International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 11 (November 2014), PP.58-63

A Survey: DDOS Attack on Internet of Things

Krushang Sonar[1], Hardik Upadhyay[2]
[1]*GTU PG School, Research Scholar, Ahmedabad, India*
[2]*GPERI, Assistant Professor, Mehsana, India*

Abstract:- Internet of Things refer as interconnection of smart object, included from small coffee machine to big car, communicate with each other without human interactions also called as Device to Device communications. In current emerging world, all of the devices become smarter and can communicate with other devices as well. With this rapid development of Internet of Things in different area like smart home, smart hospital etc. it also have to face some difficulty to securing overall privacy due to heterogeneity nature. There are so many types of vulnerability but here in this paper we put concentration on Distributed Denial of Service attack (DDoS). DoS is attack which can block the usage for authentic user and make network resource unavailable, consume bandwidth; if similar attack is penetrated from different sources its call DDoS. To prevent from such attack it need mechanism that can detect and prevent it from attack, but due to small devices it has limited power capacity. So that mechanism must be implemented at network entrance. In this paper we discuss different DDoS attack and its effect on IoT.

Keywords: - Denial of Service, Distributed Denial of Service, Device to Device, Internet of Things, Smart Object.

I. INTRODUCTION

A. Internet of Things

Technology becomes faster and smaller day by day and moving toward “always connected” model. This revolution makes each and every device to communicate with each other and fabricate new future internet. This new concept of future internet is known as Internet of Things [1]. Every device from cell phone to car, alarm clock to coffee machine becomes connected to internet with open standard IPv6 allowing unique addressing schema for them. IoT integrate physical things into information network. These physical things sense the properties from environment and send them for further processing to some information network.

There are following various security services are necessary for IoT.

1) *Confidentiality:* Message passing from source to destination could easily intercept by attacker and content can be compromised. So that message should be hidden from all relay nodes, means message securely passing End to End is required in IoT. Same can also be applying on Device storage. Simple solution for this is encryption/decryption mechanism.

2) *Integrity:* Message passing from source to destination should not alter; it should be received at receiver side same as it is sent at sender side. No intermediary should change content of message while they are passing or on device.

3) *Availability:* For continuous working of IoT and access the data whenever necessary, it is also important that services that offered by devices should always available and continuous in working mode. So it is important to detect intrusion and prevent the intrusion to ensure the availability.

4) *Authenticity:* End user should able to identify each other’s identity to ensure that they are interacting with same entities that who they claim.

B. DoS/DDoS Attacks

DoS attack is an attempt by malicious attacker to consuming resources or bandwidth of legitimate users. Such type of attacks when penetrated from various compromised node it called as DDoS. The most common DoS attack involves flooding of huge amount of traffic to consume network resource, bandwidth, target CPU time etc. Some of most common DoS attacks are SYN flood, DNS flood, Ping flood, UDP flood, ICMP broadcast etc.

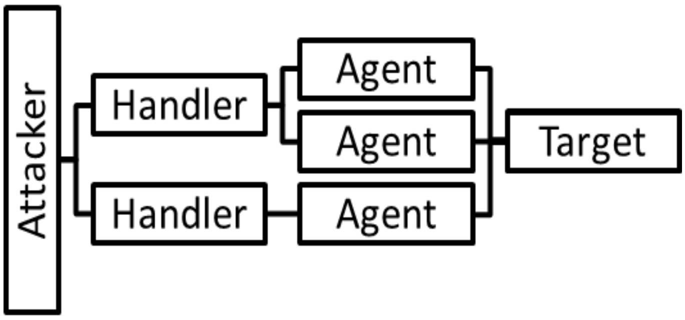

Fig.1: DDoS Attack Flow

In Fig. 1, general scenario of DDoS attack is shown where attacker uses different handler which are nothing but some high performance processing units, from this unit they use different agent to send flood packets into target host to consume resources and network bandwidth.

DDoS Attack Types:

1) UDP flood:

This attack is also known as session less networking protocol. In this attack, attacker floods different UDP packets on random target ports, causing host to check for application listening port repeatedly, and reply with ICMP Destination Unreachable packets. This process leads target host resources inaccessible.

