SURVEY ON NETWORK ATTACKS AND MALWARE

[1]S.Shunmuga Priya, [2]Aiswarya.S, [3]M.Birundha
[1]Assistant Professor,
[1,2,3]Department of Computer Science and Engineering,
Sri Krishna College Of Engineering and Technology
Coimbatore, India.
[1]shunmugapriyas@skcet.ac.in

Abstract

Network is defined as a group of two or more computer systems linked together. It is a telecommunication network which allows nodes to share resources. When resources are being shared in a network, there arises the threat to the data being transmitted. This paper describes the various attacks that are launched during the transmission of data or while sharing resources in a network. It also describes the cause and effect of each attack. Further, the paper involves how each attack can be dealt with, by providing the proven solutions.

I. INTRODUCTION

Network is defined as a group of two or more computer systems linked together. It is a telecommunication network which allows nodes to share resources. In computer network, networked computing devices exchange data with each other using a data link. Components of a communication system include sender, receiver, message , transmission medium and protocol. Connections between nodes are established using either wired cable (coaxial, twisted pairs, optical) or wireless. Network computing devices that originate , route and terminate the data are called network nodes. Nodes can include hosts such as personal computer , phones , servers, etc. Network categories include LAN (Local area network),MAN(Metropolitan area network) and WAN(Wide Area Network). Routing is the process of selecting network paths to carry network traffic. Applications of network include E-mail(outlook express, opera, Mozilla thunderbird),Groupware (videoconferencing, chatting),Standalone applications(Word processors, spreadsheets, DBMS, Presentation graphics),TELNET and FTP, an application facilities transfer of files from one computer to another.

However, while a user transmits data to a destination via network, there arise the chances of his data being captured by a third party. Hence an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Some attacks are physical, i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker.

The consequences of a successful attack include unauthorized disclosure whereby sensitive data is directly released to an unauthorized entity, gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk that holds the data, a threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity, altering or replacing valid data with false data that serves to deceive an authorized entity, incapacitation wherein any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources.

The need for protecting data is of growing importance due to the increasing reliance on computer systems and the Internet , wireless networks, and the growth of tiny devices as part of the Internet of Things. Increased risk of intrusion is also another concern. The attackers use the information available to them in order to exploit weaknesses in the user/organization's security, which in turn puts the data that the user entrusted to

that organization in jeopardy. Further, data volume has been growing exponentially, dramatically increasing opportunities for theft and accidental disclosure of sensitive information. The loss of sensitive data and other forms of enterprise information can lead to significant financial losses and reputational damage. When organizations fail to take the necessary steps to identify sensitive data and protect it from loss or misuse, they are risking their ability to compete. Whether it's a targeted attack or an inadvertent mistake, confidential data loss can diminish an organization's brand value, and irreparably damage the organization's reputation.

II. ATTACKS TARGETING MESSAGE

A. Packet Capturing Attack

Capturing packets of data flowing across a computer network. The software or a device used for this purpose is called a "Sniffer". It deals with capturing data like passwords, IP addresses, and protocols. Packet Sniffer sniffs without modifying the network's packets in any way. A firewall sees all of computer's packet traffic as well, but it has the ability to block and drop any packet that it's programming dictates-Packet Sniffers merely watch, display and log this traffic. Powerful aspect of Packet Sniffer is the ability to place the hosting machine's network adapter into "promiscuous mode", by setting the NIC card. Network adapters running in this mode receive not only data directed to machine hosting the sniffing software but also of all the traffic on the physically connected local network. Items sniffed include SMTP, POP, IMAP traffic, SMB, NFS, FTP traffic, Sql database, HTTP Basic and telnet authentication

Effects of this attack include allowing unauthorized computer user to view traffic destined to someone else. Also it enables the host to read actual e-mail and financial transactions, passwords off the wire in clear text.

B. Black Hole Attack

Also known as Packet Drop Attack-a type of DoS attack in which a router that is supposed to relay packets instead discards them. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. Greyhound attack , in which the malicious router accomplishes the attack selectively i.e., by dropping packets for a particular network destination. If the malicious router attempts to drop all packets that come in, the attack can be discovered fairly quickly through common network tools such as trace route. This attack is deployed majorly in attacking wireless and ad hoc networks. In wireless, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised and host is able to drop packets at his will. In mobile and ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive other hosts on the network.

