

Design and Implementation of a High-Performance Active Network Security System

Wen Ouyang¹, Kun-Ming Yu², Wen-Ping Lee³

Abstract—This paper describes the design, implementation and performance of a high-performance security system - Active Network Security Immune System (ANSIS) – based on active network. ANSIS is a compatible, scalable and practical network framework. It uses distributed security services to solve various security problems. The detective technique implemented in ANSIS can handle any type of DoS attacks, including novel worm spreading. Moreover, ANSIS not only improve the security of network system substantially, but also reduce the management and maintenance cost by a wide margin.

Index Terms—Active Network, DoS, Network Security.

I. INTRODUCTION

The growing demand of the Internet performance has greatly complicating the design of high performance network infrastructure. In spite of the convenience brought by networks, many security problems such as filching computer document, sniffing network data, computer virus, and crack arise. For these reasons, researchers had brought up various mechanisms to solve them. However, none of these mechanisms can handle the Denial of Service (DoS) attack and its transformations effectively. The issue is that DoS attacks are hard to prevent, hard to detect, and hard to respond. DoS had evolved to Distributed Denial of Service

(DDoS) using a group of computers for attacking victims. The newest type of DoS is worm spreading.

The currently used passive networks only forward packets. An active network can compute and process packets before forwarding them. For example, it can copy the packet, modify the context of packet or reroute it without following the packet's header. Thus, an active network can solve many passive network problems like vulnerability. The new generation of network security system should be able to tackle every part of security work, and an administrator comes to the picture only when unexpected issues happen. In order to cope DoS attacks and to solve the problems of current network security system, we proposed and implemented Active Network Security Immune System (ANSIS) which is a new high-detection-rate technique, a new response mechanism, and an active network based security system. Our detection technique is anomaly based. It utilizes network behavior characteristics, individual-driven security rule, and mail sending authentication. This detection technique enables ANSIS to cope with any type of DoS, including DDoS and novel worm spreading. Unlike other active network researches, ANSIS adopts the hybrid environment with both active network devices and passive network devices. Therefore, ANSIS is not restricted in a specific platform.

The paper is organized as follows. Section 2 introduces related work. Section 3 presents our detection and response mechanisms. Section 4 describes ANSIS system framework. The detail of implementation is given in Section 5. Section 6 shows the experimental results and is followed by a conclusion in Section 7.

II. RELATED WORK

There are many types of security threats in the network, for example, DoS, DDoS, port scanning, Sniffer, and Trojan Horse. To cope with those threats, tools were developed to provide a more secure network environment.

DoS would make victim or network taken out of commission by sending flurry packets to victim and

Manuscript received March 12, 2006. This work was supported in part by the National Science Council of the Republic of China under Grant NSC 93-2213-E-216-031.

¹Corresponding author and presenter

¹Wen Ouyang is with the Department of Computer Science and Information Engineering, Chung Hua University at HsinChu, Taiwan, R. O. C 300.; phone: 886-3-5186403; fax: 886-3-518-6416; e-mail: ouyang@chu.edu.tw.

²Kun-Ming Yu is with the Department of Computer Science and Information Engineering, Chung Hua University at HsinChu, Taiwan, R. O. C 300, phone: 886-3-5186412; fax: 886-3-518-6416; e-mail: yu@chu.edu.tw.

³Wen-Ping Lee is with the Computer Science Center, Chung Hua University at HsinChu, Taiwan, R. O. C 300, phone: 886-3-518-6235; fax: 886-3-518-6416; e-mail: luke@chu.edu.tw.

cause victim to consume their system resources like CPU, memory and network bandwidth. SYN flooding and SYN-FIN attack [1] are popular DoS attacks. DoS had evolved to Distributed Denial of Service (DDoS) attack. Cracker scans computers over Internet randomly by robot program to search for vulnerable computers and make them become intermediary attacker. Those intermediary attackers will start up DoS attacks at predefined time or when receiving cracker's command. The newest generation of DoS is worm DoS. Usually, there are only a few worms do DoS itself, but worm spreading that causes server or whole network system paralyzed can be seen as DoS too. Worm spreading sends packets all the time and has amplifying effect. The number of worm packets grows up exponentially. By this way, worm spreading consumes huge amount of network resources in very short time. Thus, we call it worm DoS.

