IJERMT
International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Volume 9, Issue-4 July-August- 2022
Email: editor@ijermt.org
www.ijermt.org

Assessing the Integration Potential of Open-Source Intrusion Detection Systems for Enhanced Network Security"

Prem Prakash Goyal, Research Scholar,
Department of Computer Science and Application,
Monad University, Hapur

Dr. Deepak Sharma, Research Supervisor,
Department of Computer Science and Application,
Monad University, Hapur

Abstract

Computer networks are a system of interconnected computers for the purpose of sharing digital information. The concept of a network began in 1962 when a server at the Massachusetts Institute of Technology was connected to a server in Santa Monica, California. Since that time the proliferation of computers and computer networks has increased significantly. One of the most significant challenges to networks is attacks on their resources caused by inadequate network security. The purpose of this research project was to evaluate open source, free, intrusion detection systems and how easily they can integrate into an existing network. Research was conducted for this study through a review of existing literature pertaining to intrusion detection systems and how they function.

Keywords: *Computer Networks, Security, Information Technology, Communication, Detection*

Introduction

In this research an attempt has been made to characterize the security and performance aspects of computer networks, by dividing (based on the thrust areas) research covering important fundamentals, current & emerging issues as well as potential future research work related to each of the 4 thrust areas. This research has a number of aims which is to determine whether or not there is an opportunity for a sustainable international market for computer networks, in terms of information delivery, security and technical capability. Secondly, it examines how this opportunity can be implemented at the infrastructure needs of service provider of wireless and WWW backbone, banks and merchants as well as the application and technological support. This research aims at designing a theoretical framework and application model and case study system to assess the evolution and the progress path ahead of virtual networks, the role of emerging technology such as ad hoc networks and the business models of the different stakeholders.

The effectiveness of the system can be maintained if the concurrent information is delivered at the client ends. This helps the system as well as client from bottlenecks of unnecessary data interchange. For that purpose, this research involves push technology support available in wireless technology. This research involves profile management and location-based service to generate the valuable information to deliver generated information at client end effectively. today measure problem found in the market is hacking, hanging the network and disturbing the network so with help of Analysis of IP Networks in reference Security Aspects & Performance remove the problem.

Network Security Based on IPv6

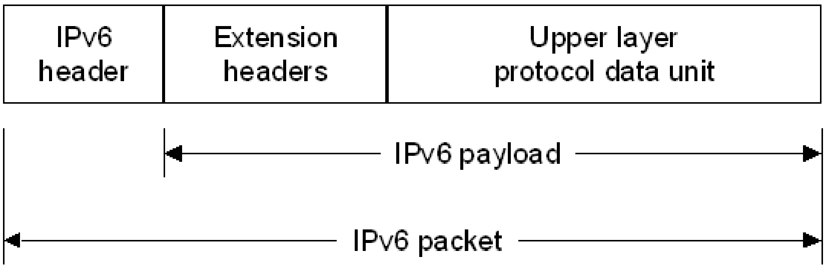
Overview of IPv6

Although the main function of Internet Protocol is to move data between networks, IPv6 has more capabilities than IPv4. An important feature is the growth of habitat. For example, all devices can have a public IP address so they can be uniquely tracked. With IPv6, the network can be used to verify the availability of these devices; even non-IT equipment in the field can be monitored with a permanent IP address.

IPv6 also has its own global configuration (auto-configuration) process, basically plug-and-play configuration to lighten the load on IT (auto-configuration works for Dynamic Host Configuration Protocol (DHCP) servers that don't need or need to be installed). Manually configuring IPv4 is already a challenge in itself, it appears that manually changing IPv6 addresses that are four times the length will cause more problems. Business and government projects will be able to realize many improvements from IPv6. You can set up a corporate intranet with the following benefits, but not limited to:

- Extended addressability
- Some automatic server configurations (some call it plug and play) and updated
- Simplified header format and Stream ID
- Latest Built-in strong IP layer encryption and End-to-end security with authentication
- (embedded security support enforces IP security
- In IPv6, setting up VPN is easier and more standardized than IPv4 because (authentication
- Extension Header (AH) and Encapsulating Security Protocol (ESP)) VPN used in IPv6 has
- lower penalties compared to VPN implemented in IPv4 [10]
- Improved support for multicast and QoS (better support for flow control and QoS for near real-time
- More and more powerful mobility mechanisms (improved support for mobile IP and mobile and computers).