Effects of this attack include degrading the TCP performance due to malicious packet dropping. Applications such as FTP, HTTP and telnet building on top of TCP achieve reliable data transmission. Nevertheless, these applications face a threat if an intruder on the data path maliciously drops TCP data packets- called TCP dropping. Thus quality of service of the applications can be degraded drastically under such an attack.[3]

C. Spoofing Attack

A spoofing attack is when a malicious party impersonates other device/user on a network to launch attack against network hosts, steal data, spread malware or bypass access control .Consists of Internet Protocol Spoofing and Address Resolution Protocol Spoofing.

IP Address Spoofing:

Attacker sends IP packets from a false source address in order to disguise itself. It involves flooding a selected target with packets from multiple spoofed addresses by sending a victim more data than it can handle. Spoof target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from target's IP address, all responses to the spoofed packets will be sent to(and flood) target's IP address. Effects include drastic collision or reduction in the overall routine of wireless network.

ARP Spoofing:

ARP is a protocol to resolve IP address to MAC address for transmitting data. Malicious party sends spoofed ARP messages across a LAN in order to link the attacker's MAC address with IP address of legitimate member of the network. This results in data that is intended for the host's IP address getting sent to attacker instead. The effects of this attack include steal into, modify data in transit or to stop traffic on a LAN. Further this attack can be launched only on LAN that uses ARP.

III. ATTACKS TARGETING RESOURCE

A. Denial of Service Attack

Machine or network resource unavailable to its intended users by disrupting services of a host connected to the internet. Flooding targeted machine or resource with superfluous requests in an attempt to overload system and prevent some or all of the illegitimate requests from being fulfilled. Often target site or services hosted on high profile web servers such as banks or credit card payment gateways are the victims. In MyDOOM, tools are embedded in the malware, and launch their attacks without knowledge of the system owner. DoS level 2 attack is to cause a launching of a defence mechanism which blocks the network segment from the attack originated. Teardrop Attack involves sending mangled IP fragments with overlapping, oversized payloads to the target. In an amplified DNS DoS attack, attacker generates crafted DNS requests that appear to have originated at the victim's network and sends them to misconfigured DNS server managed by third parties.

Effects of this attack include attempt to disrupt or degrade the functioning of the whole network or harm a specific node. These attacks are at the routing or MAC layer.The former results in a disruption of routing functionalities while the latter could potentially disrupt channel access and cause wastage of resources in terms of bandwidth and power[1]

B. Sybil Attack

An attack subverted by forging identities in peer-to-peer networks. Involves creating large number of pseudonymous identities, using them to gain disproportionately large influence.An entity on a peer-to-peer network is a piece of software which has access to local resources. A faulty node or an adversary may present multiple identities to peer-to-peer network in order to appear and function as multiple distinct nodes. After becoming part of the network, the adversary may then overhear communication or act maliciously. A reputation system's vulnerability to a Sybil Attack depends on how cheaply identities can be generated, the degree to which reputation system accepts input from entities that do not have a chain of trust linking them to a trusted entity [2].Sybil Attacks are deployed in sensor and ad hoc networks.

This type of attack can affect the fabric of internet commerce and communication.

C. Distributed Denial of Service Attack

A Distributed Denial of Service (DDoS) attack is a large scale attack , which is typically launched indirectly with the help of other computers in the network. There are several kinds of DDoS attacks. There are two main classes: bandwidth depletion and resource depletion attacks. In case of bandwidth depletion attack, the victim network is flooded with unwanted traffic that prevents legitimate traffic from reaching the victim computer. In the resource depletion attacks, the attack is targeted to tie up the resources of the victim computer [13] [14]. A new kind is DDoS Reflector attack - a kind of attack which is difficult to defend as the victim computer is flooded with traffic from other Internet servers, which cannot be compromised.

This type of attack can affect the normal operations performed by the system. And in IOT(Internet Of Things) -the wide variety of smart devices faces the difficulty of securing overall privacy.

D. Worm Hole Attack

The wormhole attack is a severe attack in ad hoc networks which is particularly challenging to defend. This is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In this attack, an attacker records packets at one location in the network, tunnels them

selectively to another location, and retransmits them into the network.

This type of attack is common in AODV(Ad-hoc On Demand Distance vector) and DSR (Dynamic Source routing). This can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems.