Port scanning scans a range of ports to determine if there is a daemon binding the port. Once a cracker learns target computer being with some special ports, a cracker is able to know the target computer's OS and there may be some security vulnerabilities.

By the popularity of Internet, the network request types are getting more diversified. Many requests cannot be offered or handled well by today's network technologies due to, for example, TCP protocol's weakness. Moreover, it takes many years for a new network service to get standardized. In order to speed up the network evolution and to let individual be able to develop individual-driven services, active networks [2, 3, 4, 5, 6, 7, 8, 9] came to the picture. Tennenhouse and Wetherall are the first to propose active network at 1996 [10]. The main difference between active network and legacy network is that active network can process and compute packet before forwarding it. Legacy network, also called passive network, only forward packets. Individuals using active network can develop a new network service or protocol that can be setup and used immediately without coordinating with other individuals and without unnecessary interaction between co-existing protocols. The typical researches of active network are ANEP [2], Active IP [11], ANTS [12], and PLAN [4].

An IDS (Intrusion Detection System) is used to find out if a system have been intruded by crackers. IDSs are classified into misuse IDS and anomaly IDS [13, 14, 15] by its detective techniques. A misuse IDS defines malicious packets based on signature database. Snort [16] is one of the most famous misuse IDS. It has higher detection rate but it cannot detect novel malicious packets. Anomaly IDS defines normal packet and assumes that a packet is malicious if it does not act according to normal network behavior model. It uses statistic, fuzzy [17] or neural network [18] to model

normal network behavior. Although anomaly IDS can detect novel attack, there are some issues. For example, if the definition of normal network behavior model is too loose, then there will be many false negatives. On the other hand, if the definition of normal network behavior model is too restrict, then there will result in many false positives. Many fault alerts are generated and it may lead to information overloading. Thus, most IDS products today are misuse based.

Anti-virus system is another tool to prevent viruses. Anti-virus system is based on signature database so it can't detect novel viruses or worms. Another drawback of anti-virus system is from its being based on file control. It would not work if the worm or virus doesn't access any file.

Although there have been many security research or systems, problems still exist. Researches using passive network framework need to change their hardware or protocols. Researches based on system API or system calls are restricted in special platforms.

Some studies equip their network devices with computing capability but no new services can be setup or upgraded by administrators.

Most active network security researches are based on active routers. Any passive routers in the network will cut-rate the effect or make the system inapplicable. Some active network researchers using mobile filter service have problems to migrate service to target active device when the network is under flurry attack.

Researches based on LAN can not resolve attack packets engaging outgoing bandwidth. Most researches only detect, log, and report data when security issues arise. It requires the network administrator to solve the problem and no automatic mechanism is provided.

Most DoS researches are focused on the situation that attacker and the intermediary attacker are both outside the network. Only a few based on SNMP [19] consider the inner network attack situation. Framework based on SNMP [19] which detects and blocks attacks automatically needs special hardware equipments. The mechanism is useless if hardware is changed. Moreover, SNMP can't guarantee the packet to be sent to destination correctly. There exists another problem although using SNMP to close network port can block attacks. When a computer such as an important server needs to connect to network round-the-clock, the SNMP mechanism is inapplicable. Besides, most research are based on misuse IDS that they can't detect novel attack or worm. The anomaly IDS has the problem either low false negatives or high false positives.

In order to solve these security problems, we present a new detective technology and an active network based

security system along with its implementation.

III. PROPOSED DETECTION MECHANISM

A new high detection rate technique to determine if a packet is normal or malicious is required to compensate the disadvantages of misuse-based and anomaly based detection technique. The target malicious packets under detection include sniffer, port scanning, DoS, and worm spreading packets. In this section, we first expand the models of normal packets and malicious packets, and then we present our anomaly based high detection rate techniques and attack response mechanisms.