IPv6 Core Capabilities include:



Because devices are identified by network addresses, communication links generally do not require identifiers (addresses), whereas communication over lines (computers) must contain characters (addresses). An IP address is an identifier used for every device connected to an IP network. In this configuration, different items (servers, routers, desktop computers, etc.) participate in communication with each other using their IP addresses as identifiers.

In Internet Protocol version 4, addresses consist of four octets. For the convenience of human communication, IP addresses are shown as separate dots, for example 166.74.110.83, where the numeric code is a short number (included) for the binary code description from the byte in question (an 8-bit number). a value in the range 0-255).

Protocol	Description
Internet Protocol version6(IPV6): RFC 2460	IPv6 is a connection less data gram protocol used For routing packets between hosts.
Internet Control Message Protocol for IPv6 (lCMPv6): RFC 2463	A mechanism that enable shostsand routers that Use IPv6 communication to report error band send status messages.
Multicast Listener Discovery (MLD): RFC2710, RFC3590, RFC 3810	A mechanism that enables one to manage subnet multicast membership for IPv6. MLD uses a series of three ICMPv6 messages. MLD replaces the Internet Group Management Protocol(l GMP) v3 that is employed for IPv4.
Neighbor Discovery (ND): RFC 2461	A mechanism that is used to manage node-to-node communication on a link. ND uses a series of five ICMPv6 messages. ND replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message. ND is implemented using the Neighbor Discovery Protocol (NDP).

TTable Key IPv6 Protocols

Main advantages of IPv6

The advantages of IPv6 can be summarized as follows:

1. Scalability: IPv6 has 128-bit addresses, while IPv4 addresses are 32-bit. The expected number of IP addresses for IPv4 is 232-1010. IPv6 provides 2128 locations. So, the number of beneficiaries nearby is 2128 - 1039.

2. Security: IPv6 includes security in its features such as payload encryption and communication authentication.

3. Real-time applications: provides better support for real-time traffic (egg., VoIP) includes "symbol flow" between IPv6 rules. Through this process, the router can determine the end-to-end stream through which data packets are sent.

4. Plug and Play: IPv6 includes a plug and play mechanism that makes it easy for devices to connect to the network. The required configuration is automatic.

IPv6 is designed to extend and support new and expanded options. For IPv4, the 32-bit address can be expressed as AdrClass netID hostID. A network segment can have a network ID or network ID and subnet. By definition, every network and every host or device has a unique address.

As mentioned earlier, IPv4 theoretically allows 232 addresses as four octal addresses.

The format and address scheme used by IPv6 are described in IPv6 address format RFC 2373. As mentioned earlier, IPv6 addresses contain 128 bits instead of 32 attributes of IPv4 addresses. The number of items by address is as follows:

IP Version	SizeofAddress Space
IPv6	128bits, which allows for 2^{128} or 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 (3.4 x10^{38}) Possible addresses.
IPv4	32 bits, which allows for 2^{32} or 4, 294, 967, 296 possible address.

Table Format & Addressing Scheme

An IPv6 address is defined as 8 groups of 16 bits each, separated by ":" characters. Each 16-bit group is represented by four hexadecimal numbers, meaning each number has a value between 0 and F (0, 1, 2, ... A, B, C, D, E, F, A = 1010, B = H10 etc. for F = 1510). Here is an example of an IPv6 address: 3223: 0BA0: 0lE0:D001: 0000: 0000: D0F0: 0010

If one or more groups of four digits are 0000 digits, you can replace the replacement with zero. Two (: :). For example, 3223:0BA0: is the abbreviation of the following address: 3223:0BA0:0000:0000:0000:0000:0000:0000 Special Purpose4 IPv6 Address (: :). according to the program: Returns or returns the received virtual address. This address is specified as 127.0 in IPv4. 0.1 addresses. In IPv6, this address is represented as Unspecified Address (: :). This address is not sent to anyone, it is used to indicate that there is no address.