E. Session Hijacking

The Session Hijacking attack is the exploitation of the web session control mechanism, which is normally managed for a session token. Since http uses many different TCP connections, the server needs a method to recognize every connections. The most useful method depends on a token that the Server sends to the client browser after the authentication of the client. A session token is composed of a string of variable width and it can be in different ways like URL, in the header of the http as a cookie, in other parts of the header, or in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Server.

This type of attack is most common on websites to protect the password by encrypting the initial login phase. It is difficult to encrypt everything in Websites. This leaves the client vulnerable.

F. Phishing

Phishing is far easier to trick someone into clicking a malicious link in a legitimate email than trying to break through a computer's defences. To make their messages look genuine from a well-known company, logos and other identifying information are taken from that company's website is included. The malicious links that are in the body of the message are designed to make it appear that they go to the spoofed organization. The use of subdomains and misspelled URLs are common tricks- URLs created using different logical characters to read exactly like a trusted domain. Some scams use JavaScript to place a picture over a browser's address bar. Phishing is popular with cybercriminals

The attack is mostly on the social events like year's major events, holidays and anniversaries, breaking news stories, both true and fictitious.

G. Brute Force Attack

A attacker trying many passwords or passphrases of eventually guessing the password of a target system or device correctly. The attacker systematically checks all possible passwords and passphrases until correct password is found. It is a cryptanalytic attack used to attempt to decrypt and encrypt data. It is used when it is not possible to take advantage of other weaknesses in an encryption system. Used for only short passwords.

This attack is most common on phones, laptop devices, mail-id passwords to steal some credential information.

IV. MALWARE

A software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, as for example Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is often disguised as, or embedded in, non-malicious files.

A. Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth. Any code designed to do more than spread the worm is typically referred to as the "payload". Typical malicious payloads might delete files on a host system (e.g., the ExploreZip worm), encrypt files in

a ransomware attack, or exfiltrate data such as confidential documents or passwords. Probably the most common payload for worms is to install a backdoor. This allows the computer to be remotely controlled by the worm author as a "zombie". Networks of such machines are often referred to as botnet and are very commonly used for a range of malicious purposes, including sending spam or performing DoS attacks.

Major functionalities of worms include using a compromised machine to spread through instant messaging, mails, sharing etc., disclosure of private or sensitive information to the hacker ,deleting files and folders of hard drive without the administrator knowing about it,causing software instability making the software showing errors whenever opened, hanging of software or closing down without any reason.

B. Trojan Horse

A malicious computer program which is used to hack into a computer by misleading users of its true intent. generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.This infection allows an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). If installed or run with elevated privileges a Trojan will generally have unlimited access. What it does with this power depends on the motives of the attacker.

Effects on the attack of Trojan horse include data corruption,formatting disks, Spreading malware across the network, Spying on user activities and access sensitive information,Use of the machine as part of a botnet(to perform automated spamming or to DDos attack),Using computer resources for mining cryptocurrencies,Using the infected computer as proxy for illegal activities and/or attacks on other computers and Infecting other connected devices on the network.

C. Virus

A virus is a self replicating program that attaches itself to an executable file or software, and then gets activated as soon as you run that software and that spreads over the system over all the files and folders and corrupt the data present within it. It is designed to corrupt its target computer and even the simplest ones can corrupt data on your PC, reformat your hard disk, or bring your system to a halt.

A computer virus always requires human interaction to be triggered and to spread to others, and is often transmitted through email attachments and internet downloads.

Effects of virus involve permanent infections that exist in a computer's RAM memory. These are capable of interrupting operating system to execute, Can corrupt files and programs that are opened, closed, renamed or copied, Overwrite viruses infected files then delete the information stored in the infected areas, makes the infected files unusable, activating themselves only when the program is executed, Directory viruses altering directory paths, changing the location of files. A boot virus may infect computer's hard drive, making it unable to boot up.

D. Ransomware

Ransom ware is a type of malware that holds your valuable data and then demands payment for its release. This usually enters your system through Trojans or redirected ads. The entry method may differ but the result is a locked down computer system or inaccessible or encrypted data. Only the payment of ransom can bring your system or data back to its original state. This is common malware to hit the cyber crime in the recent years.

Effects of this malware is majorly on corruption of data.

The areas that are affected by Ransom ware are Healthcare where patient records are made inaccessible, lab records resulting in delay, medical devices inoperable and prescriptions being postponed.

