Network Security; the Concepts, Challenges, and Solutions for Improving the Network Security

Houshang Salhiy[1], Behzad Lotfi[2]

[1] MEng in Software Engineering, Faculty Member, Institute for higher education hakim nezami Quchan
[2] MEng in Computer Architecture, Faculty Member, Institute for higher education hakim nezami Quchan
Houshang_salhiy@yahoo.com

Abstract:Considering the increasing development of the intrusions especially through the internet, and considering the importance of the data security and the necessity of providing proper services on these networks, it is increasingly important to know such intrusions. But it is very difficult to have a precise and complete vision about these intrusions and there is no agreed classification of them. Indeed, each researcher tries to classify the intrusions on basis of his/ her own under-study specification. This study intends to introduce the primary concepts of the networks and the intrusions and threats that disrupt the network security. After the introduction of the primary concepts, we will analyze the security of the computer networks and wireless networks. Then we will explain the firewalls that are important ways of improving the networks security. Finally we will provide some suggestions to increase the safety factor of the networks and to reduce the intrusions.
[Salhiy H, Lotfi B. **Network Security; the Concepts, Challenges, and Solutions for Improving the Network Security**. *J Am Sci* 2012;8(1s):79-86]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 13

Keywords: Network Security, Wireless Networks, Firewall

1. Introduction

Networks security is one of the key and most important elements for any network. If you do not know on what you are going to protect your assets, then you will never manage to do such a protection. The computers need to be protected against the threats. But what are these threats? To put it simple, the dangers are conceivable when a threat misuses an available weakness to damage a system. So, if we know the threats, then we can create some plans and methods to encounter those threats and to reduce the vulnerability of the system. The companies and organizations are mainly dynamic and ever-changing. Hence their security plan has to be continually updated. Moreover, whenever the organization undergoes major structural and/ or functional changes, it has to revisit its security plan. So, even if the organization moves to a new building, it has to revise all its new devices and everything that is changed due to such a movement. Network security includes protecting the computational resources, prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Designing a secure network requires a combination of error-tolerant systems and solutions. Such a solution for the organizations is mainly to use Network Access Control (NAC) to control the accessibility to their networks [1]. Most computer-related threats are transferred and spread through the network. When a network is intruded by the internet threats, if the threats do not be stopped, they would affect and hurt other computers and users. The organizations have to pay a special attention to the security of their computer networks. Different internet threats exist on the internet such as the viruses, malwares, spywares, adwares, trojans, etc. Among the most common threats of the computers one can point to the malwares and spywares. These are just few problems of the computer network security that can seriously hurt the security of the organizations.

2.Literature review

2.1.Concepts of network security

Security is a complicated concept with simple principles. In many cases, the very simplicity deceives us and makes the perspective of our activities vague. It is to be mentioned that the security is a multilayer process. The type and the way of defining the defensive layers can be determined and provided only after the evaluations completed. The main priority is to provide a list of the executive policies on the bases of what is more important and easier for the organization. After the priorities are confirmed, each of them has to be implemented promptly. Security evaluation is a very important part of the security programming. No executive plan can be implemented properly without the evaluation. Security evaluation specifies the main guidelines for the implementation of the security plan in order to protect the assets against the threats. Network security is a process by which a network will be secure against all types of internal and external

threats. Following steps have been suggested for creating the security:

1. To determine the part that is going to be protected;
2. To decide on the things that we have to protect the relevant part against them;
3. To decide on the way of the threats;
4. To implement the facilities that can protect your assets in an economic way;
5. To review the process and its improvement in case of finding any weakness;

In any modern network, there are several resources for the protection. Table 1 introduces a set of network resources to be protected against all types of the intrusions.

Table 1. Different types of network resources

#	Different types of network resources
1	Network equipments such as the routers, switches, and firewalls
2	The information of the network operations such as the routing tables and the configuration of the accessibility list that are saved on the router
3	Intangible resources of the network such as the speed and bandwidth
4	Information and informational resources that are connected to the network, such as databases and data servers
5	The terminals that are connected to the network to use the different resources
6	The transferring and exchanging data on the network on any time
7	The privacy of the users' operations and their using of the network resources to prevent identifying the users

The above set is regarded as the assets of any network.