2) ICMP/PING flood:

This attack work similar to the UDP flood attack, an ICMP flood overwhelms the target host resource with ICMP Echo Request (ping) packets, which sending packets as fast as possible without waiting for replies. This type of attack can consume both incoming and outgoing bandwidth, since the target's servers will often attempt to respond with ICMP Echo Reply packets, which resulting a significant overall system slowdown.

3) SYN flood:

A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by SYN-ACK responses from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

4) Ping of Death

A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size - for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

5) Zero-day DDoS

"Zero-day" is simply unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading Zero-day vulnerabilities has become a popular activity.

II. INTERNET OF THINGS ARCHITECTURE AND PROTOCOL STACK

A. IoT Architecture

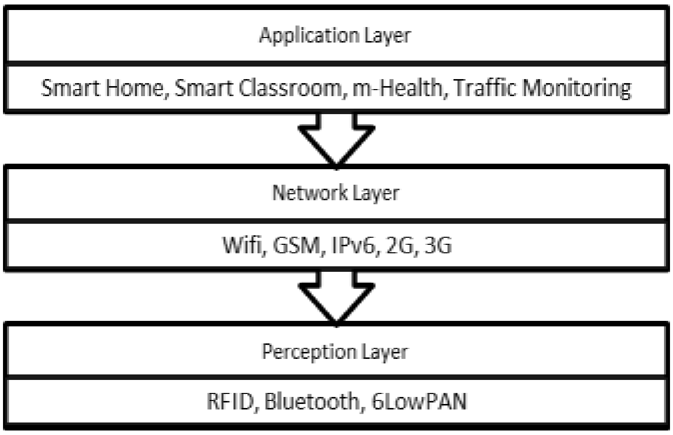

Fig.2: Internet of Things Architecture

IoT is divided into main 3 layers shown in Fig. 2 that are Application Layer, Network Layer and Perception Layer.

1. ***Perception Layer:***
   Perception layer collects all information/data from physical environment like temperature, speed, time, humidity etc. It is nothing but collection of sensor, actuators which forms Wireless Sensor Network (WSN).

2. ***Network Layer:***
   Network Layer is middle layer take control of processing data/information, broadcasting data, aggregates data etc.

3. ***Application Layer:***
   Application Layer is top most layer contains business logic, formulas and UI to user end.

B. IoT Protocol Stack

Protocol Stack of IoT shown following in Figure 3.

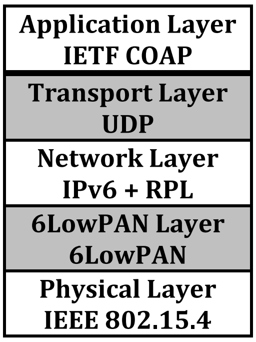

Fig. 3: IoT Protocol Stack [8]

1) Application Layer (CoAP) [2] :

It is hard to provide specific guidance for all possible applications. However, in our experience the following guidelines appear to be important for many of the applications that the authors have worked with:

- Application needs to provide correct state of operation indication.
- System should be automated that can shut down or replace faulty nodes.

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained low powered and low processing nodes (e.g., low-power, lossy) networks. The nodes often have 8-bit microcontrollers with small amounts of ROM and RAM, while constrained networks such as 6LoWPAN often have high packet error rates and a typical throughput of 10s of kbit/s. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.

CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.

2) Transport Layer (UDP) :

Transport layer protocols ensure reliability of overall function. Because of constrained code size and processing power, most sensor network programmers want to use UDP as the transport layer protocol. The sensor transmits a packet to the gateway then goes back to sleep. Since network transmission, especially for wireless sensor networks, is one of the largest consumers of power, this pattern results insignificantly larger power saving than if the sensor were to use TCP, staying awake to process the acknowledgement. However, use of UDP without retransmission at the transport layer risks a significant decrease in reliability, despite the MAC layer retransmissions provided by protocols such as IEEE 802.15.4 (ZigBee). The MAC layer retransmissions are limited and even in moderately dense sensor networks retransmissions can cause congestion, so the packets could still be dropped in the MAC layer

3) Network Layer (IPv6) :

The numbers of potential devices that can be connected to the IoT are in hundreds of billions. This requires the use of IPv6, a new version of the Internet Protocol that increases the address size from 32 bits to 128 bits (2128 unique addresses). Also, a number of protocols are being standardized to fulfil the specific needs of the IoT. Problem comes here as this is constrain network full fledge IPv6 cannot feasible to use direct, so it needs some new modification or techniques to use it with WSN.