1. Models of normal and malicious packets

The percentage of SYN packet and total packets for each IP-port set is an important property. Normally the ratio of SYN packet to total packets for each IP-port set is very low. Malicious packets like port scanning, DoS, and worm spreading usually significantly increase the ratio of SYN packets to total packets for each IP-port set to very high value. The reason is that normal packets are used to transmit data and there will be many data packets and only one SYN packet in a TCP session. Malicious packets which send many SYN packets to target host or port only have a few or even no data packets.

2. The high detection rate technique

The detection can be classified into two phases: protocol phase and state phase. The protocol phase means the malicious packet would make use of the weakness of protocol. The protocol phase detection can be procured by predefining all of the behaviors using protocol weakness and block malicious packets. The problems due to SYN-FIN packet, Null scan, Xmas tree scan, and FIN scan can be solved in this way. The state phase means using normal packets to achieve attack aim. For example, port scanning and worm spreading both use normal packet to achieve their aim. The state phase is more difficult to design. We need to watch and record every host's stat to determine if it is actually normal because every single packet looks like normal one. The above-mentioned model of normal and malicious packets can thus be applied here.

Some worms like "Nimda" and "Netsky" or "Melissa" are spreading by e-mail. These worms read Outlook's address book and send mails which the worms attach themselves surreptitiously to people who are listed in the address book. Our IP n uses **mail sending authentication** to worm from spreading by email. The security service setup on active device will block SYN packet sent to port 25 (SMTP port) temporarily and send an authentication packet to mail sending authentication agent setup on PC. The authentication packet contains a random number. Once the mail sending authentication agent receives the

authentication packet, it prompts user with the random number and ask the user to send it back. This step is cannot be done by robot because the number is random. The security service will pass the SYN packet sent to port 25 for a predefined period once it receives and authenticates the authentication packet.

In general, a legacy IDS has fixed detective rules and customization is not allowed. Our detection service can solve those problems. We define some basic security rules and our detection service allows individuals to customize their own detection rules according to their security rules. Individual can extend or modify the rules by themselves. All network behaviors that don't obey the individual-driven security rules should be treated as abnormal and blocked. This mechanism not only detects malicious packets but also force users obey the security rules.

3. The attack response mechanisms

Passive security system usually only blocks and logs malicious behavior. Some of them advertise those security events to system administrators automatically in real time. It is inefficient and costly in management and maintenance if system administrators need to handle all kinds of events. A better way is to let security system respond to these events integrally while block and log them. Computer sending malicious packet can be classified into willful and unwilling. Willful computers actually perform attacks and footprinting or create worm crack. Unwilling ones are those intermediary attackers. The system should send message to both of them in different means. These messages include source address and destination address or event occurrence time. To crackers, these messages warn them the security system has found what they did and push them to give up. To victims, these messages notify them their system encountering problems so that they can repair their systems.

The packet which should be blocked is another issue. It is unfair to the victims that security system blocks all of their packets because they are not attackers or crackers. Thus, security system should just block those malicious packets and let other normal packets pass.

IV. SYSTEM FRAMEWORK

We present a new distributed network security framework ANSIS based on active networks. ANSIS is designed to detect all types of DoS attacks including novel worm with high detection rate and low false positive rate. It is effective when outgoing bandwidth is engaged by attack packets and worms spread between PCs connected to the same switch. The attack response mechanisms of ANSIS including filtering malicious packets out, updating signature database, and system

restitution are all done automatically just like creature's immune system. Unlike previous research, ANSIS filters out only malicious packets and let other normal packets pass through the same computer infected by worm. ANSIS also sends warning message to malicious packets sender. Although ANSIS is active network based, it's not restricted by active network devices. ANSIS can accommodate the environment with both active network and passive network devices. ANSIS consists of firewall, a group of IDSs, manager server, active router, active switch, passive switch, and computers. These components provide network services like filter service, backbone filter service, alert service, detection service, and PLAN interpreter service.

