Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

DoS Attacks in Internet of Things

Vahid Shaker
Azad University,
Science & Research Branch (SRBIAU)
Tehran, Iran

Houman Zarrabi
Iran ICT Research Center (ITRC)
Tehran, Iran
h.zarrabi@itrc.ac.ir

Abstract: The Internet of Things (IoT) defines a highly interconnected network of heterogeneous devices where all kinds of communications seem to be possible, even unauthorized ones. As a result, the security requirement for such network becomes critical whilst common standard Internet security protocols are recognized as unusable in this type of networks, particularly due to some classes of IoT devices with constrained resources. Due to the limitations of energy, computation and storage for sensors, although IoT have been widely deployed in many applications such as military, ecological and health-related areas. It is a critical challenge to present the effective and lightweight security protocol to prevent various attacks for IoT, especially for the denial of service (DoS) attack. Normally, the adversaries compromise sensors and launch the DoS attack by replaying redundant messages or making overdose of fake messages. In this paper, we explore the scope of the DoS attack problem in IoT. First we outline the constraints, security requirements, and then explore types of DoS attacks in IoT.

Keywords: Internet of Things (IoT); Security, Denial of Service Attack

I. INTRODUCTION

The concept of "Internet of Things" derives firstly from Sensor Networks and Radio Frequency Identification (RFID). Its principle is to conduct long-distance identification and processing over the information from sensor networks and RFID with the help of the network technology. In the year of 2005, International Telecommunication Union (ITU) released an annual report on "Internet of Things" [1]. In the report, ITU pointed that RFID and Intelligent Computing Technology had opened an era that interconnecting global things altogether. Meanwhile, the development of information and communication technology had been extended from connecting every person to connecting everything, at any time and any place. IoT has been variously defined. The ITU defined IoT as the development of item identifications, sensor technologies and the ability to interact with the environment [1]. The European Commission similarly describes IoT as "things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."

The Internet of Things domain will encompass an extremely wide range of technologies, from extremely constrained to unconstrained, from hard real time to soft real time. IoT, because of their potential for physical isolation, may be more vulnerable to attack. In addition, due to their characteristic low processor capability, IoT do not have the capacity to utilize sophisticated anti-intrusion prevention technologies.

In classical applications of IoT, where the Internet were used only as a transporting medium of sensing reports to the task manager, adversaries were obliged to access the network physically, so that they could successfully attack it. By opening IoT to the Internet, security and privacy problems get amplified as IoT in such a case are prone also to external threats that may be launched remotely by any malicious host in the Internet. Indeed, the main source of vulnerabilities of the integration of IoT to the Internet is the asymmetric nature of the communications between constrained sensor nodes situated in a lossy IoT network and powerful Internet hosts that belong to less constrained networks. Notably, the necessity of the fragmentation of long incoming IPv6 packets, present another source of vulnerability [2], since it opens the door to several forms of Denial of Service attacks.

In IoT every smart thing/object could be connected to the global Internet and is able to communicate with other smart objects, resulting in new security and privacy problems, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by 'things/objects'. Privacy of humans and things must be ensured to prevent unauthorized identification and tracking. In this context, the more autonomous and intelligent "things/smart objects" get, problems like the identity and privacy of things emerge, and accountability of things in their acting will have to be considered.

IoT offers connectivity for both human-to-machine and machine-to-machine communications. In the near future, everything is likely to be equipped with small embedded devices which are able to connect to the Inter net. Such ability is useful for various domains in our daily life: i.e. from building automation, smart city, and surveillance system to all wearable smart devices. However, the more IoT devices are deployed, the greater our information system is at risk. Indeed, a non-negligible number of devices in IoT are vulnerable to security attacks, for example, denial of service and replay attacks, due to their constrained resources and the lack of protection methods. This kind of attacks leads to sensor battery depletion and results in poor performances of sensing applications. In more serious cases, information leak from such tiny devices can expose sensitive data to the outside [3].

The rest of the paper is organized as follows. Section II represents the related work. .In Section III, various constraints in IoT related to attack mitigation are discussed. Section IV shows security requirements. Section V discusses DoS attacks in IoT. Lastly in Section VI, conclusion is discussed.

II. RELATED WORKS

There have been several conducted studies and surveys that are relevant to the security in IoT. Authors in [4] propose a solution that uses DTLS to secure end-to-end communications between a sensor node and an Internet host, while protecting the 6LoWPAN network against DoS attacks that may be

launched by malicious Internet hosts that intend to overload the sensor node by forcing it to open too many sessions, which leads to an excessive consumption of memory and energetic resources, causing the unavailability of the service. This protection is materialized by the introduction of peer authentication at network level between the base station and the Internet host. Boudguiga et al. [5] propose a new key establishment, called SAKE (Sever Assisted Key Establishment) based on the MIKEY-Ticket mode but removing the threat of DoS attacks. SAKE allows establishing security associations between the two parties after only five exchanged messages, compared to six messages in the original MIKEY-Ticket.

