In: Advances in Communications and Media Research ISBN 978-1-60876-576-8
Editor: Anthony V. Stavros, pp.

Chapter 3

DENIAL OF SERVICE IN WIRELESS SENSOR NETWORKS: ISSUES AND CHALLENGES

Al-Sakib Khan Pathan[1]
Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongin 446-701, South Korea

ABSTRACT

Wireless Sensor Network (WSN), composed of a huge number of resource-constrained sensors can be used for a large number of security-sensitive applications. Regardless of the type of application, smooth collection and delivery of data from this type of network is one of the critical requirements. If the data supply process is hampered and thus the expected services become unavailable due to the intentional attempts of the adversaries, we consider this as a Denial of Service (DoS) attack. As DoS attack targets to jeopardize the usual services, it can often drastically curtail the utility of wireless sensor network. In this short communication, we explore the meaning of DoS in WSN, its effective mitigation techniques, and recent issues and challenges in this research area.

1 E-Mail: sakib.pathan@gmail.com.

INTRODUCTION

Wireless Sensor Networks (WSNs) can be utilized for a wide range of applications and services that often require high level security. This security encompasses a large number of challenges ranging from the nature of wireless communications, deployment model of the network, unattended environment, large and dense network, disconnected network, presence of physical stimuli, etc. Examples of some of the security-sensitive applications of WSN are; moving object tracking, intruder detection in a particular area, patient monitoring in hospital while the patient data are to be kept secret, military reconnaissance, volcano monitoring, disaster management and warning system, and the like. In addition to ensuring confidentiality and fidelity of acquired data, these applications demand smooth transmission of information throughout the network. This requires unscathed service and continuous availability of network resources for the full duration of the network's operation. However, the sensors that build up a WSN are generally low-cost devices that are equipped with limited memory, processing, radio, and battery reserves. Moreover, considering the conditions of low-cost deployment of WSN and tiny size of sensors, it is difficult to increase the capabilities of sensors even with the state-of-the-art technology. Hence, for any task in WSN, the goal is to ensure the best possible utilization of sensor resources so that the network could be kept functional as long as possible. In contrast to this crucial objective of sensor network management, a Denial of Service (DoS) attack targets to jeopardize the efficient use of network resources and disrupts the essential services in the network. Because of the wide range of methods used for creating a denial of service situation in the network, DoS attack could be considered as one of the major threats against WSN security.

DENIAL OF SERVICE AND DENIAL OF SERVICE ATTACK

Strictly speaking, we consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as a denial of service attack. In practicality, a DoS situation can occur due to any kind of incident that diminishes, eliminates, or hinders the normal activities of the network. Say for example, any kind of hardware failure, software bug, resource exhaustion, environmental condition, or any type of complicated interaction of these factors can create denial of service. It should be noted that the term 'DoS' indicates to a particular situation in the

network and when DoS situation occurs due to an intentional attempt of an adversary, it is called DoS attack.

DoS attacks can mainly be categorized into three types:

1) Consumption of scarce, limited, or non-renewable resources
2) Destruction or alteration of configuration information
3) Physical destruction or alteration of network resources

Among these three types of DoS attacks, the first one is the most significant for wireless sensor networks as the sensors in the network suffer from the lack of enough resources. Other than this type of categorization, layer wise categorization (somewhat reduced version of the layers in Open System Interconnect reference model) of DoS attacks can also be done. An attacker can choose different targets at different layers to stop proper functioning of legitimate nodes so that they cannot get the services they are entitled to.

LAYER WISE DOS ATTACKS IN WSN: ISSUES AND MITIGATION MECHANISMS

Layer wise categorization of DoS attacks was first presented by Wood and Stankovic [1]. Raymond and Midkiff [2] later enhanced the survey with some updated information. In this section, we discuss current DoS attacks based on various protocol layers and their mitigation mechanisms in wireless sensor networks.

Jamming and node tampering are two well-known DoS attacks in the physical layer. Jamming means the deliberate interference with radio reception to deny a target's use of a communication channel. Various types of jamming (Constant, Deceptive, Random, and Reactive) [3] are difficult to handle in case of sensor networks. This is because the sensors have such limited resources that if an attacker with high power and transmission range starts to disrupt the communications of the sensors, they cannot carry on their normal activities. Such an attacker can make a large portion of the network inaccessible and useless. There are some solutions available to defend against jamming attacks in WSN like; use of spread-spectrum, priority messages, lower duty cycle, region mapping, and mode change. However, most of these proposed mechanisms often prove to be expensive and unfeasible for use in wireless sensor networks. Often the sensors have very simple radios that do not have the capabilities to use sophisticated

jamming protection methods. The second type of DoS attack, physical tampering of sensors could be resisted using camouflaging of sensors, efficient design of sensor circuitry, or tamper-proofing mechanisms for sensors. Say for example, if a WSN is deployed over a rocky mountain area, the sensors could be shielded with a rocky outfit so that it becomes harder for a physical intruder to find them out and physically tamper them. Tamper-proofing methods like self-destruction or erasing important information from memory under a physical attack situation might also be a good solution. However, if low-cost requirement of WSN is to be maintained, tamper-proofing methods are inefficient as their inclusion increases the cost of each sensor in the network.