Firewall: An update service is on firewall to update the signature database automatically when the manager server got a new attack signature.

Active router: An active router with filter service.

Active switch: An active switch with filter service, alert service and detection service.

Passive switch: It is a layer 2 network device with SNMP. A mirror port links to IDS directly to mirror every packet through the switch to the group of IDSs.

Computers: The manager server will setup filter service automatically on those computers attached to passive switch.

A group of IDSs: A group of IDSs consists of misuse and anomaly IDSs connected by a load balance device to achieve real time detection. Once an anomaly IDS found novel attack packet, it analyzes its signature automatically and send the signature to manager server immediately. Misuse IDSs setup update service to update their signature database automatically when the manager server got a new attack signature.

Manager server: The manager server is responsible for the security event response service, SNMP service, setup service, event logging service, alert service, and update service. The security event response service sends message to filter service on active device to notify them the packets to be blocked when receiving attack warning message from detection service or IDS. If the attacker is attached on passive switch, then the security event response service will close network port used by attacker with SNMP service, or ask filter service on all computers attached on the same switch to filter the attack packet. The security event response service will also ask alert service sending warning message to the malicious packet sender. Event logging service logs every security event processed by manager server in order to inspect in the future. The manager server has a signature database synchronous with firewall and IDS. Furthermore, the manager server will authenticate and setup the detection service or filter service on new active device using setup service when setup service detects it. Finally, all links among active devices have priority mechanism to avoid attack packet to affect control

packet.

Filter service: The filter service is located on active switch, active router, and computers attached on passive switch. The manager server automatically sets up the filter service on new active device once manager server detects it. Filter service should be setup on those devices in general. If the system installs the service when the network is under attack, then the process of installation will make the network situation worse.

Backbone filter service: The difference between the backbone filter service and filter service is that the backbone filter service is setup on ISP's border router in order to solve the problem that the outgoing bandwidth is engaged by attack packets.

Alert service: The alert service will send warning message to malicious packet sender when receiving send command from detection service or manager server. These warning messages include information like source address, destination address, and event happen time. To the cracker, these messages warn them the security system has found what they did and make them give it up. To the victim, these messages can tell them their system has such a problem and need to be repaired.

Detection service: The detection service is used to detect DoS attack or the worm spreading. The service is setup on every active switch attached on computers based on distributed framework. The detection service will send command to filter service to block the malicious packets which was detected and ask alert service sending warning message to the packet sender. Detection service also sends the signature of these malicious packets to the manager server in order to update the signature database of firewall and IDS.

Update service: the updating service is setup on IDS and firewall. The manager server also updates signature database on firewall and IDS synchronized by update service when manager server got new signature.

PLAN interpreter service: NodeOS will pass active packets of PLAN to the service for execution and the result will be send back to NodeOS.

V. IMPLEMENTATION

We implement an active switch, active agent, and some security services in order to verify the practicality of our system framework and detective techniques.

1. Active switch

Our active switch is based on Linux 2.4.26 with AMD Durlon 750Mhz and five Intel 100Mbs NICs. We implement switching function at user level rather than kernel level. The switching functions including forwarding and maintaining MAC address hash table are written by C language and all services are written by Ocaml. All frames through the active switch will be

diagnosed to first decide whether it is active packet or passive packet. If the packet is active, it will be dispatched to PLAN interpreter to confirm and execute. If the packet is passive then it will be dispatched to different protocol services according to its protocol. In the protocol service, the packet will be passed to each security service by turns.

2. Security services

We implemented four security services including detection service, filter service, alert service, and mail service. Detection service is used to distinguish between normal and malicious packets. It uses individual-driven security policy rule to detect novel attacks. Our detection service uses the models of malicious behavior and the number of SYN packet per destination port to detect novel attacks. It considers host that sends over 50 SYN packets to the same destination port in 5 seconds as an attacker. As the active switch throughput is concerned, the detection service doesn't build in detection mechanism of other network behaviors. However, individuals can set them up either by themselves or on an IDS. Any packet matching the default rules will be treated as malicious packet and be blocked immediately. The filter service maintains a block list to determine whether a packet should be passed or blocked.

