A Survey on Different aspects of Network Security in Wired and Wireless Networks

Bharti Chopra
Student (Department of Information Technology)
Chandigarh Group of Colleges, Landran, Mohali, Punjab, India.

Dr. Parminder Singh
Assistant Professor (Department of Information Technology)
Chandigarh Group of Colleges, Landran, Mohali, Punjab, India.

Abstract- Network Security has become very crucial these days where the communication speed has been increasing at rapid rate that data travels from one part of the world to another in couple of seconds. The IEEE professional standard society advances the connecting method throughout the world which resulted from wired to wireless environment with advent of Internet. In such a complex Hybrid network, one can't abate his system from the need of higher network security as the intruders are also working at next generation level where they have switched from to traditional to smartest intruding methods. Although many security techniques are being developed and a lot of research is going on to protect network but the fields lacks a common integrated platform which can provide the solution to the existing issues. In this paper, we have analyze number of present attacks in network affecting all layers of OSI layered communicating model so that we can understand the security fallacies andalong with them their mitigation techniques are also mentioned to prevent them.

Keywords: Network Security, Intrusion , IDS, Different Layer attacks.

I. INTRODUCTION

A **network** is basically all of the components (hardware and software) involved in connecting computers across small and large distances [4]. Networks are used to provide easy access to information, thus increasing productivity for users. There are following main types of networks:

Personal area network (PAN): It is a network that is used for the communication among the personal system and its connecting devices like printer, modem, telephone, etc. in close proximity limited to one person only.

Local area network (LAN): It is a network used for connecting two or more than two persons in a small geographical area like campus , office building, etc.

Wide area network (WAN): It is a network used for connecting people at large geographical area. Large numbers of LAN are connected with each other creating a WAN so as to connect almost whole world.

Metropolitan area network (MAN): It is a hybrid network ranging between LAN and WAN where the connecting devices lies within the city. It is mainly used by the co-operate companies who want to share data from its one branch to another in the same city.

Global area network (GAN): This network is used for supporting mobile across arbitrary number satellite coverage areas and wireless LANs etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next.

Virtual private network (VPN): It is a network which is maintained by companies who wants to do the private communication over the public network. The path between the two companies in VPN is encrypted and forming a tunnel for the safe communication.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources[1]. It provides and assures all kinds of authentication and authorization of data accessing and usage in the network which are monitored by the Network administrator; therefore there are various different aspects of security:

- *Privacy*: Related with confidentiality of the data between sender & receiver.
- *Authentication*: Sender & Receiver ID must be valid & there is no intruder.

- *Integrity*: Data must be exact & original as it was sent initially by the sender.
- *Non-Repudiation*: Sender must not able to deny from the data he has sent to the receiver.

There are various Intrusion Detection Systems (IDS) established on the networks to prevent of malicious activities happening at different layers of communicating model. Intrusion detection is the process of trying to find out activities that violate security policy when they are taking place in computer networks and systems [1]. As the intrusion varies from layer to layer so the IDS varies. Intrusion in simple words can be defined as the malicious codes, files or any other mean with which the Intruder can gain the unauthorized access to the network. Thus this results in harming the all aspects of the network security. There are two main types of attacks:

- *Passive Attacks*: Based on Monitoring or Eavesdropping and hard to detect.
- *Active Attacks*: based on modification and easy to detect.

In the early days of LAN, security by controlling physical access to the facilities was raised and initiates were biggest threats [2]. But as the time passed by the advent of the Internet and adoption of WAN, intruders have found lot of alternative ways to gain the unauthorized access through various access points or just modem due to presence of such a complex hybrid network the security issue are now very high in demand. Hence the traditional techniques are not so sufficient to deal with the latest happening attacks. According to the OSI model we are having the following structure where different layers are functioning differently so the attack also varies:

