering an interface to the wireless network [11].

Many types of computer devices, sometimes referred to as clients, operate on a wireless network. Some computer devices might be specifically designed for users, whereas some computer devices are end systems. Generally, any computer device might communicate with any other computer device on the same wireless network. The network interface card provides the interface between the computer device and the wireless network infrastructure. The NIC fits inside the computer device, but external network adaptors are available that plug in and remain outside the computer device. Wireless NICs also comply with a specific form factor, which defines the physical and electrical bus interface that enables the card to communicate with the computer device. The user must consider this to ensure that the chosen wireless NIC will fit within their computer device.

Air serves many purposes, such as providing a basis for speech, enabling air travel, and sustaining life. Air also provides a medium for the propagation of wireless communications signals, which is the heart of wireless networking. Air is the conduit by which information flows between computer devices and the wireless infrastructure. Think of communication through a wireless network as similar to talking to someone. Wireless information signals also travel through the air, but they have special properties that enable propagation over relatively long distances[12]. Wireless information signals cannot be heard by humans, so it's possible to amplify the signals to a higher level without disturbing human ears. The quality of transmission, however, depends on obstructions in the air that either lessen or scatter the strength and range of the signals.

The Modem is a hardware device that enables a computer to send and receive information over telephone lines by converting the digital data used by your computer into an analog signal used on phone lines and then converting it back once received on the other end. Modems are referred to as an asynchronous device, meaning that the device transmits data in an intermittent stream of small packets. Once received, the receiving system then takes the data in the packets and reassembles it into a form the computer can use.

A router is a device that forwards data packets between computer networks. This creates an overlay internetwork, as a router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination [10]. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

© 2015, IJARCSSE All Rights Reserved

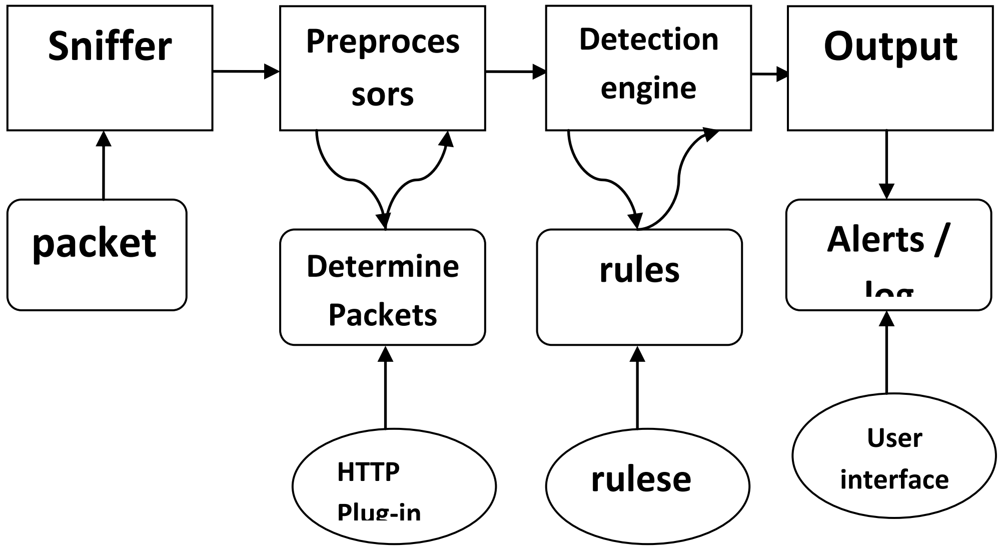

Fig. 3: Snort Architecture

Sniffer:

Sniffer monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Also sometimes called "network probes" or "snoops," sniffers examine network traffic, making a copy of the data but without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames [5]. Years ago, sniffers were tools used exclusively by professional network engineers. Nowadays, however, they are also popular with Internet hackers and people who are just curious about networking.

Preprocessor:

Preprocessors allowed the functionality of Snort to be extended, by allowing users and programmers to drop modular plugins into Snort fairly easily [1,4]. Preprocessor code is run before the detection engine is called, but after the packet has been decoded. The packet can be modified or analyzed in an out-of-band manner using this mechanism. Preprocessors are loaded and configured using the preprocessor keyword.

Detection engine:

The detection engine is the most important part of snort. Its responsibility is to detect if any intrusion activity exists in a packet. The detection engine employs Snort rules for this purpose. The rules are read into internal data structures or chains where they are matched against all packets [3,8]. If a packet matches any rule, appropriate action is taken, otherwise the packet is dropped. Appropriate action may be logging the packet or generating alerts. The detection engine is the time-critical part of Snort. Depending upon how powerful your machine is and how many rules you have defined, it may take different amounts of time to respond to different packets.

Alerts/log:

Depending upon what the detection engine finds inside a packet, the packet may be used to log the activity or generate an alert, logs are kept in simple text files, tcpdump style files or some other form [7,8]. All of the log files are stored under /var/log snort folder by default.