4) 6LowPAN Layer (6LowPAN) :

6LoWPAN integrates IP-based infrastructures and WSNs by specifying how IPv6 packets are to be routed in constrained networks such as IEEE 802.15.4 networks. To achieve this, the 6LoWPAN standard proposes context aware header compression mechanisms: the IP Header Compression (IPHC) for the IPv6 header, and Next Header Compression (NHC) for the IPv6 extension headers and the User Datagram Protocol (UDP) header. Due to the limited payload size of the link layer in 6LoWPAN networks, the 6LoWPAN standard also defines fragmentation and reassembly of datagram. 6LoWPAN defines a fragmentation scheme in which every fragment contains a reassembly tag and an offset. When security is enabled or for big application data size, the IEEE 802.15.4 frame size may exceed the Maximum Transmission Unit (MTU) size of 127 bytes; in that case additional fragment(s) are needed.

5) Physical Layer (ZigBee) :

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

III. DDOS ATTACK ON IoT

Now considering different scenario of DDoS attack on IoT based network at different Layers.

A. DDoS on Perception Layer:

1) ***RFID:*** At perception layer RFID is main technology for reading data from sensor without human interaction and touch. [3]

- **a) Jamming:** In this electromagnetic jamming is done to prevent tags from communicating with reader.
- **b) Kill Command Attack:** Using this command tag can be easily disabled. When any Tag is manufactured they protect tag write mode by password, but due to limited memory and processing it can be easily cracked with brute forced method. So any one can apply brute force on it from different place and can permanently disable tag.

c) **De-synchronizing Attack:** One effective jamming technique known as the de-synchronization attack permanently disables the authentication capability of a RFID tag by destroying synchronization between the tag and the RFID reader.

2) **802.15.4:** The IEEE standard 802.15.4 is mainly aimed to work with low power and low cost devices [4]

a) **Wide-Band Denial and Pulse Denial:** The easiest method of jamming traffic is to simply block the entire RF spectrum. This results in a total loss of the affected spectrum to all users. A generic RF generator could be used for this, but an even cheaper option is to use the 802.15.4 transceiver chips.

b) **Node-Specific and Message-Specific Denial:** For pure disruption this would be effective, but more interesting and useful applications wish to deny specific messages. This is accomplished by reading the first several bytes of the 802.15.4 Medium Access Control (MAC) header, which includes information such as the frame type and addressing information. It is possible to receive these bytes in the attacking node, and decide on the action to take, such as only jamming data being sent to a certain address.

c) **Bootstrapping Attacks:** During initial network setup (bootstrapping) some method of configuring two nodes to securely join up is required. On very resource-constrained nodes this could simply be two push-buttons on each node, which when pressed puts the nodes in a special join mode. This system relies on an attacker not being present during this initial configuration, which may be 'secure enough' for simple applications such as remote controls. The ZigBee standard uses such a system for device bootstrapping

B. DDoS on Network Layer:

The communication technologies related to the sensor networks usually include Bluetooth, IrDA, Wi-Fi, ZigBee, RFID, NUWB, NFC, Wireless Hart etc. Table 2 Shows Types of attack on Network Layer

Type Of Attack	Description
Flooding Attacks	This type of attack attacker disrupting authenticate user's connectivity by exhausting victims network's bandwidth e.g.: UDP flood, ICMP flood, DNS flood etc.
Reflection-based flooding Attacks	This type of attack attacker send fake replicated request instead of original direct request to reflectors which is routing component; hence, those reflectors sends their replies to victims and exhaust victim's resources e.g.: Smurf attack
Protocol Exploitation flooding attacks	This type of attack attacker exploit some specific features or implementation bugs of victim's protocols in order to consume excess amount of victim's resources e.g.: SYN flood, TCP SYN-ACK flood, ACK PUSH flood etc.
Amplification-based flooding attacks	This type of attack attacker tries to exploit application to generate message or multiple messages they receive to amplify traffic toward the victim. BOTNET is widely used for both amplification and reflection purpose.