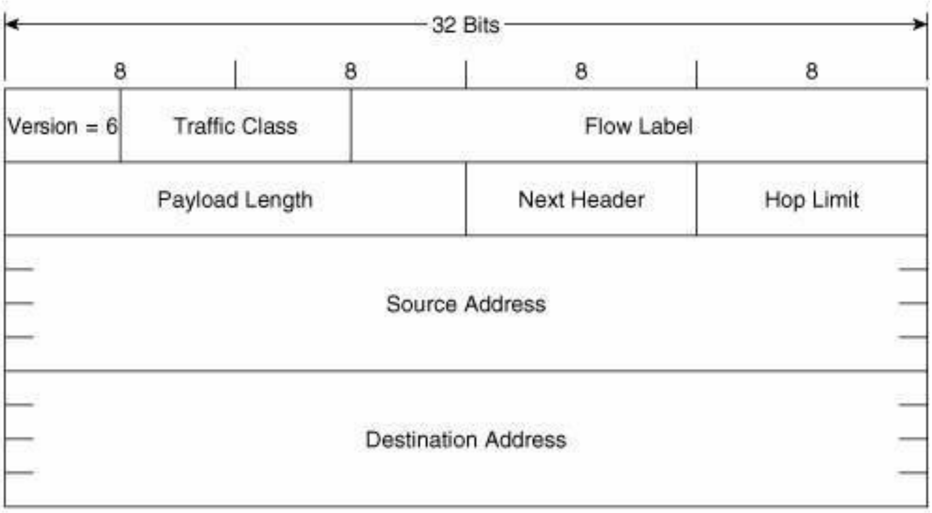
IPv6 over IPv4 dynamic/automatic addressing.

These addresses are designated as IPv4 compatible IPv6 addresses and allow IPv6 transmission to be transparent over IPv4 networks. For example, they are represented as: 156.55.23.5.

Automatic description of IPv4 over IPv6 addresses. These addresses only allow IPv4 nodes to operate on IPv6 networks. They are represented as IPv4 mapping IPv6 addresses and represented as: FFFF: (for example, FFFF: 156.55.43.3). Like IPv6 packet pattern and extension header IPv4, IPv6 is a network-independent, anonymous filename often used to address and forward packets between hosts. Connectionless means that no phase is established until data is exchanged. Unreliable means delivery cannot be guaranteed. IPv6 always forwards packets optimally.

IPv6 packets can be lost, mis-sent, duplicated, or delayed. IPv6 itself does not try to get rid of these errors. Responses to incoming packets and recovery of lost packets are handled by higher-level protocols such as TCP [13]. In terms of packet forwarding, IPv6 works like IPv4. An IPv6 packet, also known as an IPv6 datagram, begins with an IPv6 header, as shown in Figure below:

Fig -IPv6 packet header



IPv4 headers and IPv6 headers do not interact directly. A host or router with both IPv4 and IPv6 implementations must recognize and process both header formats. This causes some problems when migrating between IPv4 and IPv6 environments. The IPv6 IP header is optimized and has a fixed length (40 bytes). In IPv6, header fields in IPv4 headers have been removed, renamed, or moved to new optional IPv6 extension headers. IPv6 headers are now fixed-length objects, so the header length field is no longer required. The IPv4 "Service Type" is equivalent to the IPv6 "Traffic Class" field. The "total length" field has been replaced with the "payload length" field. Instead of individual routers, the IPv4 segment control fields (Identity, Flags, and Fragment Offset fields) have been moved to similar fields in the fragment extension header. The function provided by the Time to Live (TTL2) field has been replaced by the Jump Limit field.