III. SYSTEM ARCHITECTURE

The architecture contains one personal computer and five laptops. This network contains a high performance PC running both open source and commercial tools to generate traffic at high speeds and monitor the network performance. The laptops are connected to the desktop in wireless. The Snort is used to identify the packet loss in the system.

IV. EXPERIMENTAL RESULTS

The network was designed to test the performance of Snort on Linux operating system. To get accurate results we tested with packet sizes of 512 and 1024 for both TCP and UDP. The experiment was done for the speed rang from 250Mbps, 500Mbps, 750Mbps, 1Gbps, 1.5Gbps, 2Gbps.

1. UDP

In this section the Snort performance on UDP Protocol was addressed. When the packet size was 512, snort performed well and there were no packet drop recorded on 250Mbps. When the speed reaches 500Mbps snort stared to drop packets. At the speed of 500Mbps Snort dropped 5% Packets, at the speed of 750 Mbps Snort dropped 32% packets, at the speed of 1Gbps Snort dropped 43% packets, at the speed of 1.5Gbps Snort dropped 45% packets and at the speed of 2Gbps Snort dropped 49% packets.

Table 1: Packet Size = 512

Speed	Packet Loss Information
250Mbps	No Packet Loss
500Mbps	5%
750Mbps	32%
1Gbps	43%
1.5Gbps	45%
2Gbps	49%

When the packet size was 1024, Snort performed very well as there were no packet loss in 250Mbps, 500Mbps. Table 2 shows that when the speed reached 750Mbps Snort dropped the packets. At the speed of 750Mpbs snort dropped 25% packets, at the speed of 1Gbps snort dropped 38%packets, at the speed of 1.5Gbps Snort dropped 42% packets and finally at the speed of 2Gbps Snort dropped 44% packets.

Table 2: Packet Size = 1024

Speed	Packet Loss Information
250Mbps	No Packet Loss
500Mbps	No Packet Loss
750Mbps	25%
1Gbps	38%
1.5Gbps	42%
2Gbps	44%

The figure 4 shows that when the packet size was increased percentage of packet loss decreased and when the speed was increased the packet loss increased.

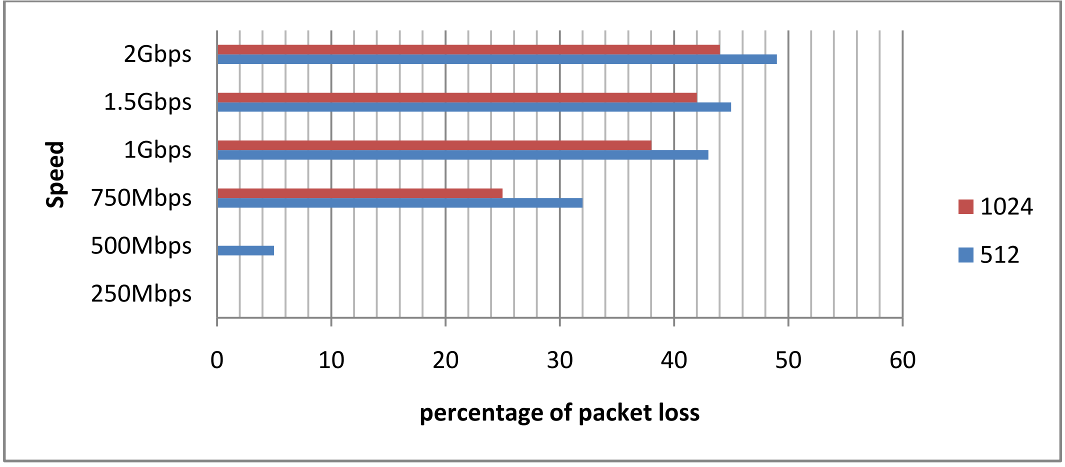

Fig. 4: Comparison of Packet loss between Pocketsize 512 and 1024 in UDP

2. TCP

in this section the Snort performance on TCP protocol was addressed. When the packet size was 512, Snort performed well, there was no packet loss in the speed of 250Mbps, 500Mbps. When the speed was 750Mbps Snort dropped 3% packets, at the speed of 1Gbps Snort dropped 15% packets, at the speed of 1.5Gbps Snort dropped 38% packets and finally at the speed of 2Gbps Snort dropped 49% packets.

Table 3: Packet Size = 512

Speed	Packet Loss Information
250Mbps	No Packet Loss
500Mbps	No Packet Loss
750Mbps	3%
1Gbps	15%
1.5Gbps	38%
2Gbps	49%

When the packet size was 1024, Snort was performed good and there was no packet loss at 250Mbps, 500Mbps and very less packets were lost in 750Mbps speed that is 1%, at the speed of 1Gbps Snort dropped 3% packets, at the speed of 1.5Gbps Snort dropped 8% packets and at the speed of 2Gbps the system dropped 11% packets. Figure 5 shows that when the packet size was increased percentage of packet loss decreased and when the speed was increased the packet loss increased.