Table 2: DoS/DDoS Attack at Network Layer

In IoT network there is one border gateway router which communicates with sensor from perception layer and forward this data to and from upper application layer.

1) ***Wi-Fi*** [5]**:**

A Network layer DoS attack can be carried out on a wired or wireless network. If a wireless network allows any client to associate to it, the wireless network could be vulnerable to a network layer attack. A network layer DoS attack is achieved by sending a large amount of data to a wireless network. This type of attack targets the wireless network infrastructure of the victim. A good example of a network layer attack is the ICMP flood

The ICMP flood attack works by an attacker sending so many ICMP ECHO REQUEST packets to the target wireless system that it cannot respond fast enough to ease the amount of traffic. If the attacker spoofs the source IP address, then the attacker can use all of its resources to just send packets, while the target wireless system has to use all of its resources to process the packets.

2) *ZigBee[6]:*

ZigBee is the only standards-based wireless technology designed to address the unique needs of low-cost, low-power wireless sensor.

a) Hello Flooding:

- Attacker Nodes send “hello” to one-hop network Attacker replays “hello” with high power antenna.
- Creates false one-hop network
- Doesn’t require encryption breaking

b) Homing Attack:

Analyse traffic for special nodes (cluster heads, key managers) and DoS special nodes to shut down entire network.

c) Black Hole Attack:

Become part of many routes, drop all packets.

C. DDoS on Application Layer:

Application layer is top most layer contains user interface basic business logic of overall application. In this layer 2 type of attack can be happen.

1) Reprogramming Attack:

In this type of attack attacker get access of source code of original programming and attacker modifies the source code such that application goes into infinite loophole so that network resource become inaccessible, and request remain infinitely waiting for reply.

2) Path based DoS [7]:

Path based DoS is an adversary overwhelms sensor nodes a long distance away by flooding a multi-hop end-to-end communication path with either replayed packets or injected spurious packets.

IV. CONCLUSIONS

Internet of Thing is rapidly developing and become necessary and useful update in near future. With this popularity of IoT security concerned with it is play vital role. Prevent IoT from DoS/DDoS attack is not easy task, it faces so many challenges due to low power, low processing and low memory. In this paper we introduce some common DoS/DDoS attack which can be malfunction entire IoT network.

REFERENCES

[1]. A. Karila, S. Fdida, M. May, and M. Potts. A. Gavras, "Future Internet Research and Experimentation: The FIRE Initiative," ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 89-92, July 2007.

[2]. Shelby Z. (2013, June) Constrained Application Protocol (CoAP). Document. [Online]. https://tools.ietf.org/html/draft-ietf-core-coap-18

[3]. Musfiq R and Srinivas S Deepak T, "Technique for Preventing DoS Attacks on RFID Systems," in SoftCOM, Split, Dubrovnik, 2010, pp. 6-10.

[4]. C.P. O'Flynn, "Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks," in New Technologies, Mobility and Security (NTMS), Paris, 2011, pp. 1-5.

[5]. Stuart C. (2007, May) 802.11 Denial of Service Attacks and Mitigation. Document. [Online]. http://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108

[6]. Arindham G Krishna C. Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation. Document. [Online]. http://www.kaspersky.co.in/images/doddapaneni,_krishna_chaitanya_ghosh,_arindam__analysis_of_denial-of-service_attacks_on_wireless_sensor_networks_using_simulation.pdf

[7]. Richard H, Shivakant M Jing D. (2005, Nov) Defending against Path-based DoS Attacks in Wireless Sensor Networks. [Online]. http://www.cs.colorado.edu/~mishras/research/papers/sasn05.pdf

[8]. N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler M. Palattella: Standardized protocol stack for the internet of (important) things, Proceedings of IEEE,(2012) 1-18