Indonesian Journal of Electrical Engineering and Computer Science
Vol. 5, No. 1, January 2017, pp. 181 ~ 186
DOI: 10.11591/ijeecs.v5.i1.pp 181-186

Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security

Syed Umar[1], P. Gayathri[2], N. Bashwanth[3], Royyuru Srikanth[4]
[1]Department of Computer Science Engineering, MLRIT, Hyderabad
[2]Department of Information Technology, GRIET, Hyderabad
[3]Department of Information Technology, IARE, Hyderabad
[4]Department of Computer Science Engineering, KL University, Vaddeswaram
*Corresponding author, e-mail: umar332@gmail.com

Abstract

The emergence of wireless sensor networks as one of the technology trends in the coming years, and some special tests of safety. The event will be thousands of tiny sensors that cheap devices, memory, radio and make, in most cases, no access to the production and energy. Some great challenges of sensor networks are different; we focus on security in the form of wireless sensor networks. To some network wireless sensor network in order to optimize use of the sensor, so that the network can be as long as possible. But the management of the important mission of the sensor network, denial of service (DoS) attacks against the destruction of the efficient use of network resources and the vital functions of the network. DoS attacks can be one of the greatest threats to security threats be considered. In fact, there are many different layers of the OSI-DOS.

Keywords: *data security, DoS attacks, network layer, TCP/IP*

1. Introduction

Wireless sensor networks consist of thousands of small devices called spatially distributed sensor nodes, or motes, sensors, networking and the ability to follow each of them, the environment of the real world, where these radio waves calculation. WSN can be used in many applications such as the military presence on the battlefield services, safety, health and environmental crisis and various interfaces. If the wireless font sensor networks, such as low cost, low power consumption, and a part that have become daily, and attention to the great work of people in the draw area. WSN are harmful for the correct functioning, including, essential environmental safety mechanisms for all types of sensor networks. But the WSN node open limited resources sensors and communication channels with no multi-hop wireless, it is increasingly difficult security problems in WSN. The network will be relatively easy in danger, that is, the branches of the control and the opponent can be easily obtained full access to the node. Therefore all changes and reset the data nodes are addressed, including the encryption keys. Together attacks overload of requests to the target system so that they can respond to legitimate traffic. Therefore, in fact, a system, or some other service nodes is legitimate sensors. In this book, Denial of Service is considered mainly because their protocols energy efficiency target for wireless sensor networks is unique. One purpose of this book is to provide an overview of DoS WSN on the Open Systems Interconnection (OSI) model based attacks.

2. Wireless Sensor Networks Security Goals

WSN is a different type of network, such as the typical computer network that many similarities between them, but also many features that are also unique shares. WSN security to protect the information and the means of attack, and behavior [1] node. It is important to ensure the safety of WSN.

2.1. Privacy of Data

Confidentiality is a possibility of the message is sent to the passive attacker over the network. Only the receiver understands the message. This problem is very safe. In this WSN,

Received July 12, 2016; Revised October 10, 2016; Accepted November 1, 2016

you can solve these confidentiality requirements. The sensor does not need to go to the neighbors. For example, the use of sensitive military inject malicious nodes emission, confidentiality prevents access to information from other nodes. Development and maintenance of confidentiality is necessary when public information and the identity of the distributed main focal point, to establish a secure communication channel sensors.

2.2. Integrity of Data

The mechanism should ensure that each organization each message travels from sender to recipient can run. The integrity of data is, even if lost the position of the confidentiality of the following reasons:
1. The malicious node in the syringe passed on to the network.
2. An alarm, and the damage or cause uncontrollable wireless channel is activated.

2.3. Data Accessing

The goal is to ensure that the service should be available at any time WSN, but it is an internal or external attack, such as Denial of Service (DOS). Another approach has been proposed by researchers in order to achieve this goal. Although some mechanisms of communication between the nodes in order to ensure a central access management for the success of each message to the recipient. The fact that the winner of the leaders of available access point or group of threats from the entire sensor network. Availability is very important that the network is functioning.