- Routing Header - Same as initial routing options for IPv4. Headers are used to indicate specific routing.
- Authentication Header (AH) - A security header that provides authentication and integrity.

- Encapsulating Security Payload (ESP) Header - A security header that provides authentication and encryption.
- Fragmentation header. Fragmentation headers are similar to IPv4 fragmentation options.
- The title of the target parameter. A header containing a set of options that should only be processed by the final destination node. Mobile IPv6 is an example of an environment where these headers are used.
- Transition Parameters Header - A set of parameters required by the router to perform certain management or debugging function.

Simple Operation of Mobile IPv6

A mobile phone is always assumed to be available at its address, regardless of whether it is currently connected to the home network or away from home. "Home address" is the IP address assigned to the mobile phone in the home subnet prefix of the home connection. When the mobile phone is at home, traditional Internet routing techniques are used to send packets to the home address of the mobile phone to the home connection. When a mobile phone is connected to an external link away from home, it can also address one or more addresses. Tracking the address is the IP address associated with the mobile phone with a unique external subnet prefix. On average, a company's IT resources are hacked several times a week. About 20% of large companies have at least two major events per year (). The challenges business planners face is only more difficult. Information security will grow at a rate far beyond what people can comprehend. Some networks may already be carrying IPv6 traffic without the administrator's knowledge. Therefore, it is important to understand what the security issue is in the context of IPv6.

Firewalls are an important mechanism that supports perimeter security, even if they are only part of the solution. Firewall-based security is a way to secure a private network by controlling incoming and outgoing data. Firewalls use policy-driven packet filtering capabilities, often used to restrict access/access to specific devices and applications. These rights are often called access control lists (ACLs). It covers the areas of information security, confidentiality, integrity and usability. Confidentiality is protection against unauthorized access, ownership or use of intellectual property. Integrity is protection against unauthorized access, modification, or loss of assets.

Also, when people talk about security nowadays, most people are talking about just writing a few lines of filtering to the Transmission Control Protocol (TCP) port-based router or perimeter firewall to prevent multiple trafficking from being allowed on the intranet. This obviously just gives a false sense of security with nothing for business continuity and damage/crime returns. For example, a filter may allow email (SMTP) streams while excluding certain streams; however, a virus or other security-breaking code could enter the stream.

Alternatively, allow other types of damage based on the generally accepted TCP flow. Coding decisions led to the so-called "mixed threat" that is now all too common. Threats combine the characteristics of viruses, worms and Trojan horses with the injury of arbitrarily coded servers and the Internet, and unleash, spread and spread attacks. Because these threats use a variety of methods and techniques, the damage often spreads quickly and can lead to extensive criminal activity.

Basic Infraction Mechanisms

Term	Definition
Attack	An attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's confidentially, integrity, or availability.
Audit	The process of examining the history of a transaction to find out what happened. An operational audit can be an examination of ongoing activities to determine what is happening. It can also be an independent review and examination.
Business Continuity Planning	Written plan describing the procedures the company takes In case of potentially disruptive events short of a disaster (for which the Disaster Recovery Plan is applicable)to assure that the operations of the Company can continue unimpeded.
Compromise	Disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification ,destruction ,or loss of an object may have Occurred.
Denial of Service	The result of any action or series of actions that Prevents any part of an information system from functioning.

Disaster Recovery Planning	Written plan describing the steps company would take to rest ore computer operations in the event of a disaster containing' four components: the emergency plan ,the backup plan, the Recovery plan ,and the test plan.
Disaster Recovery Testing	Written plan describing the steps to test the DisasterRecoveryPlan.
Fraud Discovery and Interdiction	Fraud: Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value. Fraud: Computer. Fraud: Computer Fraud: Computer.

Two types of attacks that network administrators often see are: IPv4, IPv6, and protection seeking in mixed environments.