© 2015, IJARCSSE All Rights Reserved

Table 4: Packet Size = 1024

Speed	Packet Loss Information
250Mbps	No Packet Loss
500Mbps	No Packet Loss
750Mbps	1%
1Gbps	3%
1.5Gbps	8%
2Gbps	11%

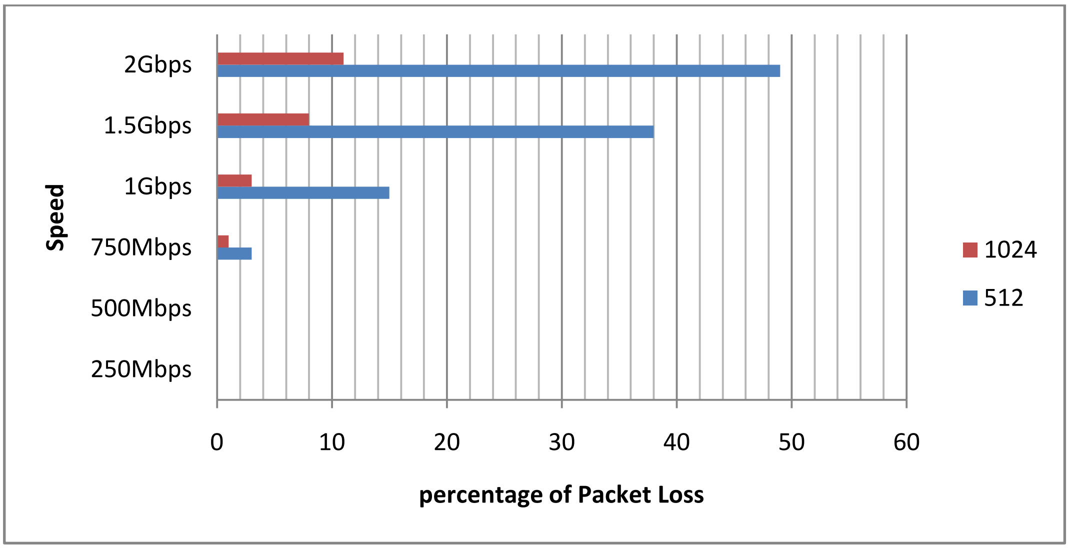

Fig. 5: Comparison of Packet loss between Pocketsize 512 and 1024 in TCP

V. CONCLUSION

In wireless network detecting packet loss is essential. In this network snort was used to identify the packet loss. The experiment identifies maximum packet loss in the network. When the packet size was increased percentage of packet loss decreased and when the speed was increased the packet loss increased. Implementation of IDS with honey pot will be identified in the future study.

ACKNOWLEDGMENT

we would like to gratefully and sincerely thank Management and principal of St.Martin's Engineering College for their guidance, understanding, patience, and most importantly, their Motivation during the paper implementation at St.Martin's Engineering College. Their mentorship was paramount in providing a well rounded experience consistent our long-term career goals.

REFERENCES

[1] Qing-xin Wu, "The Network Protocol Analysis Technique in Snort", International Conference on Solid State Devices and Materials Science, 2012, pp. 1-4.

[2] Rafeeq Ur Rehman, "Intrusion Detection Systems with Snort", Pearson Education, 2003,pp.5-80.

[3] R.China Appala Naidu and P.S.Avadhani "An Effective Evolution of Packet Loss With SNORT" InternatIonal Journal of Computer Science and Technology(IJCST) ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print), IJCST Vol. 4, Issue 3, July - Sept 2013.

[4] Snort(2012), "Snort", [Online] Available : http://www.snort.org.

[5] adeeb Alhomoud Rashid Munir, Jules Pagna Disso, Irfan Awan, Al-Dhelaan, 2011,"Performance Evalution Study of Intrusion Detection Systems", The 2nd International Conference on Ambiems, Networks and Technologies, 20122. pp.1-4.

[6] R.China Appala Naidu and P.S.Avadhani "A Comparison of Two Intrusion Detection Systems" InternatIonal Journal of Computer Science and Technology(IJCST) ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print), IJCST Vol. 4, Issue 1, Jan - March 2013.

[7] Packetloss (2012), "Packetloss", [Online] Available: http://www.nessoft.com/kb/42.

[8] Richard Bejtlich, "The Tao of Network Security Monitoring", Addison-Wesley, 2004, pp.50-60.

[9] J Bicket, "Bit-rate selection in wireless networks," MIT Master's Thesis, 2005.

[10] K. Jamieson and H Balakrishnan, "Partial packet recovery for wireless networks," in ACM SIGCOMM, 2007.

[11] J Kim et al., "Collision aware rate adaption for ieee 802.11 wlans, " in Infocom, 2006, pp.139-150.

[12] Allen Miu, Hari Balakrishnan and Can Emre Koksal, "Improving loss resilience with multi radio diversity in wirelss networks," in ACM MOBICOM, 2005.

© 2015, IJARCSSE All Rights Reserved