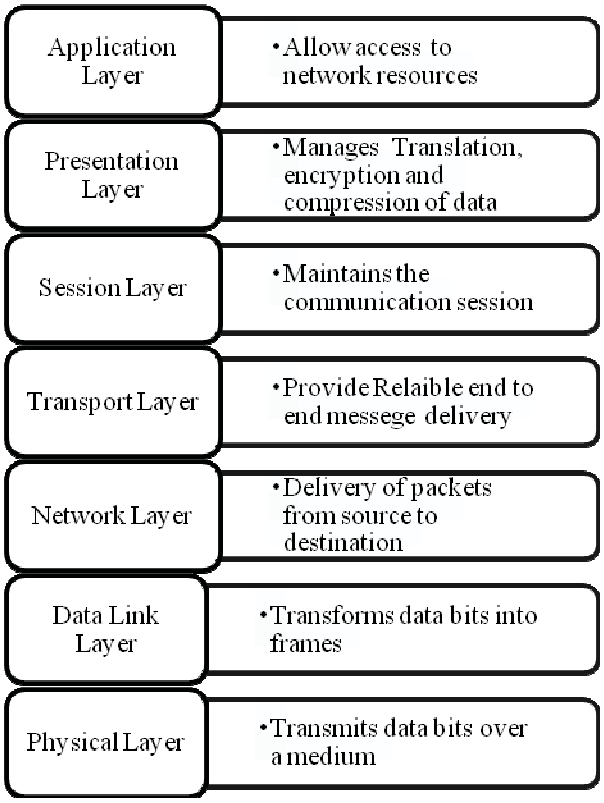

Figure 1: OSI model

II. TRANSMISSION MEDIA & PROTOCOL STANDARDS

Transmission media is a means by which a communication signal is carried from one system to another. A transmission medium can be defined as anything that can carry information from a source to a destination [5]. The two main categories of transmission media are: Wired and Wireless.

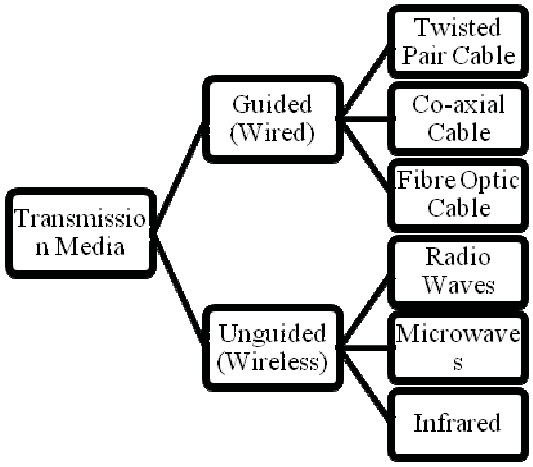

Figure 2: Transmission Media

- *Wired Media (IEEE 802.3)*: The data is travelled across the guided path where the sender and receiver are connected through dedicated path via cabling along whole network. There are few typeqs of cables which varies corresponding to their speed and reliability. The main cables are : Twisted pair, Co-axial, and fibre optic cables.
- *Wireless Media (IEEE 802.11)*: It is an unguided media where data travels from anywhere in the network in form of packets. Thus it doesn't require any sort of physical infrastructure. It is less reliable but very fast in speed. The types are: Radio waves, Terrestrial Microwave and infrared.

III. CATEGORIES OF ATTACKS

Depending upon the harm and measure of threats attacks have been categorized into following categories [1]:-
1. *Probing attacks*: In this kind of attack intruder scans and look out through the whole network to find out the vulnerabilities to corrupt the network and gain the useful information.
2. *Denial of Service attacks*: In this attacks the intruder's intention is to prevent the authorized users from various services like connecting, usage of data, etc.
3. *User to Root attacks*: Here Attacker does not have an account on the victim machine, hence tries to gainAccess [6].
4. *Remote to User attacks*: Here Attacker has local access to the victim machine and tries to gain super userPrivileges [6].

These categories further falls into following two respective areas wise and type wise attacks:

- *Wired and Wireless Network Attacks:* In physical networking environment i.e. **WiredNetwork**, the intruder just need to search for the single Access point either Telephone number or IP address. They look for the modems to access the network and known as "war dialling". Whereas in infrastructure less environment i.e. **Wireless Network**, the task of intruder has become so easy that they can enter through any narrow area and can spoil the network. The wandering of access point of wireless network known as "war driving".
- *Passive and Active Attacks*: **Passive attacks** are the monitoring attacks in which intruder only analyses the data and doesn't do any kind of interruption or modification. The main aim of the intruder is to do traffic analysis and release of message. Thus it very hard to detect the intruder that where it is present and what data he is stealing, so it's better to do prevention in such kind of attack. On the other hand, **Active attacks** are those which are based on modification of data. The main aim of intruder is to do interruption, modification and fabrication of the confidential data.

