DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5008

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURITY AND DDOS MECHANISMS IN INTERNET OF THINGS

Jeet kaur
M. Tech Student
Computer Science and Engineering Deptt.
PIET, Samalkha, Haryana, India

Dr Anju Bhandari Gandhi
Associate Professor
Computer Science and Engineering Deptt.
PIET,Samalkha, Haryana, India

***Abstract*:** Internet of Things refer as interconnection of smart item, protected from small espresso device to massive automobile, speak with every different with out human interactions also known as as Device to Device communications. In modern emerging global, all of the devices become smarter and might communicate with other gadgets as properly. With this speedy development of Internet of Things in one of a kind location like smart home, clever hospital and many others. It also have to face a few difficulty to securing overall privateness due to heterogeneity nature. There are such a lot of kinds of vulnerability but right here in this paper we pay attention on Distributed Denial of Service assault (DDoS). DoS is attack that may block the usage for real user and make network resource unavailable, consume bandwidth; if comparable assault is penetrated from exceptional resources its name DDoS.In this paper we will discuss various IoT security issues and Cryptographic Services to solve such issues.

Keywords: IoT, Fuzzy Logic, Security, Distributed Denial of Service,

1. INTRODUCTION

Technology turns into faster and smaller daily and moving towards "continually connected" version. This revolution makes every and each tool to communicate with each different and fabricate new future net. This new idea of future internet is known as Internet of Things [1]. Every device from mobile telephone to automobile, alarm clock to coffee machine will become related to net with open trendy IPv6 allowing specific addressing schema for them. IoT combine bodily matters 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. As it is a very active and new research field, a variety of questions need to be solved, at different layers of the architecture and from different aspects of information security, the following subsections analyze and summarize common challenges for security of IoT.

1.1 Security Structure

In the IoT will remain stable-persisting as a whole over time, putting together the security mechanism of each logical layer cannot implement the defense-in-depth of system[4], so it is a challenge and important research area to construct security structure with the combination of control and information.

1.2 Key Management

As key management is the important basis of security mechanism, it is always the area of research . It is still the most difficult aspect of cryptographic security.Presently the researchers don't find any ideal solution. Lightweight cryptographic algorithm or advanced performance of sensor node is still not applied. So far the real large-scale sensor network is seldom put into practice. The problems of network security will be paid more attention and turn into key points and difficulties of research in this network environment. Currently security law and regulations are still not the main focus, and there is no technology standard about the IoT. The IoT is related to national security information, business secrets and personal privacy. Therefore, our country needs the legislative point of view to encourage development of the IoT. Policies and regulations are urgently needed. In this aspect we have a long way to go.

2. SECURITY

In IOT The security of information and network should be ready with these properties such as detection, privacy, integrality and undeniability. Different from internet, the IoT will be applied to the vital areas of national economy, e.g., medical service and health care, and intellectual transportation, thus security needs in the IoT will be higher in accessibility and dependability [5].

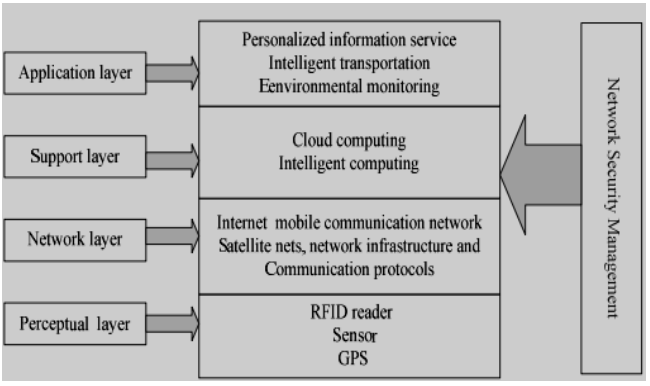

Figure 1. Security architecture of Internet of Things

2.1 Secure Architecture

In common the IoT can be divided into four key levels.
The most basic level is the perceptual layer (also known as recognition layer), which collects all kinds of information through physical tools and identify the physical world, the

information includes object properties, environmental situation etc; and physical equipments consist of RFID reader, all kinds of sensors, GPS and other equipments. The key element in this layer is sensors for capture and representing the physical world in the digital world. The second level is network layer. Network layer is responsible for the reliable transmission of information from perceptual layer, initial processing of information, organization and polymerization. In this layer the information transmission is relied on several basic networks, which are the internet, mobile communication network, satellite nets, wireless network, network communications and communication protocols are also necessary to the information substitute between devices. The third level is support layer. Support layer will set up a reliable maintain stage for the application layer, on this maintain stage all kind of intellectual computing powers will be controlled through network grid and cloud computing. It plays the role of combine application layer upward and network layer downward. The application layer is the highest and terminal level. Application layer provides the modified services according to the needs of the users. Users can access to the internet of thing through the application layer interface using of television, personal computer or mobile equipment and so on. Network security and organization play an significant role in above each level. Then we will analysis the security features.