E. Spyware

Spyware is the software installed on your computer without your knowledge that are designed to track your browsing and internet activities. The

information is then collated by a central server and used for targeted advertising.

Effects of Spyware includes Theft of credential data or information from your system or mail, Sending spam messages to the contacts in your mail, Some to capture every keystroke and mouse click, allowing hackers to follow you around the Web, as you log in to your bank account or other important sites.

V. WAYS TO OVERCOME

A. Packet Capturing Attack

1) Solution I: The only real solution for this type of attack is encryption. The detection solution is tomonitor ARP traffic on your network and detect when ARP entries are being changed. You can use a product such as an ARP watch[5].

2) Solution II: Utilise enhanced switch network sniffer detection based on IP packet routing and ARP cache position detection techniques for sniffer detection.

a) Phase I: Find out the nature of environment in which sniffer detection process is invoked. Done by running sniffer detector NIC in promiscuous mode for 30-60 seconds.

*b) Phase II:*Invoke appropriate detection technique if network is broadcast in nature then ARP cache poisoning detection technique is invoked to detect sniffer host. If network is not broadcast in nature, then enhanced switched network sniffer detection based on IP packet routing is invoked to detect a sniffer host.[6]

B. Black Hole Attack

1) Solution I: Sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing network redundancy. Since any packet can be arrived to the destination through many redundant paths, idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time, sender node will buffer its packet until a safe route is identified. Once a safe route is identifies, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destination and wait for another RREP.

Two or more nodes must have some shared hops. From these shared hopes,the source node can recognise safe routes to the destination.[8]

*2) Solution II:*Every packet in MANET has unique sequence number. This number is in increasing value. The node in regular routing protocols will keep the last packet sequence number that it has received and uses it to check if the received packet was received before the same originating source or not.

Every node needs to have two additional small sized tables: One to keep the last-packet-sequence-number for the last packet sent to every node and other to keep the last-packet-sequence-number for the last packet received from every node.

C. Spoofing Attack

1) Solution I: Effective algorithm for the authentication process and filtering of the MAC addresses of the Roger wireless devices. The implementation involves:

Identify the uniqueness of the client address and the other is to make the modification access control point list in each client. Recognising spoofing or mockery of information attack in wireless network in the effective way helps to identify the adversaries using same uniqueness of nodes in wireless network.[9]

2)Solution II: Signal Strength Analysis: RSS represents the transmission power minus signal attenuation, which is correlated to both environment conditions and distance between the transmitter and the amplitude modulation. Assuming the attacker and genuine station are separated by a reasonable distance, RSS can differentiate them and help us detect the MAC spoofing.[10]

D. Denial of Service Attack:

Coordinated automated activity by many hosts need a mechanism to control them. To prevent such attacks, it is therefore possible to identify, infiltrate and analyse this remote control mechanism and to stop it in an automated fashion. This method can be implemented by infiltrated and tracking IRC based botnets, which are the main DoS technology used by attackers today.[4]

E. Sybil Attack

1)Solution I: Resource Testing: If a number of identities possess fewer resources than would be expected if they were independent. This includes checks for computing ability, storage ability, and network bandwidth as well as limited IP addresses.

2)Solution II: Trusted Devices: In a defence related to trusted certification authorities, entities in an application can be linked in some secure fashion to a specific hardware device. Analogous to any central authority handling out cryptographic certificates, there are no specified methods of preventing an attacker from obtaining multiple devices other than manual intervention.[7]

D. Distributed Denial of Service Attack

1) Solution I: New cracking algorithm: Maintain a status table. In that table it keeps the IP addresses of current users and their status. If particular IP address has been signed on for a first time, it makes the status as genuine user. For the 2-4 times it marks as a normal user. For the 5th time it marks the particular user's IP address as attacker. After that, the user cannot get the service or access anything in that particular website. The service is denied for that particular IP address.[15]

2) Solution II: Breaking the DDOS attack chain: The "kill chain" in the Lockheed Martin paper is used to describe a model by which an adversary engages a specific target to further malicious intent Using table of Reconnaissance, Weaponization , Delivery, Exploitation, Installation and command & control[16].

E. Session Hijacking

Use SSL to have secure communication channel, There must be log out function for session termination, Trust HTTPS connection for passing authentication cookies, Adopt a secure protocol, Regeneration of Session ID after log in ,Reduce incoming connections and the life span of session or cookie[17]

F. Worm Hole Attack

Some Modifications has to be done in AODV routing protocol[18] to detect and remove wormhole attack in real world. WADP has been implemented in modified AODV. Node authentication are used to detect malicious nodes and remove false positive problem. It helps in mapping exact location of wormhole and is a kind of double verification.