IV. LAYER WISE ATTACKS AND THEIR MITIGATION TECHNIQUES

Layers	*Attacks*
Application	Request Flooding, Repeated One- shot, Application Exploit, Asymmetric.
Presentation	Cryptographic Flaws, Remote Manipulation.
Session	DNS Poisoning, Password theft, SSH MITM Downgrade.
Transport	Session Hijacking, SYN or ACK Flooding, Port Scanning.
Network	Gray Hole, Black Hole, Worm Hole, Byzantine, Rushing, Selective Forwarding, Information Disclosure, False Routing.
Data Link	VLAN Hopping, MAC Flooding, ARP Spoofing, DHCP attack, Spanning Tree.
Physical	Device Tampering, Jamming, Packet Sniffing.

Physical Layer (Layer 1): The Physical layer supports the functioning of travelling of data traffic over the network in form of bits through physical medium. It is the most vulnerable layer as the encryption and decryption takes place on this layer and intruder looks over the network through the physical means to get the useful information. The possible attacks which happen on this layer are:

1) *Device Tampering:* In such attack, the infrastructure of the network is targeted to destroy the information. These attacks mainly done are either to damage or modify the access points so as to stop the services and path of transferring data.
2) *Jamming:* Unlike device tampering attacks that are physical, jamming attacks disrupt theavailability of transmission media [8]. This is one of the kinds of Denial of Service attack which overwhelms the network path and doesn't allow the legitimate user to access the information.
3) *Packet Sniffing:* Packet sniffing refers to the monitoring of network and analysing packets travelling through that network interface. The intruder looks for the confidentially data in the passing traffic. It is passive in nature and also known as Eavesdropping. The attacks vary from wired to wireless and it is easier in wireless media to access the private information as there are number of access points.

CONTROLS:

- Access Restriction.
- Encryption of data bits.
- Biometric Authentication for logging onto the network.
- Electromagnetic Surveillance on the media.

Data Link Layer (Layer 2): The Data Link layer deals with the transformation of raw data bits into frames, physical addressing, flow control, error control and access control of the data, thus providing the node to node delivery of

data. Due to the open nature of the channels the layer two is very much vulnerable to high risk attacks. The stealing of valid IDs, traffic viewing and manipulation, etc. The main attacks come under this category of layer are:

1) *VLAN Hopping:* It is a malicious activity in which intruder on one VLAN tries to send packet to a system on another VLAN of which he hasn't access to gain control over the VLAN. There are two techniques for VLAN hopping: Switch and Double Tagging.
2) *MAC Flooding:* MAC flooding is also known as CAM table overflow where CAM stands for Content Address Memory. It stores the information of MAC address and port availability of respective VLAN. CAM has fixed size and intruder always try to overflow the table by sending large number of MAC addresses to overwhelm the table from different switch ports pretending to be as a legitimate user. It thus in the end results the switch to transform into the hub and thus broadcasts all the information to all even to unauthorized user.
3) *ARP Spoofing:*In ARP spoofing the intruder act as a legitimate user and sends an ARP reply to a host's ARP request for a server. By this the server will remain busy only with the intruder and all the actual traffic will be leaked to the intruder.
4) *DHCP attack:* DHCP stands for Dynamic Host Configuration Protocol. This attack causes the Denial of Service in which the intruder sends the large number of DHCP requests with many source MACs so as to overwhelm the server which in results causes the unavailability of service to the valid user.
5) *Spanning Tree Protocol (STP) Manipulation:* STP provides path redundancy while avoiding network loops by configuring the ports as forwarding or blocked state. In STP attack the intruder sends STP message to get the root privilege and manipulates root path; resulting in exploitation of the network topology.

CONTROLS:

- Misbehaviour Detection.
- Identity Protection.
- Wireless Application Protection.
- Frame Rate limitation.