Malicious attacks that use malicious packets and traffic to identify and exploit application vulnerabilities and cause the application to stop working (deletion) or unexpectedly. how to respond; In particular, attackers use violent attacks, hoping that the application will give them control over the target. These attacks are called escalation attacks. When an attacker takes control of a system, they can intentionally install executable files that can communicate with the attacker's command and control (C&C) system. C&C can issue a remote command to run almost any service (hosting a website, sending spam, etc.).

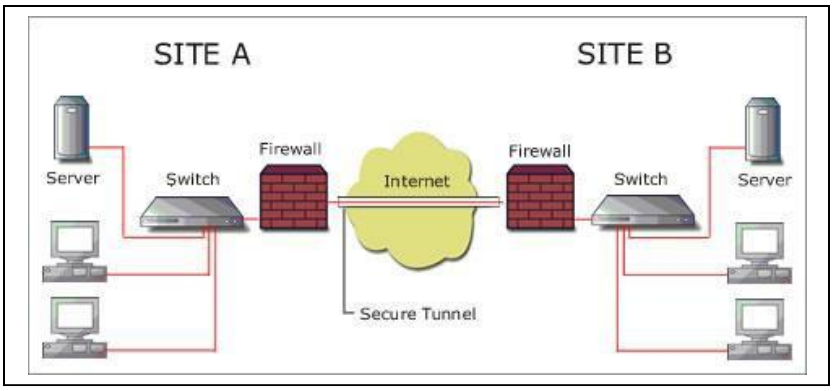
- Overflow attacks are designed to drain application, system, or network resources (performance, memory, or bandwidth capacity) and thus render users unserviceable. Flooding attacks are basically denial-of-service attacks, and vendors place special emphasis on the ability of products to block denial-of-service attacks and distributed denial-of-service (DDoS) attacks.

Firewall Capabilities

Firewall technology and implementation has changed and evolved over the years. However, in a simple definition, a firewall is a network security device that enforces an organization's security policies by allowing or denying network connections. For the firewall to work effectively, security administrators must use the organization's security policy to establish a detailed firewall process.

The policy setting is the setting that the firewall uses to examine the contents of packets passing through the device and is the basis for deciding which packets to forward. In addition to enforcing security policies, firewalls can also record traffic passing through them, making them powerful security tools [22], [20]. Figure 2.11 shows a simple electrical installation.

In addition, firewalls have the following functions: Network address definition Virtual private network Demilitarized (restricted) zone Protection against spoofing,



Network Address Translation (NAT)

In a traditional IPv4 environment, NAT facilitates end-to-end communication and provides better security. NAT provides a solution to the absence of valid IP addresses under the current IPv4 protocol by rewriting the contents of the IP packet header to be seen by a (different) IP address. This feature also allows organizations to hide details of their network topology by making all internal details visible through a single IP address (usually a firewall).

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a private network that uses a public network, usually the Internet, to connect remote locations or users. Instead of using a private, real connection like a leased line, a VPN uses a "virtual" connection that goes from a company's private network to a remote location or to employees over the Internet.

Firewall Type

When an organization wants to use network security, the firewall type should be selected based on specific requirements. The type of security entity will determine the type of firewall that should be implemented.

