International Journal of Engineering & Technology, 7 (2.32) (2018) 322-326

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Security Attacks in Wireless Sensor Networks

Lalitha Bhagavathi Gurajada[1], Sai Deepthi Rajaputra[2], Indira Gogineni[3], Riaz Shaik[4]

[1,2,3,4]*Department of Computer Science and Engineering, KLEF, Vaddeswaram, India*
**Corresponding author E-mail: lgurajada@gmail.com*

Abstract

In today's world, Security is the prime concern for each application. Network security and Computer protection are the serious issues. A broad range of Wireless Sensor Networks (WSNs) applications[1][15] are widely used in military, researches etc. The key subject of computing is to provide network security several types of attacks are increasing day by day. The attacks present in different layers are produced due to the susceptibilities present in the layers. The Seven layers in OSI model are formulated to convey the information from highest layer to lowest layer. Broadcast of data gets modified according to the layer in which it lies. Individually every layer is weak to different types of attacks. This paper models about the different attacks present in each layer of OSI.

Keywords: *Attacks, Security, Vulnerabilities*

1. Introduction

The rapid advancement of Computer network technology and internet technology is so quick that makes people aware of network security. Many types of attacks are increasing day by day which made network security an important issue. Wireless sensor networks (WSNs) have a vast field of applications, including environment monitoring, battlefield surveillance and target tracking systems. Seven layers of Open System Interconnection have individual set of functions which performs data to move from source to destination on a network. Every layer gets exploited and has their inherent vulnerabilities. Now a days , this DDoS attack constitutes a major issues and hardest security concern in Internet. Several mechanisms have been implemented to defense the network system from DDOS attacks [2]. DDOS attack targets a server as a victim with huge amount of information by flooding directly or indirectly with lots of zombie computers and prevents legitimate users from accessing. These attacks are launched easily by exploiting the flaws in protocols of internet such as TCP/UDP. Each layer has some vulnerability which ultimately causes attack. This paper gives a survey to understand attacks in different layers of OSI model and DDOS attacks with respect to different layers of OSI Reference Model.

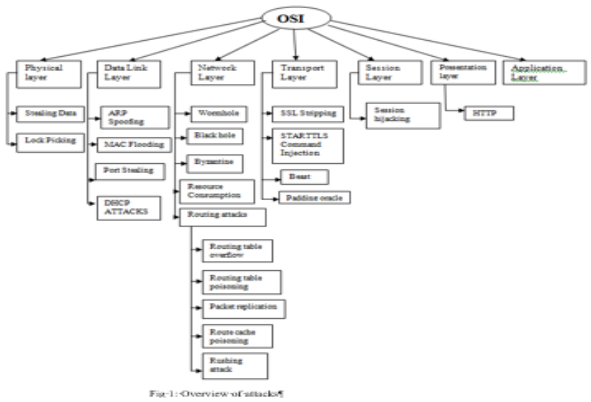


Fig: 1: Overview of attacks

2. Physical layer Attacks

2.1 Defending the Physical Layer:

Open System Interconnect comprises of seven layers in that physical layer is at the lowermost of the OSI. This layer is planned to spread the message bit streams via electronic signals, illuminations, or else radio broadcasts. The security in this layer must include the connection which is done using wire to connect systems along with the system hardware which supports services. Physical security is one of the oldest features of security. It has the main preference where the protection must begin which depends up on our condition, assets, and budget. This focuses on attackers and thieves and is united with procedural safety along with administrative controls which supplies a comprehensive view of security. DDoS attacks in the Physical layer are destruction, obstruction, exploitation, or break down of physical assets, The Impacts are the Physical resources will become impassive and they need to be repaired to increase their availability.

2.2 Attacking the Physical Layer:

Control is the significant feature for security in the physical layer. If any person attains physical control over the system, it generally holds to control a device's performance [10]. That's why physical security plays a noteworthy role in worldwide security. Here we have numerous forecasts that physical security can be challenged by (for example: stealing data, lock picking).