Network Layer (Layer 3): The function of the network layer is to provide source to destination delivery of the packets over the network. It thus ensures each packet from where it originates to the final destination which is done by logical addressing. The network layer suffers from malicious manipulation by gaining access of routing paths, injecting the intruding files and even can distract the data from the right path which can degrade the network and as well as providing false information between the communicating hosts. The main types of attacks on this layer are:

1) *Gray Hole:*Gray Hole attack is a Denial of Service attack which overwhelms the network. It is a variation of the black hole attack, where the malicious node is not initially malicious; it turns into malicious sometimes later [11]. It is very difficult to detect because the nodes here in this type of attack are very much unpredictable and volatile as they varies from normal to adversary and adversary to normal nodes.
2) *Black Hole:* In this type of attack intruder makes fool of all the valid nodes by broadcasting all the nodes especially to its neighbouring ones that intruder is authenticated user so as to gain the routing details to fetch the best optimal path to reach the required node point either it is a server or required destination node. Here only one intruder is present to make the attack from one node.
3) *Worm Hole:*Unlike black hole attack there are more than one intruder are present in the network which are having adversary nodes. These malicious nodes create shortcuts between them known as "Tunnels" to gain the access of the route by tricking the source node and cause the Denial of Service to the destination node. These adversaries have better communication resources (e.g. Power, bandwidth) than the normal nodes [8].
4) *Byzantine:* It is a combination or we say modified version of wormhole and black hole attack where the malicious nodes where one (in black hole) or more than one (in wormhole) intruding nodes are present that damages and degrades the network.
5) *Rushing:*Like in the wormhole attacks it is also a Denial of Service attack where the packets travel much faster than the normal speed from the shortcuts (i.e. tunnels) from a multi-hop route which establishes the attack called Rushing attack.
6) *Selective Forwarding:*In WAN, there is number of access points as well as number of hops through which message passes from source to destination node. Here in the network the intruder compromises any of the

access point and looks through the traffic then he'll selectively forward some data packets and drops out the essential ones. It is thus known as selective forwarding.

7) *False Routing:* in such attack the attacker do the Routing Table overflow and poisoning in which the main objective of the attacker is to overflow the routing so as to overwhelm the table and the authorized user won't be able to enter new routes to the table. And by poisoning the table the original routes will be modified and packets will be routed to the wrong path.
8) *Information Disclosure:* Here a compromised node may leak confidential or important information to the unauthorized node in the network [3]. By which the intruder can rule over the whole network.

CONTROLS:

- Content Access Filtering.
- False Routing Information Detection.
- Firewall implementation.
- Network Intrusion Detection System (NIDS) implementation.
- Virtual Private Network area provided.
- ARP / Broadcast monitoring software activation.
- Wormhole Detection.

Transport Layer (Layer 4): The Transport layer facilitates the user with the reliable and en-to-end message delivery and error recovery. Here the intruder attacks over the information being transferred between the hosts and the another vulnerability occurs at the ports in which intruder tries to use the ports for gaining confidential functions so as to steal or modify or doing both to the important information. Corresponding to these vulnerabilities the attacks occurs in this layer are:

1) *Session Hijacking:* There are two kinds of session hijacking take place at transport layer: TCP Hijacking and UDP Hijacking. In the TCP, the intruder spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a Denial of Service attack [14]. On the other hand, UDP session is similar to TCP but in UDP intruder doesn't need to worry about sequence number and other TCP mechanism.
2) *SYN or ACK Flooding:* when there is a handshaking process starts between the client and the server. The client performs a SYN request to the server and then the intruder looks for the weak point from where the server sends the acknowledgement (SYN/ACK) back to the client but attacker won't let this happen and doesn't allow the client to receive the ACK message. It results in incomplete handshaking process known as 'half-open' connection. Then the intruder keeps on sending the SYN message to server to overwhelm the server's system. The server thinks that valid user sending the messages but nothing happens as such. It generates the denial of service and known as SYN or ACK flooding.
3) *Port Scanning:* In such an attack the attacker gain access of the network by scanning the port numbers which tells about the running process which has been assigned to the valid user. An IP address and Port number functionally determine the process and the network device that is hosting the process [13].