2.2 Security Features

A. Perceptual Layer: As a rule perceptual nodes are tiny of computer influence and storage facility because they are trouble-free and with less influence Hence it is not capable to be relevant frequency hopping communication and public key encryption algorithm to security protection. And it is very complicated to set up security protection system. In the meantime attacks from the external network such as deny of service also bring new security problems. In the other hand sensor data still require the protection for integrity, dependability and privacy

B. Network Layer: Even though the core network has moderately absolute safety protection capability, but Man-in-the Middle Attack and counterfeit attack still exist, for the moment junk mail and computer virus cannot be ignored, a large number of data sending cause jamming. Hence security mechanism in this level is very essential to the IoT.

C. **Support Layer**: Perform the mass data processing and intellectual decision of network performance in this layer, intellectual processing is incomplete for malicious information, so it is a challenge to progress the ability to identify the malicious information.

D. Application Layer:In this level security needs for different application environment are different, and data sharing is that one of the characteristics of application layer, which creating problems of data privacy, access control and disclosure of information.

2.2.3 DDoS Attack in IoT To start with, Denial of Service (DoS) attack is defined as denying and disrupted valid get admission to to the provider or assets on the right track server. Even worse, Distributed Denial of Service (DDoS) attack commonly engages greater computer systems and net connections to such attacking behavior to engender actual threats that seriously blocks or suspends different users' accesses to the host server, which leads to massive business loss and consumer inconvenience. The focused provider may be disrupted by means of the assault crashing the host server with a few carefully designed packets whose content causes positive operating device to freeze or reboot. Other than that, the malicious packets occupy all of the resources at the host server with massive volumes of horrific requests, which is also called bandwidth assault in associated researches. Prevented with the aid of patching the host running machine in opposition to the identified attack, the first shape of attack will be stopped sooner or later. However, the big quantity-based totally assault is pretty hard to protection. A volume-based attack is generally initiated with putting in "bot" onto vulnerable systems. Bot generation turned into utilized in industry for automating manner. In such way, hackers can without problems populate their attacking military with zero price. Zombies' or bots' conduct will be manipulated thru secured channels in order to release similarly attacks to the focused IP or a local network. To specify the difficulties in finding answers, first, the aggregated large traffic extent exceeds throughput of many community protection gadgets and capacity of corporate internet link. Second, controlled zombie structures are geographically distributed, that is hard to find source IP addresses**.**Third, when separately examined, single attack from one source is not powerful enough to be discriminate from a legitimate request, which makes it look similar to a flash crowd created by legitimate requests at a website peak time [9].

2.3 Current DDoS Defense Strategies

Many DDoS defense strategies were proposed, implemented, and tested to be effective against DDoS attack over the Internet. In this phase, the maximum commonplace protection designs are to be reviewed for capability approach to the DDoS attack over an IoT network. Defensive techniques might be labeled by means of the collection of the attacking event. Before attack, preventive procedures have been delivered to eliminate the assault visitors. Attack detecting and figuring out mechanism is carried out to display the coming traffic. Three parameters are frequently examined in this link including useful resource IP deal with, visitors growing diploma, and similarity most of the site visitors. However, traffic diploma monitoring on occasion ought to reason false alarm because surprising traffic boom also can be the result of a flash crowd which consists of valid requests. Using the other two parameters, one might extra with a bit of luck distinguish among malicious site visitors and flash crowd. The similarity a number of the traffic of a DDoS assault is normally higher than that of flash crowd for 2 motives. First, attacking site visitors is generally generated with the aid of bots from one botnet, which shows high similarity in supply IP. Second, inside the cases that the attacking IP addresses are distributed from slave machines everywhere in the global, due to the fact all bots execute equal or similar supply code, the similarity in packet content material may also be better than those from a flash crowd. Some counter moves are taken to restriction malicious visitors. The most effective one is filtering out the packets from recognized spoofed IP addresses and losing them the use of unicast opposite route forwarding at routers. Attacks from valid IP addresses cannot be prevented in such. Firewall is a common alternatives which be used to forestall the visitors

upon recognized attackers' IP. There also are indirect strategies to remedy the DDoS hassle, as an example, the use of congestion manipulate to cut down the attacking site visitors float and growing the useful resource manufacturing at host server. However, this approach isn't pretty effective when the goal drift is small and similar to legitimate request and attacking system is quite dispensed. Some other method together with reconstructing the attacking direction to restrict quantity of packets going through, however this technique needs massive garage and computing assets for route mapping feature. Similarly, mining antique attacker facts and the use of their functions for packet sampling is likewise suggested in some researches. Even extra, by way of tracking lower back the attacking root, server can actively block the attack site visitors, which proved to be powerful defensive response mechanism