2.2. Intrusion and risk analysis

The intrusion is a risky or non-risky attempt to use or change an accessible resource on the network in a way that such a use has not been considered as its normal use. The network intrusions can be divided into three general groups:

1. Unauthorized access to the resources and data through the network
2. Unauthorized manipulation of the information on the network
3. The intrusions that lead to the disruption in the provided service, known as the Denial of Service

The key term in the two first groups include the unauthorized activities. It is on the network security policy to define any authorized and unauthorized activity, but in more general words, we can define the unauthorized access as the attempts of a user to see or change the information and data that are not relevant to him. The information on the network includes the information available on the computers that are connected to networks such as the servers of the databases and the web, exchanging information on the network, and the information exclusive to the network parts that are going to do the activities like the routing tables of the routers. The network resources can include the terminal equipments like the router and firewalls, or the connection mechanisms. One of the common issues of the security in computer networks is the denial of service intrusion in which the intruders attempt to make the services and data of a system inaccessible, thus when the users try to use the system for their authorized objectives, the system is too busy to response the request of its authorized users. In recent years, DdoS intrusions have targeted the accessibilities on the internet. The first case of such intrusions happened on February 7th 2000 in which Yahoo was targeted, so that its portal was inaccessible for three hours. Moreover, on February 8th 2000, CNN, eBay, Buy.com, and Amazon websites were targeted by the intruders led to the complete collapse or significant slowing [14]. According to the reports, during the 3 hours of the intrusion to Yahoo, this company lost more than 500,000 dollars of its commercial and advertisement benefits. Besides, in recent years, DdoS intrusions are increasingly used by the swindlers and commercial competitors on the websites of the banks, commercial companies, online agencies, retailers, public sectors, and event on the websites of the providers of the internet security services. For example, in March 2005, five Holland hackers were arrested for doing the DdoS intrusion to the public websites in protesting against the offered plans of the government [3] [4]. The activities of the hackers made the public websites inaccessible for 5 days. As specified by the annual report of the Sisco corporation (figure 1), the Denial of Service intrusion is one of the most important threats against the computer systems that is being increasingly extended.

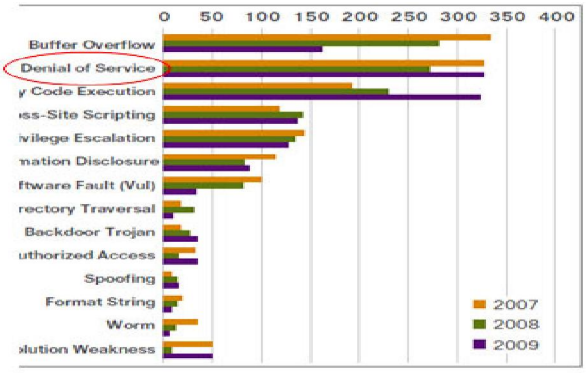

Figure 1. Important vulnerabilities and threats of the computer systems

After determining the threatening factors we have to evaluate different risks. The best case is to protect the network against all errors. But such a best case cannot be fulfilled easily and inexpensively. Accordingly, we have to have a proper evaluation of the different types of the threats so that we can identify their most important ones on the one hand, and to detect other sources that have to be protected against such threats on the other hand. Two main factors in risk analysis are as follow:

1. The probability of the intrusion
2. The damages to the network in case of any successful intrusion

After the risk analysis, we have to define our network security policy so that the probability of the risks and the scale of the damages are being minimized. The security policy has to be public and overall. It does not deal with the details. The details would be changed in short time, but the general principles of the network security that forms its policy have to be fix and stable. Indeed, the security policy plays three main roles:

- What has to be protected and why
- Who has to be the responsible for the protection
- Makes the grounds to resolve any probable confliction

Security policies can be divided into general groups:

- Permissive: whatever is not specifically forbidden is authorized.
- Restrictive: whatever is not specifically authorized is forbidden.