- Packet filters
- Proxy or application-level filtering
- State Audit

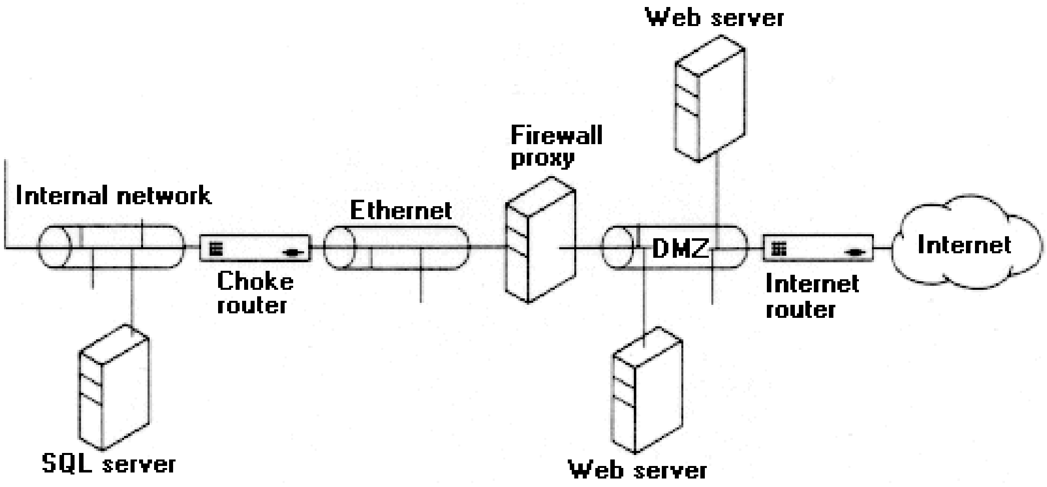


Fig. Layer coverage by different types of firewalls

Packet Filter Packet filter firewalls work by examining packets and focusing on collecting header information to make filtering decisions. This type of firewall usually only works by measuring location, address and port service. While packet filtering firewalls may not have great features or high security, they are inexpensive and can handle large traffic.

Proxy

Proxy firewalls are considered by many to be the most efficient yet secure firewall technology. The main difference of this process from packet filtering is that there is no direct communication between the client and the server.

A proxy acts as an effective intermediary between the two endpoints it needs to communicate with and only allows connections through the proxy domain.

Status Check

This gives security administrators a level of granularity and greater flexibility to enforce the necessary controls based on the priority of the asset.

As well as firewall type and layout, it is important to ensure that policies and security policies appropriate to the firewall are applied. Firewalls only provide a false sense of security unless security administrators understand the types of traffic and flows that should be allowed on a given network. This is true in any environment, whether it's IPv4 or IPv6. Given that security is installed in the environment and often only managed in the environment, this time will force organizations to find ways to improve their architecture with IPv6.

Most firewalls that support IPv6 have separate IPv6 and IPv4 policies. Therefore, regardless of the environment (pure IPv4, pure IPv6, mixed IPv4 / IPv6), these rules must be combined to properly manage and safely prevent accidents.

IPv6 Address Security

IPv6 has a very large address space and /64 is usually the smallest address for a local area network (LAN). This large address space benefits from a secure location, as address and port scanning of subnets will be more difficult and time consuming.

As mentioned earlier, an IPv6 address has two parts: a subnet prefix that represents the network it is connected to, and a local identifier. IPv6 stateless address auto configuration helps with IP address management, but causes some concern as Ethernet addresses are encoded in fewer than 64 IPv6 addresses. Hypothetically this could be used to monitor a host moving on the network using different ISPs. IPv6 supports temporary addresses, allowing applications to control whether they want to use permanent IPv6 addresses or private temporary addresses [RFC4218].

IPv6 Anycast Address Security Fraud: Computer issues with Anycast addresses remain.

1. Use general procedures on content servers. These systems provide information to all systems and are not particularly concerned with privacy as they make their content publicly available. However, they are interested in honest information and refuse to serve the opposition. For example, someone checking a search engine's results or blocking certain machines from accessing the search engine would be a serious concern.

There are also public content servers that provide services open to all systems but must protect confidential information. They use appropriate levels of authentication and authorization controls to ensure that information is only accessible to appropriate users.

2. Immediately use an existing IP address from outside websites to authenticate without a certificate. Today, with IP address spoofing and TCP number guessing becoming increasingly common attacks, these applications open themselves up to public connections and rely on other systems such as firewalls for general security.

3. Get current IP address but try some authentication with DNS, use good FQDN for management. (This is usually done by looking up the IP address backwards, then doing a forward lookup and verifying that the IP address matches the reverse address in a future view.) These applications are subject to many attack areas that use the Address spoofing process. And TCP code guessing, because the attacker knows this, can create a DoS attack using fake addresses with real DNS records.

4. The use of cryptographic security techniques ensures non-denial by strengthening peer-to-peer and data integrity with or without confidentiality. Such systems may also be vulnerable to denial-of-service attacks.