2.4. Authentication of Data

Authentication ensures that the message is an authorized user. WSN attack not only the change in the size of the packet network packet. Both references verify the identity of the sender. For symmetric or asymmetric mechanism for the sending and receiving nodes, which encrypts to calculate the shared secret message authentication code (MAC) Powers? Various methods have been developed to use the secret key researchers, but the energy sensors and design constraints uncomfortable encryption techniques are complex.

2.5. Avoiding Old Data

The freshness of the data means that the data and the last in order to ensure that the message is not repeated opponent. In order to tackle the problem, at such a time or against Unsigned Properties need to be added to each packet in order to check the freshness of the package.

3. Attack of DoS in WSN

Denial-of-Service [DoS] attack events to reduce eliminate or prevent the normal use of the Internet. Private Service resource DOS attack legitimate users can be expected under normal circumstances. Therefore, a system or service to the user. Inside the DOS place as a consequence of a hardware failure, software failure, the Austin, environmental conditions, or a complex combination of these factors EXH. Dos outer shell, as the company's enemy, known as a DOS attack.

The main types of DoS attacks:

1. Consumption of scarce, limited, or non- renewable resources like bandwidth or processor time
2. Destruction or alteration of configuration information between two machines
3. Disruption of service to a specific system or person
4. Disruption of routing information.
5. Disruption of physical components

These three types of attacks against flooding, the first sensor wireless sensor network, it is important not to have sufficient resources online.

4. Attacks of DoS at Various Conditions

The sensor networks are usually divided into layers and layered architecture WSN vulnerable to DoS attacks can cause any level of the sensor network. Essay low categorization ace of DoS attacks was proposed by Wood and Stankovic [2]. Later, Raymond Midkiff [3] extended poll with some updated information. In this article, denial of service attacks is made on separate layers and the possible countermeasures.

4.1. Physical Layer

The physical layer is responsible for the selection of the frequency, the carrier frequency generation, signal detection, modulation, and encoding of the data [4]. The nodes in WSN can be deployed in a hostile and insecure environment in which the attacker has physical access. Two types of attacks on the physical level:

4.1.1. Jamming

This denial of service attack, the enemy tries hamper the functioning of the network broadcasting the high-energy signal. Even with the less powerful sources of interference, the opponent can potentially disrupt network communication by spreading disturbing means. Jammers attacks can be further classified as:

1. Constant, who harms are sent to the packages
2. More than that to send a continuous stream of bytes on to let the network appear as legitimate traffic
3. Random, randomly alternating between sleep disturbance and energy
4. Responsive sends jam signal when you hear the service

The counter measures to block and spread variations on the communication spectrum, frequency hopping, and as the spreading code. FHSS (FHSS) [5] is used for high-speed signals on the carrier among many frequency channels using a pseudo random sequence known to the transmitter and receiver. Without the ability to the sequence of the frequency selection An Tracking the attacker is not able to block the used frequency in a snapshot. Since the range of possible frequencies is limited, an attacker may jam in place of the wide frequency band. The spreading code has been used a different technique to defend against attacks and disorder is common in mobile networks. This technique requires a greater manufacturing complexity and energy, which restricts its use in the WSN. In general, for the maintenance of low cost and low energy consumption measuring device are limited to the use of a single frequency, and therefore very sensitive to overload attacks.

4.1.2. Manipulation of Data

Sensor networks usually work out. Because unattended and distributed nature of WSN nodes are very vulnerable to physical attacks. [6] Physical attacks cause irreparable damage to the nodes. The opponent can manipulate captured to obtain the encryption keys from the junction of the circuits, modifying the program codes, or even replaced by evil sensor [7]. Temper counter measures involves tampering isolation physical node package that exists.