2.2.1 Stealing Data:

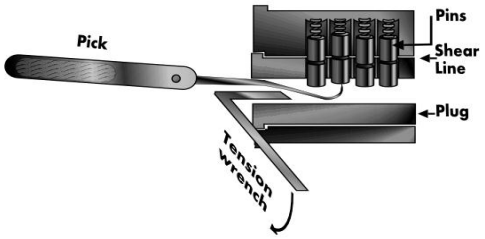
This Physical layer attack is the major effortless aspect for a malicious insider to effort, since they previously contain an approach to the system. State sponsored industries might obtain the profit from the trade secrets and insider information. Some of these attacks have become informal as progressions in electronics and optoelectronics contain intelligence work, interception, and infor-

mation theft complicated to identify. These tools usually need some physical access**.**

2.2.2 Lock Picking:

Avoid a lock is nothing but a lock picking and it is a very slow method. Cat Burglar Persons normally try to break a window, interfere a doorframe, or knock a hole in the sheetrock soonthan their determination to pick a lock. Mostly lock picking is learned individually by everyone. Lock picking is the strategy where we have to open a door without a key of a lock's components. The essential mechanisms used together to pick locks are Tension wrenches and angled flat head screwdrivers appear in a variety of thickness and sizes .Lock Picking performs some operations like picks small angled and pointed comparable to dentist pick.

Fig 2: Common Lock Picking



The security attacks in the physical layer are fewer mainly effective. They might avoid all the controlsthat exist in the superior layers of the stack (heap). Mobile devices in this layer enhance the risk of these attacks as they can setup a malicious code in the system or effortlessly eradicate huge quantity of information (data).

3. Data link Layer Attacks

Data link layer is the second layer. Security within this layer is strong as well as the weakest part also. The security issue in the layer has not been addressed in fact. The pathetic part might be the data link layer which permits interoperability and interconnectivity within the network system[3]. Still a concession happens in this layer that permits internal attacks; it might not be identified by superior layers. The data link layer offers some functions like practical and technical means to convey the information among the network entities and to recognize the possible accurate errors that might arise in the physical layer. Tool based attacks[4] are also possible on this layer. This layer in networks is highly feasible to quite a few attacks. They are

1. ARP Spoofing
2. MAC Flooding
3. Port Stealing
4. DHCP Attacks

3.1 ARP Spoofing:

Local Ethernet recognizes Ip address to physical machine address is mapped using Address Resolution Protocol (ARP). Whenever hosts want to find a MAC Address for an Ip Address, it requests by sending ARP request. A reply of ARP message with Physical address is obtained from other host which has the Ip Addresses.

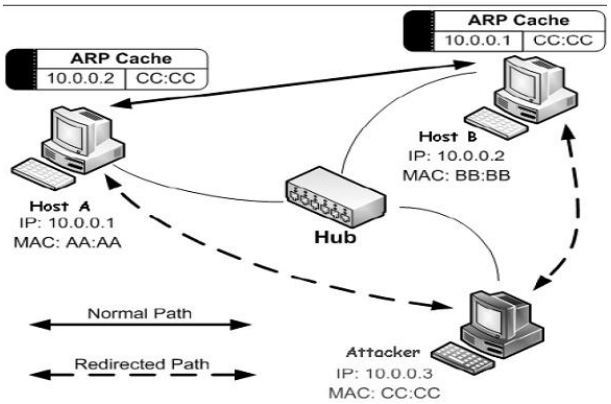


Fig 3: ARP Poisoning

This attacker allows the intruder to make false assumptions as legal host and then stops data frames onto the network. With the help this attack, many other attacks are also launched on to the network system such as denial of service, man-in-middle attack, Session hijacking.

3.2 MAC Flooding:

MAC addresses, switch port numbers, and other information are stored in each switch of Ethernet stored in a table format which is named as Content-Addressable Memory (CAM) table which has a fixed size of memory. This attack is also called as CAM table flooding attack. Switch port is connected to the attacker which makes to flood the switch interface using more number of Ethernet frames with false MAC addresses [5]. In less time, the table gets filled with fake MAC addresses .Due to the limited size of memory; table can't store the more MAC addresses. Once table gets filled, It starts acting like a network hub which floods the frames to all orts using broadcast communication.