3. DDOS ATTACKS IN IOT

Now considering exceptional state of affairs of DDoS assault on IoT based network at distinct Layers. A. DDoS on Perception Layer:
1) RFID: At perception layer RFID is fundamental technology for reading data from sensor with out human interaction and contact. [3] A) Jamming: In this electromagnetic jamming is completed to prevent tags from communicating with reader.
B) Kill Command Attack: Using this command tag can be easily disabled. When any Tag is synthetic they guard tag write mode via password, but due to confined reminiscence and processing it could be easily cracked with brute pressured technique. So any person can apply brute force on it from special location and might completely disable tag. C) De-synchronizing Attack: One effective jamming method called the de-synchronization assault permanently disables the authentication functionality of a RFID tag through destroying synchronization between the tag and the RFID reader. **2)** 802.15.4: The IEEE general 802.15.Four is in particular aimed to work with low electricity and occasional fee gadgets [4] A) Wide-Band Denial and Pulse Denial: The easiest method of jamming visitors is to clearly block the complete RF spectrum. This effects in a complete lack of the affected spectrum to all users. A customary RF generator could be used for this, however an even cheaper choice is to use the 802.15.4 transceiver chips.

B) Node-Specific and Message-Specific Denial: For natural disruption this would be powerful, however greater interesting and useful packages desire to disclaim specific messages. This is completed with the aid of analyzing the first numerous bytes of the 802.15.4 Medium Access Control (MAC) header, which incorporates records consisting of the body type and addressing information. It is viable to get hold of these bytes inside the attacking node, and decide on the action to take, inclusive of handiest jamming records being sent to a sure deal with. C) Bootstrapping Attacks: During initial community setup (bootstrapping) a few technique of configuring nodes to soundly be a part of up is needed. On very resource-restrained nodes this can truely be pushbuttons on each node, which while pressed places the nodes in a special be a part of mode. This machine is based on an attacker now not being present at some point of this initial configuration, which may be „cozy enough? For easy packages along with far flung controls. The ZigBee standard makes use of this sort of machine for device bootstrapping .

3.1. DDoS on Network Layer

The verbal exchange technology related to the sensor networks typically include Bluetooth, IrDA, Wi- Fi, ZigBee, RFID, NUWB, NFC, Wireless Hart and so forth. Table 1 as shown belowgives the sorts of assault takes place in Network Layer. Table 1: DoS/DDoS Attack at Network Layer

Type Of Attack	**Description**
Flooding Attacks	This sort of attack attacker disrupting authenticate person's connectivity with the aid of laborious sufferers network's bandwidth. E.G.: UDP flood. ICMP flood, DNS flood and many others.
Reflection-based flooding Attacks	This type of attack attacker ship fake replicated request rather than original direct request to reflectors that's routing factor; consequently, the ones reflectors sends their replies to sufferers and exhaust sufferer's resources e.G.: Smurf attack
Protocol Exploitation flooding attacks	This sort of assault attacker make the most some precise features or implementation insects of victim's protocols on the way to eat excess quantity of victim's assets e.G.: SYN flood, TCP SYN-ACK flood, ACK PUSH flood and so on.
Amplification-based flooding attacks	This form of assault attacker attempts to take advantage of utility to generate message or multiple messages they get hold of to expand traffic toward the sufferer. BOTNET is broadly used for both amplification and reflection reason.

In IoT community there may be one border gateway router which communicates with sensor from perception layer and forward this statistics to and from higher software layer.

1)Wi-Fi [5]:
A Network layer DoS assault can be executed on a stressed out or wireless community. If a wireless network lets in any consumer to companion to it, the wireless community can be liable to a network layer attack. A network layer DoS assault is carried out by means of sending a large amount of records to a wireless network. This kind of attack goals the wi-fi community infrastructure of the victim. A precise example of a community layer assault is the ICMP flood. The ICMP flood attack works through an attacker sending so many ICMP ECHO REQUEST packets to the goal wi-fi device that it can not reply rapid enough to ease the amount of visitors. If the attacker spoofs the supply IP deal with, then the attacker can use all of its assets to simply send packets, while the goal wireless device has to use all of its sources to process the packets.