CONTROLS:

- Access Control List method.
- Firewalls setup.
- Stateful Inspection of packets.
- Strong Transmission & Layer Session Identification.
- Client Puzzles

Session Layer (Layer 5): The session of communication is being administered by the session layer. It is the Network Dialog Controller of the network which establishes, maintains and synchronizes the connection between the two or more than two hosts.In the Session Layer, identity is the key factor, and the main controls at this layer focus on the establishment of identity [7]. Therefore the main attacks under this layer are:

1) *DNS Poisoning:*DNS poisoning is when an attacker redirects the client user to some different fraudulent website rather than the entered website to the browser. The attacker is able to fool the client by manipulating the IP address which redirects the client to fake site.
2) *Password theft:* It is the technique used for discovering passwords. Passwords are the main access control methods by which the server admin manages and login to the network resources and applications. Therefore these are the favourite target points of the intruders. Types of such attack are: Brute force attack, dictionary attack and rainbow table attack.
3) *SSH MITM Downgrade:* Man In The Middle is an active attack where the attacker looks and analyses the network traffic for manipulation. At this layer MITM (Man In The Middle) is the SSH down grade scam, where the attacker fools the SSH (Secure Shell) server and client into diverting to SSH1(lower encryption protocol) instead of SSH2(high encryption protocol). Therefore, the created connection will be with insecure confidential credentials and attacker will easily capture the password for entering to the network.

CONTROLS:

- Patches Encryption Authentication.
- Specific account Credentials and authentication expiration.
- Session Identification Protection.
- Limiting failed session Attempts by timing constraint or blocking after some attempts.

Presentation Layer (Layer 6): The Presentation Layer takes care of the organisation, encryption and decryption of the data in accordance with syntax and semantics of the communication between the hosts. The intrusions and vulnerabilities occur at this layer due to the abridged functioning with respect to the privacy and authentication. The attacks underlies this layer are:

1) *Cryptographic Flaw:* In such kind of attack the intruder tries to hack the encrypted text so as to get the original message from unreadable message. Cryptographic presentation services can fall prey to weakness in their implementation of fundamental design [7]. It is the main target for the intruders these days because of presence of many flaws even after declared to be secure.
2) *Remote Manipulation:* In this the intruder is sitting on any system except the server which in the network area of the server. From that point the intruder tries to gain the root access of the server system. By doing such unauthorized attempts the intruder can gain the full access of the server system when once the root is hacked, which results in whole exploitation the network as well.

CONTROLS:

- Surveillance of cryptographic process and continuous review of process.
- Incoming and outgoing data inspection.
- Root access control mechanism.

Application Layer (Layer 7): The application layer is the top most layer in the stack of OSI model. It facilitates the user interface and resource services(like mail, directory services, file transfer, etc.) to the end user. Because of the open-ended nature of the application layer it suffers from many threats and hampers the security of the network. The main types of attacks under this layer are:

1) *Request Flooding attack:* The Request flooding attacks overloads the server by sending the number of application layer resources(HTTP, SMTP, FTP, etc.) requests to the server pretending as these are coming from a legitimate user at very high speed and frequency rate. It thus in the end results in crash of server working and overwhelm its session resources.
2) *Repeated one-shot attack:* The repeated one-shot attack means sending the many same kind of 'high-work loaded" request to the server which means single work but containing huge volume of data to be done. These kinds of work loaded requests are send many times which results in degrade of the services of the server.
3) *Asymmetric attack:*These attacks are same as above repeated one-shot attack but with the difference that the attacks are not repeated in this only once the server is being loaded with the large amount of work.

4) *Application Exploit attack:*These attacks are done by the intruder to get the vulnerable and weak access point in the applications so as to exploit the operating system of the server and would be able to gain access to the admin's system, network, resources, etc.

CONTROLS:

- Data Integrity Protection.
- Data Confidentiality.
- IDS monitoring system.
- Host based firewall system.
- Standards, testing and review of applications code and functionality.

V. RELATED WORK

A lot of attacks are present on the networks which are exploiting the number of hosts both in wired and wireless networks. There are number of attacks as per protocol stack and security attributes and along with them preventive approaches are provided layer wise (Bing Wu, 2006). The study by (J. Sen, 2011) provided the threat models and security goals for secure routing in the wireless networks, identified different attacks on different layers, and presented various security analysis and countermeasures for different routing protocols. The complete security solution requires the prevention, detection and reaction mechanisms applied in network (K.P. Manikandan, 2011). The attacks are analyzed main categories wise on different protocols such as TCP, UDP, ARP and ICMP (Amrita Anand, 2012). The study by (Gursewak Singh, 2013) focused on the layer wise attacks, defining them individually and there layer wise procedure to prevent each and every attack.