In the link layer, three main DoS attacks are collision, battery exhaustion, and unfairness. Error correcting codes (ECC) can be used for resisting collision. However, use of ECC incurs more processing and communication overheads. The second type of link layer attack, battery exhaustion can be launched with repeated requests for using the wireless channel. A naive link layer implementation could be an easy target for battery exhaustion attack. Feasible defense mechanisms against battery exhaustion caused by repeated transmissions can be the use of time division multiple access (TDMA) or rate limitation. The third type of attack, unfairness is a weaker form of DoS attack. This threat may not entirely prevent legitimate access to the channel, but can degrade service for real time MAC protocols. Use of small frames could be helpful in handling unfairness in WSN though this particular issue may be regarded as a separate research issue related to fairness in sensor networks. Raymond and Midkiff [2] talk about denial-of-sleep attack, however this is basically a form of battery exhaustion attack where the attacker prevents the radio of a sensor node from going into sleep mode and thus tries to drain the energy resources of sensors.

In the routing layer, DoS attacks are; spoofing, replaying, misdirection of traffic, hello flood attack, and homing. Arbitrary handling of network traffic with spoofing, replaying, and misdirection could be resisted by using egress filtering, authorization, and monitoring while hello flood attack could be mitigated using pairwise authentication of nodes or by using geographic routing. The last type of routing layer attack, homing attack has a different flavor. It tries to block the normal functioning of the special-purpose nodes in the network. As there might be several sub-ordinate nodes under one such node (say for example, a cluster head in a clustered network), hindering the services of this key node can hamper the activities of all other dependent nodes and thus a portion of the network might become useless. Different types of cryptographic schemes, algorithms, management message hiding, secure clustering [4], etc. can be used for preventing homing attack.

Flooding and desynchronization are the two common attacks in the transport layer. While packet authentication mechanism could handle desyncrhonization attack, flooding could be mitigated using client puzzles or traceback mechanisms. However, it should be noted that using traceback mechanism in WSN might be difficult because of scarcity of resources, random failure of nodes, and intermittent communications among the participant nodes.

In the application layer, some DoS attacks can be launched. If the communications of nodes in a WSN are triggered by each occurred event, an application layer DoS attack could be launched by using some external physical stimuli. In such a case, the attacker uses the external stimuli to stimulate the nodes with huge number of events to be sent towards the base station. This attack is not effective when sensor readings are sent after making a gist or with regular intervals (for example, a clustered network where the clusterheads collect the raw data first and then send reports to the base station after certain intervals). On the other hand, some type of intrusion detection mechanism (IDM) can be used to detect the presence of any external entity in the network if a particular region creates a large volume of readings within a short period. An effective IDM can prevent the instant triggering of sensors by notifying the presence of intruder in the network and isolating it or ignoring it. However, such type of IDM is difficult to develop as sensor nodes cannot determine the legitimacy of a particular physical stimulus rather they only sense the event and get triggered. Path based DoS (PDoS) attack [5] is another kind of application layer DoS attack. Each of the nodes in a path towards the base station needs to participate in the forwarding process of a particular packet containing sensor readings. If a large number of bogus packets are sent through a path towards the base station, it can keep the nodes busy, deny transmission of legitimate traffic by occupying network resources, and significantly drain the resources of the sensors. Use of various authentication mechanisms or replay protection mechanism could be the effective countermeasures against this type of attack. A third type of application layer attack could be launched if a WSN allows reprogramming of the network. Reprogramming of a sensor network may be needed for version control, scope selection, encoding-decoding, code dissemination, completion validation, code acquisition, switching to a new program, and/or for network management purpose [6]. In these cases, if the process of reprogramming is not secure enough, the attackers can actively cut off a portion of the network by using bogus messages. Good authentication mechanism for the whole process can resist this type of attack.

CONCLUSION

Other than the mentioned attacks, many other attacks like wormhole attack or sybil attack can also cause denial of service situation in the network. In fact, many attack mechanisms and targets of attacks overlap with each other; but considering different circumstances, they are given different tags and names. Among all types of DoS attacks in WSN, physical layer attacks are the most difficult to handle. This is because the sensors are not built with powerful radios or the nature of wireless sensor network needs unattended environment. More efforts may be given to develop efficient jamming protection methods or we may need to wait for the technological advancements so that the sensors get enough low-cost resources to fight against any type of physical attack. For all the layers, though it is often quite difficult to know whether any particular DoS situation in WSN is caused intentionally or unintentionally, there are some common detection and defense mechanisms. In this short communication, we have discussed these current issues and challenges. As DoS attack covers a large number of attacks and threats in WSN, finding efficient mechanisms for effective prevention of DoS situations still remains as an open research issue. As "*Prevention is better than cure*", future research efforts should mainly be directed towards developing DoS prevention mechanisms instead of searching for "*cures*".

REFERENCES

[1] Wood, A. D. and Stankovic, J.A. (2002). Denial of Service in Sensor Networks. IEEE Computer, vol. 35, no. 10, 2002, pp 54–62.

[2] Raymond, D. R. and Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing, January-March 2008, pp 74-81.

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

[4] Pathan, A.-S. K. and Hong, C. S. (2006). A Key-Predistribution-Based Weakly Connected Dominating Set for Secure Clustering in DSN. LNCS 4208, Springer-Verlag 2006, pp 270-279.

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

[6] Wang, Q., Zhu, Y., and Cheng, L. (2006). Reprogramming Wireless Sensor Networks: Challenges and Approaches. IEEE Network, May/June 2006, pp 48-55.