3. Service installation interface

A service installation interface should be provided since active device is programmable. We implemented an interface to help user to automatically load all dependent services in terms of service's profile, to protect other services, and to compile and link all necessary service together when setting up or updating a new service.

4. Active agent

Since the detection service sends warning message and mail-sending-authentication message, there should be an agent to receive the warning message and prompt user to do the procedure of mail sending authentication; hence, we implemented an active agent. The active agent is running under Microsoft Windows and stays at tray in peacetime. But once it received warning message sent by detection service, it will pop up a window to notify the user that some of their packets or frames have been blocked.

VI. EXPERIMENT

A simulation environment is set up to experiment the throughput of our active switch and the accuracy of

detection service. In the throughput experiment, we used an Apple iBook G4 with 100Mbps NIC as sender and IBM T30 with 100Mbps NIC as receiver. The sender sends burst UDP packets to receiver with different packet sizes through our active switch and Hogwash [20]. The Hogwash is an IDS and packet scrubber. It detects attacks over network and filters them out. The hardware of active switch/Hogwash having AMD Durlon 750Mhz and five Intel 100Mbps NICs uses Linux 2.4.26. In the detection rate experiment, we prepared a worm spreading computer running Microsoft Windows 2000 Server and infected by CodeRed, Nimda, Blaster, Netsky, and Nachi worms in order to generate worm packets. We also prepared eight computers running Windows 2000 Server without any patch to let worms infect them. We use tcpdump [21] on active switch to count the number of packets that worm spreading computer had sent and the number of packets that can be passed through the switch. There are two other computers in the experiment. One is IBM compatible PC that running Microsoft Windows 2000 Professional and another is iBook that running Mac OS X 10.3. The system had been patched; therefore, they wouldn't be infected by worms. We use them to see if there is a normal packet which will be blocked by our security services. All computers are connected by 100Mbps Ethernet. Next, we will discuss the throughput and the detection rate of our system.

1. Throughput

In the throughput experiment, the sender computer sends burst UDP packets to receiver with different frame sizes through our active switch and Hogwash, and the result is as figure 1 and 2. In this experiment, our active switch is with full security service except detecting UDP DoS. It is to obtain practical throughput data and prevent the testing UDP packets from being blocked by security service. In figure 1, the throughput of our active switch is over 100Mbps using over 1024 bytes frame. In figure 2, the frame size affecting the forward rate greatly and our active switch has 100% forward rate using over 1024 bytes frame. In any situation, our active switch outperforms Hogwash.