2) ZigBee[6]:
ZigBee is the simplest requirements-primarily based wireless technology designed to deal with the unique wishes of lowcost, low-power wi-fi sensor. A) Hello Flooding:
- Attacker Nodes send “hello” to at least one-hop community Attacker replays “hi there” with excessive strength antenna.- Creates fake one-hop network
- Doesn"t require encryption breaking
b) Homing Attack:
Analyse traffic for special nodes (cluster heads, key managers) and DoS unique nodes to shut down entire network. C) Black Hole Attack:
Become part of many routes, drop all packets.

3.2. DDoS on Application Layer:
Application layer is pinnacle maximum layer contains consumer interface basic commercial enterprise common sense of common utility. In this deposit 2 form of assault may be happen.
1) Reprogramming Attack:
In this sort of assault attacker get get admission to of supply code of original programming and attacker modifies the source code Such that application is going into limitless loophole so that network useful resource end up inaccessible, and request continue to be infinitely waiting for respond.
2) Path based DoS [7]:
Conventional DDoS preventive measures and defenses too carefully rely on electricity supply, computing property, and longtime processing. Considering the traits of IoT environment, all such preconditions have to be avoided inside the layout of IoT defense tool. One needs to preserve it in thoughts that IoT hardware components are incredibly heterogeneous and very constrained in energy deliver and computing functionality while evaluating to traditional nodes over the internet which includes personal pc systems, smart cellular telephone, and pills. Other than that, keeping real-time conversation in IoT network is fairly crucial, longtime processing will motive put off and goal omit at some stage in the venture of identifying malicious site visitors

4. CONCLUSION

Conventional DDoS preventive measures and defenses too closely depend upon electricity deliver, computing assets, and longtime processing. Considering the characteristics of IoT environment, all such preconditions have to be avoided inside the design of IoT defense device. One needs to hold it in mind that IoT hardware components are distinctly heterogeneous and very constrained in energy deliver and computing capability when comparing to standard nodes over the net inclusive of non-public computer systems, clever cellphone, and drugs. Other than that, preserving actual-time verbal exchange in IoT community within reason critical, longtime processing will reason put off and goal omit throughout the undertaking of figuring out malicious site visitors. Considering all the device and environment constraints of IoT network, implementing light weight protecting mechanism for node gadgets is the first key for the design. Additionally, dispensing defending mechanism across the multi-layer structure of IoT is likewise applicable as the second one key to the answer. Third, adding more security gadgets in a small subnet as a checking center is likewise viable. Such device could be accountable for examining packets, keeping facts of antique attacking facts, and monitoring back the root of attacks to proactively reject chance in the future. Since the security mechanism is predicated on a small organization of nodes whose computing resources are separated from the overall IoT information collecting nodes, it would be fee-efficient to enable such mechanism on a small percent of hardware in preference to all devices over the IoT community.

Table 2.: About various DDoS Defense Mechanisms

Traceback Method	**Hop Count Filtering [9-11]**	**ICMP [12,13]**	**Logging [14,15]**	**Packet Marking [16-23]**	**Packet Marking & Logging [24]**	**FDDA [25]**
ISP involvement	None	Low	Moderate	Low	None	None
No. of attack packets needed for traceback	1	Very Large	1	Very Large	1	Large
Processing overhead	Very Low	Low	Low	Low	Very Low	High
Storage	Very Low	Low	Low	High	High	High
Ease of implementation	Yes	Yes	Yes	No	No	No
Scalability	Highest	High	Fair	High	High	Highest
Bandwidth overhead	None	Low	None	None	None	High
No. of functions needed to implement	3	2	3	2	5	6
Ability to handle major DDOS attack	Yes	Yes	Yes	Poor	Yes	Yes
Classification	IDS Based	Proactive	IDS Based	Proactive	IDS Based	IDS Based
OSI model layer and protocols	IP. Network Layer	ICMP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer

REFERENCES

[1] Gavras, Anastasius, Arto Karila, Serge Fdida, Martin May, and Martin Potts. "Future internet research and experimentation: the FIRE initiative." ACM SIGCOMM Computer Communication Review 37, no. 3 (2007): 89-92.

[2] Onar, Krushang, and Hardik Upadhyay. "A survey: DDOS attack on Internet of Things." International Journal of Engineering Research and Development 10, no. 11 (2014): 58-63.

[3] Tagra, Deepak, Musfiq Rahman, and Srinivas Sampalli. "Technique for preventing DoS attacks on RFID systems." In Software, Telecommunications and Computer Networks (SoftCOM), 2010 International Conference on, pp. 6-10. IEEE, 2010.
O'Flynn, Colin P. "Message denial and alteration on IEEE 802.15. 4 low-power radio networks." In New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on, pp. 1-5. IEEE, 2011.