1. Self-Destruction (tamper-proofing packages)
   Every time someone accesses the physical sensor nodes nodes vaporize the contents of memory, and prevents information leakage.
2. Fault-tolerant protocols - protocols designed for WSN has to withstand such an attack.

4.2. The Data Link Layer

4.2.1. Collision

A collision occurs when two nodes try to transmit on the same frequency, at the same time [8]. When packets collide, they are removed, and the need for retransmission. The opponent can strategically lead to collisions in a specific package, such as ACK control messages. One possible consequence of these collisions is expensive exponential back-off. An opponent could easily crack the communication protocol and constantly sending messages in an attempt to generate collisions.

Counter measures for collisions is to use error correction codes.

4.2.2. Exhaustion

Node harmful disrupts Media Access Control Protocol, which requires continuous or transmission on the channel. This eventually leads to starvation for the other nodes of the network at the entrance to the canal.

Counter measures to fatigue:

MAC received speed limit, allowing the network to ignore the excessive demands, thus avoiding the energy loss caused by the transfer. Using time division multiplexing, wherein each node a time interval in which it can be transferred has been assigned.

4.2.3. Collection of Data

This attacker interaction between two nodes for data transmission. For example, using wireless LAN (IEEE 802.11) Request to Send (RTS) and Clear to Send (CTS). An attacker can send RTS CTS node means messages repeatedly reactions of targeted recruiting deplete an adjacent node.

Countermeasures for the collection of information to check against this type of attack node can restrict the admission of compounds of the same identity, or the use of replay protection and strong authentication connection.

4.3. Network Layer

4.3.1. False Routing Information

The most direct attack against the routing protocol is to focus on the network routing information. An attacker can create, modify, or playing routing information to a fault in the network. These conditions include the creation of routing loops attract or repel the network traffic of the selected nodes, lengthen or shorten the source path creates false error messages, allowing the distribution network and increase latency end-to-end.

Counter measures for false routing is the MAC (Message Authentication Code) to connect after the report, so the recipient can verify that the reports were false or altered. To defend against information counters outplayed or time may be included in the reports.

4.3.2. Selective Redirection

In a multi-hop WSN network to send messages to all nodes must accurately relay messages. An attacker could compromise the safety of the junction at risk, so that selectively sends messages to other waterfalls.

Counter measures for the selective forwarding attacks are:

1. Use multiple paths for data transmission.
2. Detecting malicious node or assume that fails then try an alternative route.
3. Apply implicit recognition that ensures that the packets are sent because they were sent.

4.3.3. Sinkhole

The sinkhole attack, the attacker node compromise seems attractive to its neighbors to forge routing information [9]. The result is that neighboring nodes select a node affected as the next hop node route information via. This type of attack is very simple selective progress, since all traffic from a wide area network will flow through the infected node. Counter measures to the sinkhole attack is the Geo-routing protocols, such as one of the groups, the routing protocol, since they can withstand attacks Sinkhole because their topology is built with the localized data and traffic changes course based on the physical location of the sink node, thereby making it difficult to draw elsewhere to a sump.

4.3.4. Sybil Attack

It is an attack in which a node more than one identity on the network. E 'was originally described as an attack designed to defeat the mechanisms of redundancy targets in data storage systems distributed peer-to-peer networks [10]. Author describes this attack in terms of WSN. In addition up to beating the storage, Sybil attack is also effective against routing algorithms, data aggregation, and voting, counter measures for Sybil attack is the use of identity certificates. During initialization ago

Implementation of nodes some information sensors assigned to them by the server. The server creates a certificate for each node which binds the identity of node unique information. To demonstrate its node identity need to present the certificate.

4.4. Transport Layer

The two attacks are possible on the transport layer:

4.4.1. Flooding of Data

In this protocol, in which state holds on both sides in communication degrade sensitive to memory resources. This is due to the number of false claims of an attacker, so that legitimate users can not access resources.