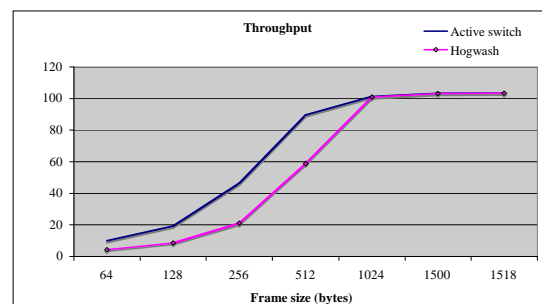


Figure 1: Throughput of Active switch and Hogwash

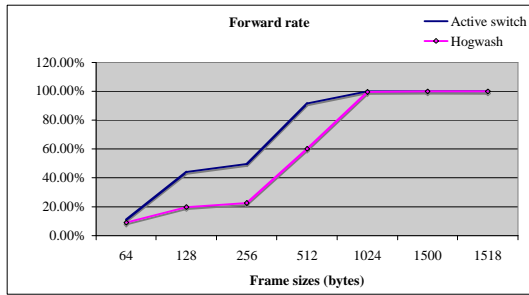


Figure 2: Forwarding rate of Active switch and Hogwash

2. Detection rate

There are two experiments about detection rate. The first one is the rate of worm packets passing through Hogwash compared with that of our active switch with detective mechanism. The results are as figure 3. The rate for Hogwash is above 50%. It is because Hogwash is a misused IDS and there is no signature of Blaster and Nachi; therefore, it can't detect these worms and block them. In another test, we connect eight computers, which are without any patch, to our active switch with filter service, alert service, mail service, and detection service. The experiment persists 72 hours and there is no computer infected by any worm. In fact, eight computers are all infected by worms in 1 hour once our security service was removed from active switch. The result is as figure 4. We also had connected two computers to our active switch in the same time. They are used to perform daily work such as browsing web and connecting to FTP server, BBS server, and sshd server. There is no packet detected or blocked by our security services.

Our system improves over previous works. It sends the warning message to both the infected computer and network administrators; therefore, users are capable of knowing that their computers are sending malicious packets and have been blocked. To crackers, these messages warn them their misbehavior has been tracked and make them give it up. To victims, these messages notify them their systems have encountered problems so that they can repair their systems. This mechanism can not only prohibit crackers but also reduce the manpower of administrators.

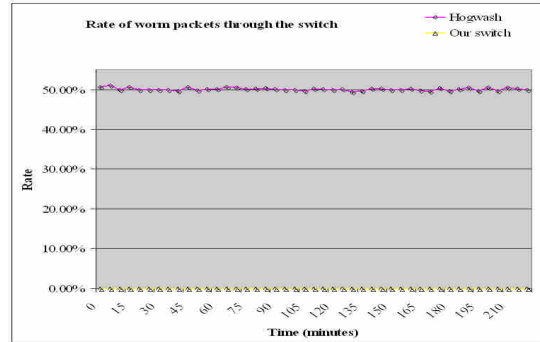


Figure 3: The rate of worm packets through active switch and Hogwash

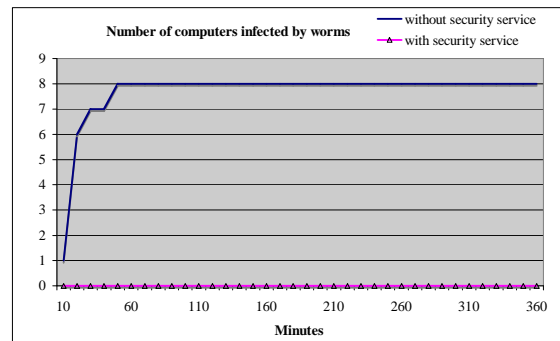


Figure 4: The number of computers infected by worm.

VII. CONCLUSIONS

In the paper, we present a new high detection rate technique, new response mechanism, and an active network based system: Active Network Security Immune System (ANSIS). Our anomaly-based detective technique combines the characteristics of network behavior, individual-driven security rule, and mail sending authentication together. It detects novel attacks including novel worm spreading as well as resolves the typical problems of legacy anomaly IDS and low false negatives or high false positives. The experimental results show that our detection services and filters can block all worm packets without any false positives. Our active switch can produce the throughput of active network up to 100Mbps and coexist with passive network perfectly. Alert service warns user that his computer is infected by worms and solves the problem of worm spreading through email. Both the procedures of ANSIS, such as involve blocking overall attacks and attack response, and post processes, are all automatic. Thus, ANSIS is a compatible, scalable, and practical network framework. It not only substantially improves the security of network system, but also reduces the cost of management and maintenance by a wide margin