3.3 Port Stealing:

In this attack, the traffic which is directed to one port is stolen and is directed to other port of a switch [9]. Packets which should be received by one computer is directed to other computer in this attack. This makes the switch to believe that the intruders' port is the correct destination for a packet.

3.4 DHCP Attacks:

Ip addresses are allocated to the systems for a specific period of time using DHCP. Servers of DHCP are attacked which are in order causes denial of service. In this spoofing attack, attackers set up an dishonest DHCP server which causes military action for providing addresses to the clients. With the help of rogue default gateway which performs military actions against clients with host machines and DHCP responses which an attackers provides. Data frames from the host servers are moved to route gateway where an attacker obstructs all the frames and will give reply to actual gateway or drops them.

4. Network Layer Attacks

Network layer is third layer of the OSI model and this layer has many tasks based on the applications, but the foremost tasks are energy consumption, Limited memory and buffers. DDoS attack in the Network layer is ICMP Flooding. The result can affect available network bandwidth and force extra load onto the firewall. The following attacks define the security in the network layer.

4.1Wormhole Attack:

This attack allows an intruder to receive the packets at particular place of the system it then underpasses to another place of the network system where the packets are send back again to the system [4]. This underpass amongst two plot attackers is stated as a wormhole. It might be recognized over a single long-range wireless link or an even over a wired link amongst the two plot attackers.

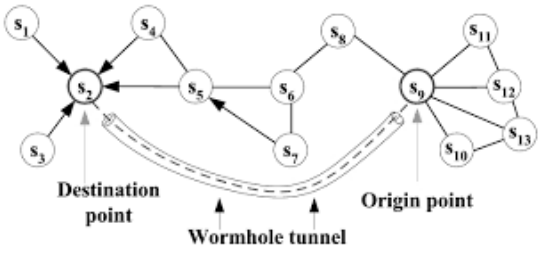


Fig 4: Worm Hole Attack

By the transmission character of the radio channel the intruder can produce a wormhole number of packets which are not addressed to it. If appropriate methods which are not hired, then it will be difficulties to safe guard the network system against the wormhole attack. Most of the popular routing protocols may fail to discover the legitimate routes.

4.2 Black Hole Attack:

This attack makes a harmful node falsely promotes best paths to the destination node in the process of path finding or in the route update messages.

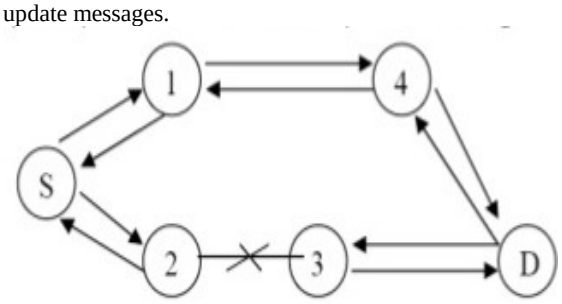


Fig 5: Black hole attack

The purpose of the harmful node is to cause difficulty for route investigating procedure[6] or to suspend the data(information) packets which are being sent to the target node which is concerned.

4.3 Byzantine Attack:

With this byzantine attack a set of cooperated nodes or a cooperated intermediate node works together and take away such producing direction-finding loops, packets which are routed on non-optimal paths and some dropping packets. These failures are rigid to distinguish. The network might be seen working normally in the lookout of the nodes; however it might reveal this failure.

4.4 Resource Consumption Attack:

A harmful node which strive to devour/surplus the assets of the some other nodes present in the network system. These are aimed to be battery capacity, bandwidth, and computational power. The attacks might be in the system of needless request for the money or progressing of hard packets to nodes [7]. By via the battery power of one more node and to facilitate the node becomes continuously active by pumping the packets to the node is identified to be asleep deficiency attack.

4.5 Routing attacks:

Present we have numerous categories of attacks presented on the routing protocol that is intended to unsettle the function of the network system[8]. Within the routing protocol, we have many attacks they are:
Routing table overflow
Routing table processing
Packet replication
Route cache poisoning

4.5.1 Routing Table Overflow:

In this attack of routing protocol the opponent node publicizes routs to unreal nodes, to the approved nodes existing in the system network. The major aim of this attack is to originate an excess in the routing table that could avert the formation of entrances equivalent to fresh authorized paths .