Usually the idea of the restrictive security policies is better and more suitable than the permissive ones because the permissive policies have several security problems and we cannot consider all unauthorized cases. The involved elements in the security policy are listed and provided in RFC 2196. When the security policy is defined, we have to begin its implementation as a network security plan. The constitutive elements of the network security policy are shown in table 2.

Table 2. Constitutive elements of any network security plan

#	Different types of network resources
1	Security features of any device, such as the admin password
2	Firewalls
3	VPN integrators for remote access
4	Intrusion detection
5	Security servers
6	Remote access and access-restrictive mechanisms for the different devices of the network

2.3. Security zones

Defining the security zones plays an important role in establishing a secure network. Indeed one of the best defensive methods against the network intrusions, designing regional and typology-bases network security. One of the most important ideas on its use in the modern secure networks is to define the zones and to separate the different zones of the network from each other. The equipments installing in each zone have different needs and thus each zone provides the protection of each package depending on the security requirements of the installed equipments on that zone. Moreover, zoning a network will lead to a higher stability on that network.

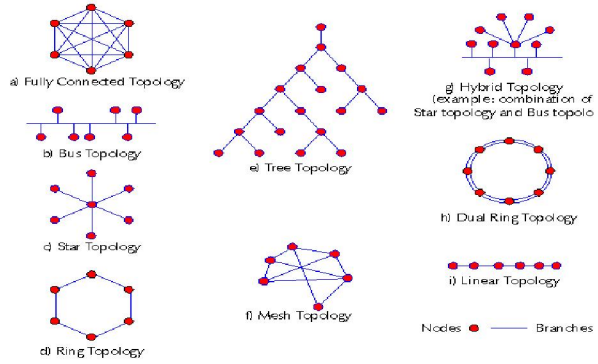

Figure 2. Different types of network typology

The security zones are defined based on the following strategies.

A. The equipments and devices that have highest rate of need (private networks) are placed in the most secure zone. These networks are not usually accessed to the public or accessed from the other networks. The accessibility to these networks is controlled by a firewall and other security facilities such as Secure Remote Access (SRA). The authorized or unauthorized identification is highly monitored and controlled in this zone.

B. The servers that can be accessed just by the internal users are placed in a secure, private, and separate zone. The access to these equipments is controlled by firewall and the accesses are completely monitored and logged.

C. The servers that have to be accessed from a public network are placed in a separate zone without make it possible to access to the more secure zones from these servers.

D. Using firewalls in a layering form and using different firewalls will make it possible to save the overall network in case of any security problem in one of the firewalls. Besides, such a strategy will reduce the need to use the backdoor.

3. Security of computer networks

The security of computer networks is one of the most important problems. The most important base for establishing a network next to the proper hardware configuration is the issue of assuring the network security. Protection, support, and maintenance of the computer data, important information, sensitive programs, needed softwares, and any important data on the memory stick of the computer is called the computer security. The idea of network security intends to meet three important factors that form the security triangle. These factors include the followings:

- Confidentiality and trusteeship
- Integrity
- Accessibility

These three factor (known as CIA) form the fundamental principles of the information security in the network, so that all needed strategies to secure the network or the equipments all are based on the need to apply these three parameters in the maintenance and information exchange environments [10]. Confidentiality and trusteeship means that the information is just accessible to the persons who need it. For example, losing this security feature can be compared to the lost of a part of a confidential file of a company and the accessibility of the press and newspapers to it. Integrity is a concept relating to the systematic sciences and in sum, integrity can be defined as follows: the changes in the information has to be done by some specific authorized persons and processes, and even the authorized persons or processes have not to make any change without the authorized reason or permission. Information integrity has to be preserved both inside and outside the system. That is, any specific data, either inside or outside the system has to be integrated, and if this piece of that undergoes some changes, the authorized persons inside and outside the system has to know it simultaneously. The parameter of accessibility guarantees the continual accessibility of the information system. Thus even if all security points are considered well while some factors (like the like the loss of power) make the system down, then we cannot claim that such a system is secure.