G. Phishing

*1)Solution I:*Network level protection: Network level protection is usually implemented by not allowing a range of IP addresses or a set of domains to enter into the network[19]. It allows the administrator of that website to block messages from those systems that usually send spam or phishing email. 'Domain name system blacklists' [20], used by Internet service providers (ISP's) is generated and updated by studying traffic behavior. This approach is reactive in nature.

*2)Solution II:*Authentication: Authentication is to filter phishing email to confirm whether the email was sent by a valid path and the domain name is not being spoofed by phisher. Authentication increases the security of communication, at both the user and domain levels. User level authentication is employed through password. However these can easily be broken by increasing phishing attacks. Domain level authentication is implemented on the provider side. Microsoft has introduced a technology called Sender ID [21] for domain level authentication . A similar technology called Domain Key [22] is produced by Yahoo. To be effective, providers on both the sender and the receiver side must employ the same technology.

H. Brute Force Attack

*1)Solution I:*The smart phone equipped with the new keypad[24] increases the time required for brute force attacks by the finder through formation of random buttons, random button arrangement and display delay time. Consequently, the owners are able to secure more time to become aware of the loss or theft and take action.

2)Solution II: The various modules[25]- Locking of Accounts, Time bound Login, Query – Based Authentication, One-Time Password Authentication , Using CAPTCHA, Unique IP address Login can make difficult of Brute force attack.

I. Worms

The use of intrusion detection systems to protect against the various threats faced by computer systems by way of worms. Intrusion detection systems attempt to detect things that are wrong in a computer network or system. IBM Zurich Research Laboratory has developed a system that specifically targets worms rather than trying to prevent all breaches of computer security. Called Billy Goat, the specialized worm detection system runs on a dedicated machine connected to the network and detects worm-infected machines anywhere in it. Billy Goat has been proven effective at detecting worm-infected machines in a network. It is able to detect infected machines within seconds of their becoming infected. Furthermore, not only is it able to detect the presence of a worm in the network, it can even provide the addresses of the

infected machines. This makes it considerably easier to remedy the problem.[11]

J. Trojan Horse

Use network firewall. Firewall can detect, limit, and change data flow passing through the firewall, and protect the information, arrangement, and operation of network to the greatest extent without informing others. Firewall can maintain the network security according this effect. Firewall can be divided into two kinds, one is virus firewall, while the other is network firewall . Network firewall has the function of screening data packages between computer and internet to effectively avoid attack from network. [12]

K. Virus

This includes software vaccines or filters; encryption, access control software (e.g. RACF, ACF2, and Top Secret), "test-to-production" control procedures, back-up and recovery procedures, personnel selection and review controls and physical access control[27].

Identification and authentication, discretionary access controls, process isolation, and auditing are relevant countermeasures for the virus whose mission is to destroy or modify user data.

L. Ramsomware

CryptoDrop[28] focuses on detecting ransomware through monitoring the real-time change of user data. The union of these individual indicators provides a strong measure of suspiciousness of a process. By tracking these indicators and monitoring for this condition in a single running process, we can develop a reputation score that indicates whether the program is likely behaving maliciously. Once a threshold score is reached, CryptoDrop alerts the user and suspends the suspicious process.

M. Spyware

Install an anti-virus software package and keep it updated all times. The most popular brands include Norton, Microsoft Defender, McAfee, Spybot , Search & Destroy, Pest Control,Don't download shareware from unknown sources. Don't click on any pop-up or advertisement for free anti-spyware software.,even if they carry the name and logo of a well-known publisher ,Set your browser and operating system security level to at least the medium setting for best results, Install a firewall , use a separate router in your home network, Avoid questionable Web sites. If a virus alert appears on your screen as you visit a Web site, don't click on it, or close it. Instead, type control-alt-delete to launch the Task Manager and use the "End Task" command to close the window. Use your own anti-virus software to run a complete scan of the system.

REFERENCES

[1]. Vikram Gupta, Srikanth Krishnamurthy, Michalis Faloutsos,"Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks",IEEE.