Wang et al. [6] gave a very detailed survey of security issues in wireless sensor networks, which can be considered as a reference for IoT. The authors identified the constraints and the requirements based on the existing attacks against IoT at different layers. They also presented the key management systems in WSN according to the employed cryptographic primitives. Atzori et al. [7] focused on authentication, data integrity and privacy issues in IoT, particularly in RFID systems and sensor networks. Kumar et al. in [8] gave a general overview of security and privacy issues in IoT. They provided a description of different security threats and privacy concerns while processing, storing, and transmitting data. Existing surveys in relation with IoT security is that they generally focus on identifying the challenges and the security threats present in IoT.

III. CONSTRAINTS IN IOT

Individual sensor nodes in IoT are inherently resource constrained. They have limited processing capability, storage capacity, and communication bandwidth. Each of these limitations is due in part to the two greatest constraints- limited energy and physical size. The design of security services in IoT must consider the hardware constraints of the sensor nodes:

• **Energy:** Energy is the important constraint for IoT. Energy consumption in sensor nodes used in IoT can be categorized in three parts: Sensor transducer, Communication among sensor nodes, microprocessor computation. The study in [9] found that each bit transmitted in communication among sensor nodes consumes about as much power as executing 800–1000 instructions. Thus, communication is more costly than computation in IoT. Any message expansion caused by security mechanisms comes at a significant cost. Further, higher security levels in IoT usually correspond to more energy consumption for cryptographic functions.

• **Computation:** the embedded processors in sensor nodes are generally not as powerful as those in nodes of a wired or ad hoc network. As such, complex cryptographic algorithms cannot be used in IoT. Due to Limited capability of sensor nodes, conventional security mechanisms with large computation and overhead of communication are inappropriate in IoT.

• **Memory:** memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There is usually not enough space to run complicated algorithms after loading OS and application code. In the Smart Dust project, for example, Tiny OS consumes about 3500 bytes of instruction memory, leaving only 4500 bytes for security and applications [9]. This makes it impractical to use the majority of current security algorithms [10]. With an Intel Mote, the situation is slightly improved, but still far from meeting the requirements of many algorithms.

• **Unreliable communication:** Unreliable communication is a dangerous threat to sensor security. Normally connectionless protocol is unreliable. Packets may get impaired due to highly congested nodes and channel errors. Besides, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Simple error handling scheme implementation may generate high overhead. In Some situation though the channel is reliable, the communication may not be possible. The packets may collide in transfer and may need retransmission due to the broadcast nature of wireless communication [11], [12].

• **Transmission range:** the communication range of sensor nodes is limited both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather and terrain.

IV. SECURITY REQUIREMENTS

IoT is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of IoT as encompassing both the typical network requirements and the unique requirements suited solely to IoT networks. The goal of security services in IoT is to protect the information and resources from attacks and misbehavior. The security requirements in IoT include:

• **Availability:** which ensures that the desired network services are available even in the presence of denial-of-service attacks. The sensor nodes must be available when needed. High availability network of things should remain functional, especially against denial-of-service attacks, such as flooding of incoming messages to targeted nodes forcing them to shut down

• **Authorization:** which ensures that only authorized sensors can be involved in providing information to network services. IoT devices should be able to verify whether certain entities are authorized to access their measured data. At the network layer, only authorized devices should be able to access IoT network. Unauthorized devices should not be able to route their messages over IoT devices, because it may deplete their energy.

• **Authentication:** which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.

• **Confidentiality:** is the most important issue in network security. Every network with any security focus will typically address this problem first which ensures that a given message cannot be understood by anyone other than the desired recipients. Exchanged messages in IoT may need to be protected. An attacker should not gain knowledge about the messages exchanged between a sensor node and any other Internet entity.

• **Integrity:** which ensures that a message sent from one node to another is not modified by malicious intermediate nodes. Thus, integrity ensures that any received data has not been altered in transit.

• **Nonrepudiation:** which denotes that a node cannot deny sending a message it has previously sent.

• **Freshness:** which implies that the data is recent and ensures that no adversary can replay old messages. This is important to secure the communication channel against replay attacks.

V. DoS ATTACKS IN IoT

In this section we first define and explore attack concept and then present Types of DoS attacks in IoT.