VI. CONCLUSION AND FUTURE WORK

In this review paper, we have covered the introduction of the various types of networks and the network security issues varying in different network links. Whether there is a wired media or wireless media they fall into the same categories of attacks. Here we have represented the reviews of different research work where attacks are varying layer wise from top to bottom stack of the OSI model. All these aspects and reviews lead us to the idea of new research. Thus in future we have planned the integrated Intrusion Detection System (IDS) on the Hybrid Network (i.e. both wired and wireless media) working on cross layer especially on the MAC layer. It is because the MAC layer is the weakest layer and easily gets compromised.

REFERENCES

[1] Mrs. Sneha Kumari, Dr. Maneesh Shrivastava, "A Study Paper on IDS Attack Classification Using Various Data Mining Techniques", International Journal of Advanced Computer Research, ISSN (print): 2249-7277 ISSN (online): 2277-7970, Vol. 2, No. 3 Issue-5 September-2012.

[2] M. Thangave, P. Thangaraj, "Efficient Hybrid Network (Wired and Wireless) Intrusion Detection using Statistical Data Streams and Detection of Clustered Alerts", Journal of Computer Science 7 (9): 1318-1324, ISSN 1549-3636, 2011.

[3] Jaydip Sen, "Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses", Innovation Lab, Tata Consultancy Services Ltd., India, pp. 279-309, 2011.

[4] http://computernetworkingnotes.com/network-technologies/basic-networking.html

[5] http://www.mu.ac.in/myweb_test/syllFybscit/dcn.pdf

[6] M. Revathi, "Network Intrusion Detection System using Reduced Dimensionality", Indian Journal of Computer Science and Engineering, ISSN: 0976-5166, Vol. 2, No. 1, pp. 61-67, 2011.

[7] Damon Reed, "Applying the OSI Seven Layer Network Model To Information Security", SANS GIAC GSEC Practical Assignment version 1.4b Option One, November 21, 2003.

[8] Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey",Springer, 2005.

[9] Joseph Soryal, Tarek N. Saadawi, **"**IEEE 802.11 DoS attack detection and mitigation utilizing Cross Layer Design**",** Ad Hoc Networks, Vol. 14, pp. 71-8, March 2014.

[10] http://www.alliedtelesis.com/solutions/p-1061.html

[11] Himadri Nath Saha, "Study of Different Attacks in MANET with its Detection & Mitigation Schemes", International Journal of Advanced Engineering Technology, E-ISSN: 0976-3945, pp. 383-388, Vol. 3, Issue 1, January-March 2012.

[12] Thomas W. Shinder, "Chapter 12- Filtering, Intrusion Detection, and Attack Management", The Best Damn Firewall Book Period (Second Edition), pp. 413- 437, 2007.

[13] John V. Harrison, Hal Berghel, "A Protocol Layer Survey of Network Security", ADVANCES IN COMPUTERS, Vol. 64, ISSN: 0065-2458, DOI 10.1016/S0065-2458(04)64003-4, pp. 109-157, 2005.

[14] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Department of Computer Science and Engineering, Florida Atlantic University, 2006.
[15] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions" In proc. IEEE Wireless Communication, UCLA, Los Angeles, CA, USA, Vol. 11, pp.38- 47, ISSN: 1536-1284.
[16] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao , "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks" in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.
[17] Amrita Anand, " An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols" in International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 8, August 2012 ISSN: 2277 128X, 2012.
[18] Gursewak Singh, Rajveer Kaur, Himanshu Sharma, "Various Attacks and their Countermeasure on all Layers of RFID System" in International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Vol. 1, Issue-5, March 2013.
[19] L. Zhou, Z. J. Haas (1999), Cornell University, New York, USA. "Securing ad hoc networks", IEEE Network, Volume: 13, pp. 24-30, ISSN: 0890-8044.
[20] Rakesh Kumar Singh, Rajesh Joshi and Mayank Singhal, "Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)", International Journal of Computer Applications 68(4):25-29, Vol. 68, No. 4, April 2013.
[21] Amrita Anand, Brajesh Patel, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 2, Issue 8, August 2012.
[22] Julian Jang-Jaccard, Surya Nepal, "A survey of emerging threats in cybersecurity", Journal of Computer and System Sciences, Vol. 80, Issue 5, pp. 973-993, August 2014.