The security in the network is being fulfilled in two ways:

a. Software programs
b. Hardware parts

At best, software programs and hardware parts are used simultaneously. Software programs usually include firewalls and anti-malware programs (malwares include viruses, worms, Trojan horses, adwares, etc.). Hardware parts generally include firewalls. These parts control the input and output ports of the computer and provide some visions about the intruders, especially the special signs of the intruder. Don't forget that as the best seller provider of the operation systems, Microsoft is equipped with a firewall program by default. This program can provide its OS users with a level of security. But it is obvious that the Microsoft software is not sufficient for securing the computers. So at the first step of securing a network, it is necessary to equip the organization with a strong anti-malware program that is able to be updated so that it can show a suitable reaction against the intrusion of the malware programs. Antivirus program can be a good option in this regard because this program is able to update itself continuously and the program itself is upgraded and edited each six months in order to have a more optimized and stronger search engine to find the malware programs. It is highly recommended to use the original version of this program because in the cases of any problem, the original company will support your device promptly.At the second step of the network security we have to use the divider apparatus. Divider apparatus is classified into two models: one adjustable and configurable model, and an on-adjustable and un-configurable model. It is possible that some parts exist in the first group handling some settings of the configuration, but they are not fully equipped with the facilities of the parts of the second group. This divider apparatus usually produced in Core model and they are provided to connect the central service providers to each other to the internal network or to the internet world. They are placed in the main layer of the network connection division from the side of the central service providers to the internal clients, vice versa. This part can prevent the reproduction of a malware programs and the log-in and log-out of the hidden intruders within an internal networks, from one computer to the another one. But if the number of the users and service clients of an organization is higher than the number of the output ports of a CoreSwitch central divider, then we can use other dividers that are configurable and economic to control the log-in and log-outs of each category or unit. For the hardware parts, CiscoSwitch is a good option that has captured the best global brand to itself in this field and plays an important role in this regard by its capability of upgrading its parts and training its experts.

At the third step of the securing, we will require to purchase the software program or the hardware part of the firewall. Hardware part is more important in this step because it is more stable, more powerful, and it has fewer problems than the similar sofwares. The hardware part has to be installed at the very beginning of the path of internet to the organization, i.e. where the insecure internet is injected to an organization. We suggest Cisco ASA or Astaro Firewall. Don't forget that using both hardwares in

parallel is absolutely the best case because if one of the parts is down or stopped, the other one can manage and control the inputs and outputs. But in the software programs, we need to install a software on the central service provider of the firewall because the insecure internet is being entered into the organization just through this central service provider. We have to know that the organization has to use special hardware parts so that the routers can be placed before and after that hardware part. Again we suggest using Cisco ASA parts within the internal wall and after the routers part.At the fourth step of securing the network, we need another hardware part, namely the router of the internal network. This part is able to be configured to show the rout of the inputs and outputs, internet subscriptions, adjusting the inputs and inputs of the firewall, and the exit of the information in form of the internet from the organization to the urban or inter-urban computers vial the phone lines etc. again we suggest the products of Cisco Company. At the next step of the network security, the organization needs to have the needed equipments for adjusting the electricity, and the backup apparatus for supplying emergency electricity power to make it possible to provide full-time and non-stopped services and to adjust the electricity power for all hardware parts of the network including the dividers, routers, and service providers. Due to the possible risks of electricity lost such as losing the data of the service providers, dividers and routers this system is very important. The last step of securing the network is to capture a backup of all information and files of the main software programs on a backup service provider. This is the last layer of inter-organizational network security.

3.1. Security in wireless networks

Since current wireless networks are increasingly developing in our today world, and since the nature of these networks is based on the radio signals, thus the most important point in using such a technology is to know their weaknesses and strengths. Considering the necessity of knowing the risks of using such networks, we can reach an accepted level of security by proper configuration. Thus in part we are going to deal with the security in wireless networks. Three securing methods in wireless networks are as follow:

Wired Equivalent Privacy:

In this method, the communication of the unauthorized users is blocked. This method is suitable for small networks because it require manual settings (KEY) in each client. The encoding base of WEP is used in this method by RSA on the basis of RC4 algorithm.