A. Attack Concept

Attacks include any action that intentionally aims to cause any damage to the network. They can be divided according to their origin or their nature. An origin-based classification splits attacks into two categories, external and internal, whereas a nature-based classification splits them into passive attacks and active attacks.

External attacks: Includes attacks launched by a node that does not belong to the logical network, or is not allowed to access to it.

Internal attacks: Includes attacks launched by an internal compromised or malicious node. This is a more severe type of threat since the proposed defense toward external attacks is ineffective against compromised and internal malicious nodes.

Passive attacks: A passive attack is a continuous collection of information that might be used later when launching an active attack. For that, the attacker eavesdrops packets and analyzes them to pick up required information. Due to the nature of the wireless communication medium which is widely shared, it is easier for an attacker to launch such an attack in this environment than in traditional wired environments. The security attribute that must be provided here is information confidentiality.

Active attacks: Includes almost all other attacks launched by actively interacting with victims, such as: sleep deprivation torture, which targets the batteries; hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them; jamming, which causes channel unavailability by overusing it, attacks against routing protocols that we will see in the next section, etc. Most of these attacks result in a denial of service, which is a degradation or a complete halt in communication between nodes.

B. Types of DoS Attacks in IoT

DoS attack attempts to make the resources in the network unavailable to the authorized users. For example, a resource consumption attack is considered as one type of DoS. This attack is continuously sending packets to a node in order to consume its resources and waste the network bandwidth [13]. DoS attack is an impelling inside attack in the form of interference or collision at the receiver side, which can causes serious damage to the functions of IoT. Iot networks are susceptible to DoS attacks since they rely on deployed miniature energy-constrained devices to perform a certain task without a central powerful monitoring point [14] [15]. DoS attacks are a particularly great threat to IoT. The attack involves overloading or crashing the target device with a flood of requests, causing it to become unavailable.

Jamming: In this type of DoS attack occupies the communication channel between the nodes thus preventing them from communicating with each other.

Node tampering: Physical tampering of the node to extract sensitive information is known as node tampering.

Collision: This type of DoS attack can be initiated when two nodes simultaneously transmit packets of data on the same frequency channel. The collision of data packets results in small changes in the packet results in identification of the packet as a mismatch at the receiving end. This leads to discard of the affected data packet for re-transmission [16].

Unfairness: As described in [16], unfairness is a repeated collision based attack. It can also be referred to as exhaustion based attacks.

Battery Exhaustion: This type of DoS attack causes unusually high traffic in a channel making its accessibility very limited to the nodes. Such a disruption in the channel is caused by a large number of requests (Request To Send) and transmissions over the channel.

Hello Flood Attack: This attack causes high traffic in channels by congesting the channel with an unusually high number of useless messages. Here a single malicious node sends a useless message which is then replayed by the attacker to create a high traffic.

Homing: In case of homing attack, a search is made in the traffic for cluster heads and key managers which have the capability to shut down the entire network.

Selective Forwarding: As the name suggests, in selective forwarding, a compromised node only sends a selected few nodes instead of all the nodes. This selection of the nodes is done on the basis of the requirement of the attacker to achieve his malicious objective and thus such nodes does not forward packets of data.

Sybil: In a Sybil attack, the attacker replicates a single node and presents it with multiple identities to the other nodes.

Acknowledgement Flooding: Acknowledgements are required at times in sensor networks when routing algorithms are used. In this DoS attack, a malicious node spoofs the Acknowledgements providing false information to the destined neighboring nodes.

De-Synchronization: In de-synchronization attack, fake messages are created at one or both endpoints requesting retransmissions for correction of non-existent error. This results in loss of energy in one or both the end-points in carrying out the spoofed instructions.

Unauthorized Tag Disabling (Attack on Authenticity): The DoS attacks in the RFID technology leads to incapacitation of the RFID tags temporarily or permanently. Such attacks render a RFID tag to malfunction and misbehave under the scan of a tag reader, its EPC giving misinformation against the unique numerical combination identity assigned to it. These DoS attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

Sinkhole (Black Hole): In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information [17]. The end result is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple, as all traffic from a large area in the network will flow through the adversary's node. In such type of attacks the eavesdropper act like a black hole, where the eavesdropper listen the route request packets from its neighbors and reply them back using fake/wrong information about shortest route toward sink node. Data movement towards sink can be done by every node in its surrounding set the attacker as a next node. Any node wants to send data to a base station will forward it towards attacker. This offers the attacker to analyze these packets and extract vital information [18].

Wormhole: This DoS attack causes relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunneling of bits of data over a link of low latency.

DoS Attacks Using Modification: DoS attacks can be launched by modifying routing information [19], such as altering control message fields of data packets or forwarding routing messages with falsified values.