4.5.2 Routing Table Poisoning:

The cooperated nodes in the network system propel untrue updates of routing otherwise alter unaffected route renew packets propel to further uncompromised nodes.

4.5.3 Packet Replication:

Here an opponent node duplicates some decayed packets. This devours extra bandwidth and battery power resources existing to the nodes might cause needless misunderstanding in the process of routing.

4.5.4 Route Cache Poisoning:

Here the every node maintains a path catch that would hold the information about the routes which became popular in the current time. Like table poisoning an opponent would toxic the path cache to attain parallel goals.

4.5.5 Rushing Attack:

In demand routing protocol we use identical repression through the process of route discovery are weak towards this attack. A opponent node which gets a route request packet from the source node floods the packet rapidly throughout the network earlier other nodes which receives the similar route request packet could respond.

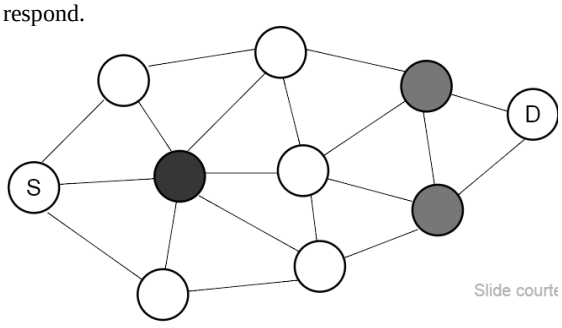


Fig 6: Rushing Attack

Nodes that receive real route request accept those packets to be copies of the packets previously received through the opponent node and therefore discard those packets. It is difficult to find these attacks in ad hoc wireless networks.

5. Transport Layer Attacks

This is the 4th layer of OSI model. The tasks of this stage comprise continuous communication transmission abilities self-determining

of the essential network, all along the division, error control and flow control. Continuous communication broadcast otherwise linking appliances in the transport layer could be characterized into:

1. Connection Oriented e.g. TCP
2. Connection less e.g. UDP

This layer offers the service of linking applications collected using ports. Subsequently IP offers a most excellent attempt delivery, and this layer is the primary layer of the TCP/IP stack to propose consistency [12]. The attacks in this layer are:

5.1 SSL Stripping
5.2 STARTTLS Command Injection Attack
5.3 Beast

5.4 Padding oracle attacks

DDoS attacks in the Transport layer are SYN Flood, Smurf Attack; they reach bandwidth or connection limits of hosts or networking equipment

5.1 SSL Stripping:

Here several attacks effort to eliminate the utilize of SSL/TLS overall by means of altering non-encrypted protocols which stipulate the use of TLS, exactly altering HTTP traffic and HTML pages since they go by on the wire . Some of the attacks are mutually acknowledged as "SSL Stripping" (a form of the more generic "downgrade attack").

5.2 STARTTLS Command Injection Attack:

These attacks are which are evolved among the insecure and TLS-secured traffic. Many IETF application layer protocols will use an application stage command for upgrading apparent extra association to use TLS. Several executions of STAR TTLS with a fault in which an input buffer of an application-layer has reserved commands that have been pipelined with the STARTTLS command, so that information received before to TLS negotiation are performed after TLS concession . This issue is determined by demanding the input buffer of an application-level command to be zero prior negotiating TLS.

5.3 Beast:

This attack uses the problems with the TLS 1.0 employment of Cipher Block Chaining (CBC) to decipher the parts of a packet, and precisely to decipher Hyper Text Transfer Protocol cookies when it runs over TLS .

5.4 Padding Oracle Attacks:

In this attack a significance of the MAC-then-encipher plan which is present in all existing version of TLS is the presence of this attacks a fresh life of such type of attacks is called as Lucky Thirteen attack, a decision side-channel attack that permits the intruder to decipher random cipher text.