Counter measures at the transport layer or flooding is a mystery to each new node joins the network, so that the node can connect to the network only if it solves the puzzle. It will also be a limit on the number of connections that can maintain a node at a time, or a mechanism to remove all traces, but it's hard sensor networks through restrictions sudden unavailability of some nodes due to their failure.

4.4.2. De- Synchronization of Data

In this opponent parodies repeated message to the terminal nodes and end nodes require falter retransmission. So, your opponent can force legitimate end nodes continue to try to correct errors that do not really exist losses. Countermeasures against the attack authentication packets before they are delivered to the terminal nodes if they belong to an authorized user or not

4.5. Application Layer of OSI

4.5.1. Path-based DoS

In this adversary injects packets flood played end to end communication between two nodes, each node on the path to the base station forwards the packet, but if they are sent large amounts of fake packets will all be occupied. Thus, this attack will consume bandwidth, and the energy of nodes [11].

4.5.2. Reprogramming Attack

Program your mind to reprogram may be due to the network nodes to the release, change old program upgrade, or for any other purpose network management [12]. If this reprogramming process is safe, the attacker can take control of a large part of the network. Counter measures for attacks on the application layer the best authentication method or anti-reproduction DoS attack at different levels and possible counter measures.

5. Conclusion

Safety plays a central role in the implementation of wireless sensor networks. In this article, we have to attack the network of sensors, wireless, classified each layer of the TCP / IP. The attacks, the plot against the measures, so that the wireless sensor network of highly respected, that is the nature of the attack, because prevention is better than cure. Sensor networks are threatened attacks on the physical level, like all other layers of denial. All levels, except for the natural, very difficult not determine the attack or the intent. Finally DoS attacks effective at every level, so a special emphasis on reaching prevention. Security, and plays an important role in the implementation of wireless sensor networks. In this article, we have to attack the network of sensors, wireless, classified each layer of the TCP / IP. The attacks, the plot against the measures, so that the wireless sensor network of highly respected, that is the nature of the attack, because prevention is better than cure. Sensor networks are threatened attacks on the physical level, like all other layers of denial. All levels, except for the natural, very difficult not determine the attack or the intent. Finally DoS attacks effective at every level, so that would identify a particular attention and prevention.

References

[1] Deng J, Han R and Mishra S. *Defending against Path-based DoS Attacks in Wireless Sensor Networks*. ACM SASN'05, November 7, 2005, Alexandria, Virginia, USA. 2005: 89-96.

[2] Wang Q, Zhu Y and Cheng L. Reprogramming Wireless Sensor Networks: Challenges and Approaches. *IEEE Network*. 2006: 48-55.

[3] Sanaei, Mojtaba Ghanaat Pisheh, et al. Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack. *International Journal of Computer Networks and Communications Security*. 2013; 1.1.

[4] Raymond DR and Midkiff SF. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing.* 2008: 74-81.

[5] X Du, H Chen. Security in Wireless Sensor Networks. *IEEE Wireless Communications*. 2008.

[6] Xu W, Trappe W, Zhang Y and Wood T. *The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks*. ACM MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA. 2005: 46-57.

[7] Wood AD and Stankovic JA. Denial of Service in Sensor Networks. *IEEE Computer*. 2002; 35(10): 54–62.

[8] Zia T, Zomaya A. Security Issues in Wireless Sensor Networks. *Systems and Networks Communications (ICSNC)*. 2006: 40 – 40.

[9] SK Singh, MP Singh and DK Singh. A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks. *International Journal of Computer Trends and Technology*. 2011.

[10] JR Douceur. *The Sybil Attack*. in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02). 2002.

[11] David R Raymond and Scott F Midkiff. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*. 2008; 7(1): 74-81.

[12] ECH Ngai, J Liu and MR Lyu. *On the intruder detection for sinkhole attack in wireless sensor networks*. in Proceedings of the IEEE International Conference on Communications (ICC "06), Istanbul, Turkey. 2006.