5. Use cryptographic security techniques (such as opportunistic IPsec) without strong authentication. Therefore, provides information with integrity or confidentiality when communicating with unknown/unrecognized leaders.

These applications, like the first category above, cannot perform management based on network data because they do not know the identity of the peers. However, they can use a high-level personalization strategy to control access. The availability of IPsec (and similar solutions) and communication channels allows systems (vulnerable to man-in-the-middle (MITM) attacks) to operate in the privacy of fellow personal security. A classic example is the Remote Direct Data Placement Protocol (RDDP), which works well if there is a channel connection when used with opportunistic IPsec. A link channel provides a link between the IP layer and the application protocol.

Redirect Attack

Next, we list some countermeasures. If the route can be disrupted, packets to all destinations may take priority over all destinations. This can be done by first injecting a long shot into the routing group, allowing the longest match algorithm to forward the packet to the attacker. Similarly, DNS can be affected and changes can be made to the hostname information to advertise a different IP address for the hostname that works better than the hostname. Any system on the path from the host to the target host can be compromised and used to disrupt traffic.

It can best be added to the system to accomplish this attack. Typically, these attacks only work if the attacker is on the way when they launch the attack. However, in some cases, an attacker can create a DoS attack that persists for at least a while after getting off the road. An example of this would be an attacker who uses Address Resolution Fraud: Computer (ARP) or ND spoofing to attach himself or send a packet to a black hole (source constantly experiencing L2). ARP/ND entries will remain in the neighbour's cache for some time (about a minute for ARP, but depends on configuration) after the attacker is gone.

Time shift attack

The term "time shift attack" is used to describe an attacker's ability to launch an attack after leaving the path. Thus, the attacker may be on the road at certain times, spying on or modifying packets; it will then present the attack when the attacker is not on the way. In the current internet, it is not possible to perform this attack to modify packets.

However, some time after the attacker leaves, it can cause a DoS attack, for example, by leaving a fake ARP entry in one of the paths, or by leaving a fake TCP reset packet text that is seen as the TCP initial number. on the way. makes the message sent to the black hole. This is different from the classic redirect attack. The difference is that the new place is non-existent or unreachable. Therefore, sending the packet to the new destination causes the packet to be dropped by the network target, resulting in a denial of service.

Third-Party Denial of Service Attacks

Attackers can use the redirection capability to cause unnecessary third-party overloads.

For example, if A and B are communicating, an attacker X could force A to send a packet destined for B to some third party in C. A third-party DoS attack can target a specific host's resources or target a specific IP. Visit before attacking the network infrastructure by overloading routers or connecting even if there is no host at that address. The discussion in RFC 4218 identifies some of the issues that IPv6 network planners need to address.

Basic IPv6 Security Considerations

This section covers security issues related to additional features in IPv6 such as message flows, neighbour discovery, and message extensions.

IPv6 Stream Labelling Issues

A packet identifier uses a trio of label, address, and destination address to identify the flow of a particular packet. Packets are processed according to a specific stream by nodes configured for a specific stream state [RFC3697]. Since the mapping of the connection to a particular protocol is due to the IP address of the IPv6 header and the text result, the user can get better by changing the IPv6 headers or injecting packets with bogus addresses or tags. This can also lead to a denial-of-service attack as it is likely to send bad traffic with the highest priority. The device then prioritizes bad traffic that may affect the availability of the network.

ICMPv6 Issue

The Internet Control Message Protocol (ICMP), version 6 (ICMPv6) plays an important role in IPv6. Features provided by ICMPv6 include:

- Automatic Address Configuration
- Duplicate Location Detection
- Echo Request and Echo Response
- Error Reporting
- Neighbour Availability and Address Resolution
- Router Renumbering
- Router broadcasts Is it from authorized routers
- Is there security for neighbour broadcast
- Is there a return from the router from which the packet was sent?