6. Session Layer Attacks

The session layer executes some procedures like, sets up manages and terminates exchanges and conversations. Session Layer has some features like:

Session Checkpoint
Session Termination
Session Adjournment
Session Termination
Half and Full duplex operations

Session Hijacking: This attack consists of the development of the web conference control method [11] that is usually handled for a session token. This attack tries to make settlement for the token by robbery or expecting a valid token to achieve unauthorized access to the web server. The session of this token can be compromised in many numerous ways, the most popular ones are Man-in the middle attack in this the attacker stops all connections between the hosts. Protocols which depend on the alter of the public keys to guard the communications are often the aim of these types of attacks.

7. Presentation layer Attacks

Presentation layer is the 6th layer of the OSI model and regularly this layer is not executed otherwise it is executed as a side characteristic into protocols belonging to other layers. It does not seem that there are any attacks here. DDoS attack in the Presentation Layer is performed by Malformed SSL Requests, inspecting SSL encryption packets is resource intensive. SSL is used by attackers to tunnel HTTP attacks to aim the server. The affected systems could prevent accepting SSL connections or automatically restart.

8. Application layer Attacks

It is the 7th layer of the OSI model. The target of this layer is to tire out the resources which are consuming too much. There are some attacks and they attack on windows web server, apache as they are weaker. These attacks are more beneficial in popularity than DDoS attacks and they are most sophisticated .DDoS attacks in the Application Layer are possible in PDF GET requests, HTTP GET, HTTP POST, website forms (login, uploading photo/video, submitting feedback)[16] .The result of these attacks is reaching resource limits of services, Resource starvation.

Some of the attacks in this layer are:HTTP, Web based email etc.

HTTP: This is the most well-known attack of the application layer and this http makes use of a botnets to force a goal and to enlarge an excessive amount of resources when reacting to a Http Request.

HTTP Floods, Web based email and other DDoS attacks of the application layer have a mimic behavior which the user gets difficulty to detect other types of attacks.

8. Conclusion

In this paper we have given a detailed survey on attacks which occur in all the layers and a comprehensive explanation regarding features of each layer and their vulnerabilities which causes occurrence of attacks. DDOS attacks are also explained in detail regarding each layer and their consequences. Now a day's DDOS attacks became a serious threat for wired and wireless networks. The future advancements in DDOS attacks is required to overcome the drawbacks with the defensive techniques which are already in existence.

References

[1] Riaz Shaik Shaik Shakeel Ahamad Key management schemes of wireless sensor networks: A Survey fronteiras journal of cial ,technological and environmental science v.6,n.2,may-august 2017

[2] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[3] GReAT, Kaspersky Lab Expert: The Red October Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies
[4] http://www.iaeng.org/publication/IMECS2008/IMECS2008_pp1143-1148.pdf
[5] Dave Jing Tian, Kevin R. B. Butler, Joseph I. Choi, Patrick McDaniel, Padma Krishnaswamy, Securing ARP/NDP From the Ground Up, Information Forensics and Security IEEE Transactions on, vol. 12, pp. 2131-2143, 2017, ISSN 1556-6013.
[6] Sharma, R. Singh, G. Pandey, Detection and Prevention from Black Hole attack in AODV protocol for MANET, Published in International Journal of Computer Applications, vol. 50, no. 5, 2012.
[7] Riaz Shaik Shaik Shakeel Ahamad ,An agent based hybird approach for dynamic key management system in dynamic wireless sensor network Journal of advanced research in dynamical and control systems vol.9,Issue 2,Oct 2017
[8] Harris Simaremare, Abdelhafid Abouaissa, RiriFitri Sari, Pascal Lorenz, Performance Analysis of Optimized Trust AODV using ANT Algorithm, IEEE ICC 2014 - Communications Software Services and Multimedia Applications Symposium, pp. 1843-1848.
[9] http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Layer-1-The-Physical-Layer.pdf
[10] http://bladesecurity.blogspot.in/2013/09/layer-5-attacks-session-layer-attacks.html
[11] https://tools.ietf.org/html/rfc7457
[12] http://www.informit.com/articles/article.aspx?p=361984&seqNum=10
[13] http://www.psafe.com/en/blog/here-are-the-largest-ddos-attacks-in-history/
[14] Riaz Shaik Shaik Shakeel Ahamad Enhanced Attack Resistant agent based dynamic key management in dynamic wireless sensor newtworks International journal of civil enggineering and technology 8(12),2017,pp,69-76
[15] DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.