Service Set Identifier:

WLAN networks have several local networks each of which has a unique identifier. These identifiers are being placed in several access points. To access the relevant network, each user has to do the settings of SSID of the identifier.

Media Access Control:

In this method, a list of MAC addresses that are used in a network is entered into the relavant Access Point (AP), thus only the computers are allowed to access that have these MAC addresses. In other words, when a computer sends a request, its MAC address is getting compared with the relevant MAC address in the AP and then its permission to access is investigated. This securing method is also suitable for the small networks because in large networks it is very difficult to enter these addresses to the AP [6].

3.2. Security weakness in wireless networks

The common risk in all wireless networks - regardless of their protocol or relevant technology- is based on their dynamic structure in using radio signals instead of the wire and cable. Using these signals, the hackers can pass the security barriers of these networks and the network structure to show themselves as the members of these networks and if they succeed to do so, they can access to the vital information, attack the service providers of the organization, ruin the data, disrupt the communications of the network nodes with each other, produce fake and misleading data, misuse the effective bandwidth of the wireless network, and other malware activities.

By and large, the following security facts are common in all groups of wireless networks:

- All security weaknesses of the wired networks are also true about the wireless networks. Indeed, not only there is no dimension of the design and structure exclusive to the wireless networks that can lead to a higher level of security, but as mentioned earlier, this group of the networks is sensitive against some more risks.
- Passing the security barriers, the hackers can easily access to the information resources of the computer systems.
- Those critical data that are not encoded or their encoding is not enough secure and are transferring between the two nodes of wireless networks can be theft and changed by the hackers.
- DoS intrusions to the wireless equipments and systems are very common.
- Stealing the passwords and other security elements, the hackers can connect to their needed

networks like the authorized users of the wireless networks without any barrier.

- The hackers can steal the needed security elements to monitor the users while accessing to other important data of the users.
- Portable computers which can and are permitted to use wireless networks can be easily stolen. If the hackers steal such hardwares, they have managed to take the first step to intrude the network.
- Any hacker can use the common points between a wireless network in an organization and its wired network (that is usually the main and more sensitive network) and hack the wireless network to find a way to access to the resources of that wired network.
- At another level, the hackers can disrupt the performance of the entire network by hacking the controlling elements of a wireless network.

3.3. Firewall

Firewall is a software-based or hardware-based system that helps keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted. In this structure, any organization that wants to control its incoming and outgoing data has to cut all direct communications of its internal network with the external world and all these communications will be done through a gate that is called firewall. All TCP and IP packets have to be entered into the firewall before coming to or going out of the network to be processed according to the security and protecting criteria.

Table 3. Objectives of establishing firewalls

#	Objectives
1	To manage, maintain and control the policies and services that are provided on the networks separately from each other
2	To selecting the internal services that are provided for outside of the network, vice versa
3	To control the security and to manage the users' accessibility
4	To protect the information before the hackers who are going to intrude the internal network

High capable networks use professional hardwares to connect to the internet, but there are some softwares that have been produced for this goal and that are installed on the PC systems. Firewall software is absolutely necessary to have a suitable and secure connection to the internet. SP2 of the XP Windows had this capability and had a high security to connect to the network. Moreover, it is recommended to use proper antivirus softwares besides using firewall to connect to the internet network.