[2]. Kuan Zhang , Xiaohui Liang ,Rongxing Lu ,Xuemin Shen"Sybil Attacks and Their Defenses in the Internet of Things", IEEE Internet of Things Journal (Volume: 1, Issue: 5), Oct 2014.

[3]. Xiaobing Zhang , S.F. Wu , Zhi Fu , Tsung-Li Wu," Malicious packet dropping: how it might impact the TCP performance and how we can detect it", Network Protocols, 2000. Proceedings. 2000 International Conference on 14 November 2000.

[4]. Felix C. Freiling,Thorsten Holz, Georg Wicherski,"Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks",2005.

[5]. Mohammed Abdul Qadeer , Arshad Iqbal, Mohammad Zahid , Misbahur Rahman Siddiqui," Network Traffic Analysis and Intrusion Detection Using Packet Sniffer", Communication Software and Networks, 2010. ICCSN '10. Second International Conference on 26 Feb,2010.

[6]. Abdul Nasir Khan, Kalim Qureshi, Sumair Khan," An Intelligent Approach of Sniffer Detection", The International Arab Journal of Information Technology, Vol. 9, No. 1, January 2012.I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[7]. Brian Neil Levine,Clay Shields, N. Boris Margolin," A Survey of Solutions to the Sybil Attack",2006.

[8]. Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park, "Black Hole Attack In Mobile Ad Hoc Network ",ACM-SE 42 Proceeding of the 42nd Annual Southeast Regional Conference,Pages 96-97, 02 April,2004.

[9]. S.Raguvaran," Spoofing attack: Preventing in wireless networks", Communications and Signal Processing (ICCSP), 2014 International Conference on 3 April, 2014.

[10]. Y. Sheng , K. Tan, G. Chen, D. Kotz, A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", INFOCOM 2008. The 27th Conference on Computer Communications. IEEE ,13 April, 2008.

[11]. J. Riordan , A. Wespi, D. Zamboni," How to hook worms [computer network security]", IEEE Spectrum (Volume: 42, Issue: 5) ,May 2005.

[12]. ZHU Zhenfang ,"Study on Computer Trojan Horse Virus and Its Prevention", International Journal of Engineering and Applied Sciences (IJEAS)(ISSN: 2394-3661, Volume-2, Issue-8) August ,2015.

[13]. Thomas Dubendorfer, Matthias Bossardt, Bernhard Plattner; Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation; Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17 - Volume 18, 2005.

[14]. Stephen Specht, Ruby Lee; Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures; Department of Electrical Engineering, Princeton Architecture Laboratory for Multimedia and Security, Technical Report CE- L2003-03, May 16, 2003.

[15]. V. Priyadharshini, Dr. K. Kuppusamy, "Prevention of DDOS attacks using New cracking algorithm", IJERA, 2012.

[16].Bryan Harris ,Eli Konikofff , Phillip Peterson, "Breaking the DDOS attack chain" ,August 2013 CMU-ISR-MITS-2

[17]. Laxman Vishnoi, Monika Agarwal, "Session hijacking and its counter measures", IJSRET, AUGUST 2013.

[18]. Juni Biswas, Ajay Gupta, "Wormhole attack detection and prevention techniques in MANET using AODV routing protocol", FEB 2015 in ICIIS(9th conference).

[19]. "A Survey of Phishing Email Filtering Techniques",
Ammar Almomani, B. B. Gupta, Samer Atawneh, A. Meulenberg, and Eman Almomani

[20]. DNSBL. Information Spam Database Lookup. Accessed 28 May
2012,available: http://www.dnsbl.info/

[22]. microsoft, Sender ID ,2008, available:http://www.microsoft.com/

[23]. Yahoo, DomainKey Library and Implementor's Tools,accessed 29 may 2012,Available: http://domainkeys.sourceforge.net/

[24]. I.Kim ,"Keypad against Brute force attacks on smartphones", IET on 9 July 2012.

[25]. Swetha, "Jamming of Brute Force attacks", IEEE, 2013.

[26]. Tzu-Yen Wang, Shi-Jinn Horng , "A Surveillance Spyware Detection System Based on Data Mining Methods " published in Evolutionary computation IEEE congress on Sept 2006.

[27]. G.M. Al Dossary, " Computer virus prevention and containment on mainframes", published in 2002 at International Carnahan Conference.

[28]. Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R. B. Butler, "Cryptolock : Stopping Ransomware" , IEEE 36th conference,2016.