Neighbour Discovery Issues

Routing header

NOTE: which blocks all IPv6 packets carrying Routing Headers (other than blocking type 0 and allowing others) has serious implications for future IPv6 enhancements. Although a small percentage of firewalls block other types of routing headers by default, it is impossible to bind IPv6 routing headers. For example, Mobile IPv6 [RFC3775] is based on Type 2 Routing Header; Massive blocking effects on Routing Headers will make Mobile IPv6 impossible to deploy, but may be necessary until more control is achieved. A firewall policy designed to prevent packets containing RH0 cannot simply filter all traffic using the tag; It should be possible to block the forwarding of type 0 traffic without blocking other types of routing headers. Also, the default setting should allow redirection with a non-0 extension.

DNS Issue

• Local addresses should not be copied.

• The address-based security model identifies vulnerabilities and is not recommended.

• Setting up authorization mechanisms (e.g., shared secrets or public-private keys) between nodes and DNS servers must be done manually and can take a lot of time and expertise.

• Setting up a reverse tree is somewhat complicated, but reverse DNS checks provide the weakest security.

- Only (suspicious) security-related apps will be merged with other processes when checking users.

- Backlinks between 6to4 addresses and Teredo addresses are vulnerable to dynamic DNS updates.

Conclusion

In this paper we have conferred a comprehensive overview of the state-of-the- art research work on QoS support in MANETs. We have presented the issues and challenges involved in providing QoS in MANETs in terms of the research work on QoS models, QoS resource reservation signaling, QoS routing and QoS MAC, which are required to ensure high levels of QoS.

Related areas for further research include power consumption, resource availability, location management, interlayer integration of QoS services, support for heterogeneous MANETs, as well as robustness and security. Continued growth is probable in this area of research in order to develop, test and implement the essential building blocks for providing efficient and seamless communications in wireless mobile ad hoc networks. In modern times, computer networks are very important as information technology is increasing rapidly all over the world. The network and data communication are the essential factors to rise information technology in the world as technology's advancement is on the system, including the gadgets. Networking may have seemed like a necessary evil in the past. With these tools, though, you can now create meaningful and impactful relationships everywhere you go. Practicing your networking skills can help you become more confident and help you meet new, interesting people.Organizations [8] should take at least the following steps regarding IPv6 security:

• Create an IPv6 security plan

• Disable IPv6/Tunnelling

It follows that network/security administrators need to make detailed plans to create a reliable IPv6 environment.

References:

[1] Bradley, T. *Glossary*. http://netsecurity.about.com/library/ glossary/bldef appg.htm.

[2] BroadbandReports.com, dslreports.com. Does IPv6 introduce new security vulnerabilities? New York: Silver Matrix LLC, Feb, 15, 2008. http://www.broadbandreports.coml faq/ipvsixl 4.0 _IPv6 _Security.

[3] CSO Online. http://www.csoonline.com/glossary/category.cfm?ID= 13.

[4] Desmeules, R. *Cisco self-study: Implementing Cisco IPv6 Networks (IPv6).Cisco* Press, June 6, 2003.

[5] Hermann-Seton, P. *Security features in IPv6.* SANS Institute 2002, as part of the Information Security Reading Room, 2002.

[6] ICANN Security and Stability Advisory Committee (SSAC). *Survey of IPv6 support in commercial firewalls.* Oct. 2007.

[7] IPv6 Portal, http://www.ipv6tf.org/meet/faqs. php

[8] Juniper Networks. An IPv6 security guide for U.S. government agencies: Executive summary, *The IPv6 "World Report Series,* Volume 4. Sunnyvale, CA:, Juniper Networks, Feb. 2008.

[9] Kaeo, *M.*, D. Green, J. Bound, and Y. Pouffary. IPv6 security technology paper, *North American IPv6 Task Force (NAv6TF) Technology Report*, July 22, 2006.

[10] Lioy, A. Security features ofIPv6, Chapter 8, *Internetworking IPv6 with Cisco routers*, Silvano Gai. New York: McGraw-Hill, 1998, also available at www.ip6.com/us/book!