Figure 3. Way of establishing the firewall

Different types of the firewalls usually have more or less the mentioned functionalities. But the way of fulfilling such functionalities by the firewalls is different from each other. These differences lead to different levels of performance and security of the firewall. In this regard, firewalls are classified in five groups as follow:

a. Circuit- Level Firewalls: these firewalls operate as a relay for the TCP connections. They disconnect the TCP connection with the backup computer and instead, they response the primary computer themselves. Just after the establishing their own connection they allow the flow of data toward the target computer. In this connection, only the relevant data packets are allowed to pass. This group of firewalls don't read the data of the information packets, thus their speed is high [17], [18].
b. Proxy Server Firewalls: proxy server firewalls analyze the data packets within the application layer. A proxy server cuts the requests that are provided with its back applied program and

instead, sends the request itself. On the other hand, the proxy server firewall receives the reply of the request first and then it sends it to the applied programs itself. This method prevents the direct connection of the programs with the servers and external applied programs to provide a high rate of the security. Since these firewalls do not recognize the user- level protocols, thus they can impose some restrictions on these protocols. Moreover, they can analyze the contents of the data packets to impose the needed restrictions. Of course this level of analysis can lead to the low speed of these firewalls. Besides since these firewalls have to process the incoming traffic and the information of the applied programs of the user, their efficiency is reduced. In most cases, the proxy servers are not clear for the final users and the user has to make some changes in the program to apply these firewalls. Each program that wants to use pass kind of firewall has to make changes in the stack of the firewall protocol.

c. Not-stateful Packet Filters: this filters have a simple function. They are placed in the path of a network and use a series of the principles to allow some packets pass and block some others. These decisions are made on the basis of the available information about the addressing in some protocol layers such as IP and in some cases on the basis of the available information in other protocol layers like the TCP ad UDP. These filters can work well when the users have a good vision about the application of the services needed for the protection of the network. Additionally, these filters can be rapid because they do not operate like the proxies and they do not have any information about the protocols of application layer.

d. Stateful Packet Filters: these filters are smarter than the simple filters. They block almost all incoming traffic but they can let their stack machines to respond. They do so by preserving the connection logs that their stack machines had generated in the transferring layer. These filters are the main mechanism for using in order to implement firewall in modern networks. These filters can log all traces of different information through the transferring packets. For example, the source and target UDP and TCP port numbers, TCP numbers, and TCP flags are all logged. Many new stateful filters can detect protocols of application layers such as HTTP and FTP, thus they can control the accessibility on the basis of the needs and speed of these protocols [17] [18].

e. Personal Firewalls: personal firewalls are the firewalls that are installed on personal computers. They have been designed to encounter the network intrusions. These firewalls are usually aware of the running programs of the machine and only allow the communications of these programs. Installing a personal firewall on a PC is very useful because the offered level of the security of the firewall will increase the network security. On the other hand, since many new intrusions are being done from the within of the protected network, the network firewalls cannot anything with them, thus the personal firewall can be very useful. Usually, there is no need to change the program to pass the installed personal firewall like the proxy.

4. Solutions for increasing the security of the systems

Operation systems in specific and all softwares in general have several security holes. By passing the time, these holes can be easily discovered by the hackers. Discovering these security holes, the producers of the softwares design some patches for repairing these holes and provide these patches to the users of their own softwares. If you want to prevent the hackers' intrusions to your computer, download the latest security patches from the website of the producer of the operation system and other softwares such as Office, and install them on your computer. The following points are suggested for increasing the security of your computer:

- Study the needed level of the security of computers considering the saved data on them, their environment, and the cases and methods of their use and application;
- Study the available settings of the computers and detect their vulnerabilities and security holes using new and professional programs;
- Do all needed settings and install all needed programs in order to improve the logical security of the computers and apply any needed security for the files
- Control the users' accessibility to the files on the basis of the following points:
  - Read only
  - Read and edit
  - Read, edit and delete
  - Read, edit, delete, and control the accessibility of the other users
- Log and record the accessibility of the users to the determined files (e.g. to detect the user who edits specific files), and encrypt system files in order to prevent the access of other users (even the network admin) to those files.

5. Conclusion

The goal of network security is quite simple. The goal of the network security is to protect the

network and its related parts and to prevent any unauthorized access or misuse of the network. One of the practical solutions of having a secure network in an organization is to pay enough attention to the necessity and importance of the threats as well as protecting the organization against the attacks and intrusion. To have a higher rate of network security, the organizations have to use preventive tools and know that how these threats can be reduced and how the communicational routs can be controlled.