Tunneling: Two remote nodes may collaborate to encapsulate and exchange messages between them through existing data routes, and make impressions as they are adjacent. Therefore, they may collaborate to falsely represent the length of available paths by encapsulating and tunneling between them legitimate routing messages generated by other nodes, preventing the intermediate nodes from correctly incrementing the metric used to measure path lengths (such as hop count).

Attacks Using Fabrication: This class includes attacks based on the generation of false routing messages. Such attacks are difficult to detect.

Rushing Attacks: Recently, Hu et al. [20] have defined a new attack called a rushing attack. In almost all on-demand routing protocols, to limit the route discovery overhead each node forwards only one RREQ originated from any route discovery, generally the first one received. This property can be exploited by rushing the forwarding of received RREQs. For a route discovery, if the RREQs forwarded by the attacker are the first to reach each neighbor of the target, then any route obtained by this route discovery will include the attacker. That is, when a neighbor of the target receives the rushed RREQ from the attacker, it forwards that RREQ, and will not forward any further RREQ from this route discovery. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes). In general terms, an attacker that can forward RREQs more quickly than legitimate nodes can launch such an attack and include itself in all the discovered routes.

Neglect and Greed Attack: This attack occurs at the network layer. When a packet is transmitted from a sender to a receiver, then in between both these nodes, there occur a number of other nodes through which the packet is routed before reaching to the final destination. Transmission is said to be successful when the packet is completely reached to its destination. In the meanwhile, malicious node can force multi-hopping in the network, either by splashing some packets or by routing the packets towards a wrong node. This attack disturbs the behavior of the adjoining nodes, which may not be able to receive or send messages.

Interrogation: An interrogation attack imposes on the two way handshake (request-to-send/clear-to-send) that several MAC protocols use to reduce the hidden-node problem. An adversary can misuse a node's resources by frequently sending RTS messages to obtain CTS responses from a directed adjoining node.

VI. CONCLUSIONS

If no security mechanisms are applied in IoT, the applications of intelligent traffic, intelligent medical treatment, public safety of city, logistics management and intelligent production process management based on IoT will cause many security problems and the development of IoT will be delayed. In this paper we surveyed DoS attacks existing in Internet of Things that may prove to be very detrimental in the development and implementation of IoT in the different fields.

VII. REFERENCES

[1] International Telecommunication Union. ITU Internet Reports 2005. The Internet of Things. 2005.

[2] R. Hummen, J. Hiller, H. Wirtez, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN fragmentation attacks and mitigation mechanisms, in: The Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2013.

[3] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, journal of Ad Hoc Networks, Survey on secure communication protocols for the Internet of Things, 2015.

[4] T. Kothmayr,C. Schmitt, W. Hu, M. Brunig, G. Carle, DTLS based Security and Two-Way Authentication for the Internet of Things, Ad Hoc Networks 11 (8) (2013) 2710–2723.

[5] A. Boudguiga, A. Olivereau, N. Oualha, Server assisted key establishment protocol for WSN: a MIKEY-ticket approach, in: 12th IEEE Trustcom, 2013.

[6] Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Commun. Surv. Tutorials 8 (2). (2006).

[7] L. Atzori, A. Iera, G. Morabito, The Internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[8] S. A. Camtepe, B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: A Survey, Technical Report TR-05-07, Rensselaer Polytechnic Institute, 2005.

[9] J. Hill et al., "System Architecture Directions for Networked Sensors," ASPLOSIX: Proc. 9th Int'l. Conf. Architectural Support for Programming Languages and Operating Systems, New York: ACM Press, 2000, pp. 93–104.

[10] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 521–34.

[11] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey," chapter 17, Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. Auerbach Publications, CRC Press 2006.

[12] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, 38(4):393–422, 2002.

[13] C. Karlof, N. Sastry, and D. Wagner, " TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", ACM SenSys'04, November 2004, pp. 162–175.

[14] Raymond, D.R. and Midkiff, S.F., "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", Pervasive Computing, 2008, vol. 7, Issue 1, pp. 74 - 81

[15] David R. Raymond and Scott F. Midkiff, "Denial of service in sensor networks". Computer ISSN 0018-9162, IEEE Computer Society, 2002, vol. 35, pp. 54-62.

[16] Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg, "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology; eISSN: 2319-1163 | pISSN: 2321-7308.

[17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, May 2003.

[18] Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala, Security Against Black Hole Attack In

[19] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," 10th IEEE Int'l. Conf. Network Protocols (ICNP '02), Nov. 2002.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Wksp. Wireless Security WiSe 2003, San Diego, CA, USA, Sept. 2003.