[5] Sonar, Krushang, and Hardik Upadhyay. "A survey: DDOS attack on Internet of Things." International Journal of Engineering Research and Development 10, no. 11 (2014): 58-63. Doddapaneni, Krishna, and Arindam Ghosh.

[6] "Analysis of Denial-of-Service attacks on Wireless Sensor Networks using simulation." IT Security for the Next Generation-European Cup 2011 (2011).

[7] Deng, Jing, Richard Han, and Shivakant Mishra. "Defending against path-based DoS attacks in wireless sensor networks." In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 89-96. ACM, 2005.

[8] Palattella, Maria Rita, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. "Standardized protocol stack for the internet of (important) things." IEEE communications surveys & tutorials 15, no. 3 (2013): 1389-1406.

[9] Wang, Haining, Cheng Jin, and Kang G. Shin. "Defense against spoofed IP traffic using hop-count filtering." IEEE/ACM Transactions on Networking (ToN) 15, no. 1 (2007): 40-53.

[10] Borah, Satya J., Sanjay Kumar Dhurandher, Isaac Woungang, and Vinesh Kumar. "A game theoretic context-based routing protocol for opportunistic networks in an IoT scenario." Computer Networks (2017).

[11] Hui, Jonathan W., Wei Hong, and Jean-Philippe Vasseur. "Recording packet routes using bloom filters." U.S. Patent 9,455,903, issued September 27, 2016.

[12] Izaddoost, Alireza, Mohamed Othman, and Mohd Fadlee A. Rasid. "Accurate ICMP traceback model under DoS/DDoS attack." In Advanced Computing and Communications, 2007. ADCOM 2007. International Conference on, pp. 441-446. IEEE, 2007.

[13] Gamundani, Attlee M., and Andreas Joseph. "An Analysis of Network Defensive Techniques Towards Organisational Security." (2016).

[14] Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." Computer 50, no. 2 (2017): 76-79.

[15] Singh, Jatinder, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers. "Twenty security considerations for cloud-supported Internet of Things." IEEE Internet of Things Journal 3, no. 3 (2016): 269-284.

[16] Yu, Shui, Wanlei Zhou, Song Guo, and Minyi Guo. "A feasible IP traceback framework through dynamic deterministic packet marking." IEEE Transactions on Computers 65, no. 5 (2016): 1418-1427.
1Park, PyungKoo, HeeKyoung Yi, SangJin Hong, and JaeCheul

[17] Prakash, P. Banu, and ES Phalguna Krishna. "Achieving High Accuracy in an Attack-Path Reconstruction in Marking on Demand Scheme." i-Manager's Journal on Information Technology 5, no. 3 (2016): 24.

[18] Doss, Srinath, Sreekumar Narayanan, and John Anand. "Detecting IP Spoofing using Hop Count Filtering based dynamic path update approach." Journal of Multidisciplinary Engineering Science Studies 3, no. 1 (2017).

[19] Bhavani, Y., V. Janaki, and R. Sridevi. "Survey on Packet Marking Algorithms for IP Traceback." (2017).

[20] Cheng, Long, Dinil Mon Divakaran, Aloysius Wooi Kiak Ang, Wee Yong Lim, and Vrizlynn LL Thing. "FACT: A Framework for Authentication in Cloud-Based IP Traceback." IEEE Transactions on Information Forensics and Security 12, no. 3 (2017): 604-616.

[21] Brust, Matthias R., and Ankunda R. Kiremire. "A Concise Network-Centric Survey of IP Traceback Schemes based on Probabilistic Packet Marking." arXiv preprint arXiv:1601.08011(2016).

[22] Saurabh, Samant, and Ashok Singh Sairam. "Increasing Accuracy and Reliability of IP Traceback for DDoS Attack Using Completion Condition." IJ Network Security 18, no. 2 (2016): 224-234.

[23] Suresh, S., and N. Sankar Ram. "A Review on Various DPM Traceback Schemes to Detect DDoS Attacks." Indian Journal of Science and Technology 9, no. 47 (2016).

[24] KrishnaKumar, Bharathi, P. Krishna Kumar, and R. Sukanesh. "Hop count based packet processing approach to counter DDoS attacks." In Recent Trends in Information, Telecommunication and Computing (ITC), 2010 International Conference on, pp. 271-273. IEEE, 2010.

[25] Park, PyungKoo, HeeKyoung Yi, SangJin Hong, and JaeCheul Ryu. "An effective defense mechanism against DoS/DDoS attacks in flow-based routers." In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, pp. 442-446. ACM, 2010.