REFERENCES

- [1] W. Richard Stevens, "TCP/IP Illustrated, Vol. 1", Addison-Wesley, 1st edition (January 1, 1994), ISBN: 0201633469
- [2] D. Scott Alexander, bob Braden, Carl A. Gunter, Alden W. Jackson, Angelos D. Keromytis, Gary J. Minden and David Wetherall. "Active Network Encapsulation Protocol (ANEP)", RFC Draft. 1997.
- [3] Kenneth L. Calvert, Samrat Bhattacharjee, Ellen Zegura, and James Sterbenz, "Directions in Active Networks", IEEE Communications Magazine, Volume: 36, Issue: 10, Oct. 1998, Pages: 72 – 78
- [4] Michael Hicks, Jonathan T. Moore, David Wetherall, and Scott Nettles, "Experiences with Capsule-based Active Networking", DARPA Active Networks Conference and Exposition, 2002. Proceedings, 29-30 May 2002 Pages: 16 – 24
- [5] Patel, A., "Active Network technology: A through overview of its applications and its future", Potentials, IEEE, Volume: 20, Issue: 1, Feb-March 2001, Pages: 5 – 10
- [6] Beverly Schwartz, Alden W. Jackson, W. Timothy Strayer, Wenyi Zhou, r. Dennis Rockwell, and Craig Partridge, "Smart Packets for Active Networks", Open Architectures and Network Programming Proceedings, 1999. OPENARCH '99. 1999 IEEE Second Conference on, 26-27 March 1999, Pages: 90 – 97
- [7] Sushil da Silva, Yechiam Yemini, and Danilo florissi, "The NetScript Active Network System", Selected Areas in Communications, IEEE Journal on , Volume: 19 , Issue: 3 , March 2001, Pages: 538 – 551
- [8] Jonathan M. Smith, Kenneth L. Calvert, Sandra L. Murphy, Hilarie K. Orman, and Larry L. Peterson, "Activating Networks: A Progress Report", Computer, IEEE, Volume: 32, Issue: 4, April 1999, Pages: 32 – 4
- [9] David L. Tennenhouse, Jonathan M. Smith, W. David Sincoskie, David J. Wetherall, and Gary J. Minden, "A Survey of Active Network Research", Communications Magazine, IEEE, Volume: 35, Issue: 1, Jan. 1997, Pages: 80 – 86
- [10] D. L. Tennenhouse and D. Wetherall, "Towards an Active Network Architecture". In Proc. of Multimedia Computing and Networking 96, San Jose, CA, January 1996.
- [11] David J. Wetherall and David L. tennenhouse. "The ACTIVE IP Option", In proceedings of the 7th ACM SIGOPS European Workshop, Connemara, Ireland, September 1996.
- [12] D. Wetherall, J. Guttag, and D.L. Tennenhouse, "ANTS: A toolkit for building an dynamically deploying network protocols", In IEEE OpenArch '98, San Francisco, CA, April 1998
- [13] David Endler, "Intrusion Detection Applying Machine Learning to Solaris Audit Data", Computer Security Applications Conference, 1998, Proceedings., 14th Annual , 7-11 Dec. 1998, Pages: 268 – 279
- [14] James A. Hoagland and Stuart Staniford, "Viewing IDS alerts: Lessons from SnortSnarf", DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, Volume: 1, 12-14 June 2001, Pages: 374 - 386 vol.1
- [15] Susan C. Lee and David V. Heinbuch, "Building a true anomaly detector for intrusion detection", MILCOM 2000. 21st Century Military Communications Conference Proceedings, Volume: 2, 22-25 Oct. 2000, Pages: 1171 - 1175 vol.2
- [16] Patel, A., "Active Network technology: A through overview of its applications and its future", Potentials, IEEE, Volume: 20, Issue: 1, Feb-March 2001, Pages: 5 – 10
- [17] John E. Dickerson and Julie A. Dickerson, "Fuzzy Network Profiling for Intrusion detection", Fuzzy Information Processing Society, 2000. NAFIPS. 19th International Conference of the North American, 13-15 July 2000, Pages: 301 – 306
- [18] Susan C. Lee and David V. Heinbuch, "Training a Neural-Network Based Intrusion Detector to Recognize Novel Attacks", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS-PART A: SYSTEMS AND HUMANS, VOL. 31, NO. 4, JULY 2001
- [19] Douglas r. Mauro & Kevin J. Schmidt, "Essential SNMP", O'REILLY, 1st ed edition (October 15, 2001), ISBN: 0596000200
- [20] <http://hogwash.sourceforge.net/>
- [21] <http://www.tcpdump.org/>