The following suggestions can protect the organizations against the security threats to some extent. To be sure about the security of the computer networks, the organizations have to consider the following points:

- Using updated knowledge on the security threats of the network
- Knowing the fact that the websites of social networks can be a gate for the new internet threats
- Using suitable and proper security settings
- Installing a suitable firewall to prevent unwanted network traffic
- Using NAC for protecting and securing the data and other IT resources
- Making IDPS for having a higher emphasis on the security
- Considering security policy
- Training the employees and making them aware of the importance of the network security

Corresponding Author:
Mr. Houshang Salhiy
Institute for higher education "hakim nezami Quchan iran
E-mail Houshang_salhiy@yahoo.com

Resources

1. Borg , J. .A Comparative Study of Ad Hoc & Peer to Peer Networks.; University College, London, 2003.
2. Ramanathan, R.; Redi, J. .A Brief Overview of Ad Hoc Networks: Challenges and Directions.; IEEE Communications, no. 50th Anniversary Commemorative Issue, 2002; pp 20-22.
3. Stamouli, Ioanna.Real-time Intrusion Detection for Ad Hoc Networks.; University of Dublin, 2003.
4. Patwardhan, A.; Parker, J.; Joshi, A. .Secure Routing and Intrusion Detection in Ad Hoc Networks.; University Of Maryland, 2003.
5. Zhang, Y.; Lee, W. .Intrusion Detection onWireless Ad Hoc Networks.; in Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom.00), 2000.
6. Anjum, F.; Subhadrabandhu, D.; Sarkar, S. Signature-based Intrusion Detection for Wireless Ad-Hoc Networks"; In Proceedings of Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, 2003
7. Deng, H.; Zeng,, Q. A.; Agrawal, D. P. SVMBasedIntrusion Detection System for Wireless Ad Hoc Networks; In Proceedings of the IEEE Vehicular Technology Conference, 2003.
8. Brutch, P.; Ko, C. .Challenges in Intrusion Detection for Wireless Ad Hoc Networks; Proceedings of the Workshop on Security and Assurance in Ad-hoc Networks in Orlando, 2003.
9. Tseng, C. Y.; Balasubramanyam, P.; Ko, C.; Limprasittiporn, R.; Rowe, J.; Levitt, K. .A Specification based Intrusion Detection System for AODV.; In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003, pp. 125.134. ACM Press,.
10. Wang, B.; Soltani, S.; Shapiro, Jonathan K.; Tan, P. N. .Local Detection of Selfish Routing Behavior in Ad Hoc Networks.; Department of Computer Science and Engineering, Michigan State University, 2004.
11. Thomer M. Gil, "MULTOPS: a data structure for denial-of-service attack detection", Ph.D. Thesis, Vrije University, Dec 2000.
12. Jelena Mirkovic, "D-WARD: Source-End Defense Against Distributed Denial-of-Service Attacks", Ph.D Thesis, University of California, Los Angeles, 2003.
13. Vrizlynn Thing Ling Ling , "Adaptive Response System for Distributed Denial-of-Service Attacks", Ph.D. Thesis, College London, Aug 2008.
14. Jelena Mirkovic, Janice Martin and Peter Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms", Computer Science Department, University of California, 2002.
15. Christos Douligeris ,AikateriniMitrokotsa , DDoS attacks and defense mechanisms: classification and state-of-the-art", 13 October 2003, Available from: http://www.sciencedirect.com.
16. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE, "Distributed Denial of Service Prevention Techniques", April 2010.
17. Karthikeyan .K.R and A. Indra, "Intrusion Detection Tools and Techniques –A Survey", International Journal of Computer Theory and Engineering, Vol.2, No.6, December 2010.
18. JelenaMirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", funded by DARPA, University of Delaware and University of California, 2004.
19. Abraham Yaar, Adrian Perrig, Dawn Song, "Stack Pi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", IEEE Journal, Carnegie Mellon University, Vol. 24, Oct 2006.

11/22/2012