A SURVEY ON DENIAL-OF-SERVICE ATTACKS DETECTION AND PREVENTION MECHANISMS IN WIRELESS SENSOR NETWORKS

Chunnu Lal
Assistant Professor
Quantum Global Campus, Roorkee, Uttarakhand, India

Abstract

Wireless sensor networks (WSNs) are currently used in many application areas such as military applications, control and tracking applications, habitat monitoring applications where they face attacks already experienced by the Internet and wireless ad hoc networks. One such attack is that of Denial-of-Service (DoS), which we believe will only become more prevalent as sensor networks become more pervasive and accessible. With the inherent resource limitations of WSN devices, they are particularly susceptible to the consumption and destruction of these scarce resources. Denial-of-Service (DoS) attacks have become a major threat to WSNs. It is critical challenge to develop the effective and lightweight security mechanism to detect and prevent various attacks for WSN, especially for the Denial-of-Service (DoS) attack. This paper discusses current state of art in various security mechanisms which detect and prevent the Denial-of-Service (DoS) attack in WSNs.

Keywords-Wireless Sensor Network (WSNs), Denial-of-Service (DoS) Attack, Sensor Node, Base Station (BS)

I.INTRODUCTION

Wireless Sensor Network (WSN) is a network which have a large number of small sensor devices that sensing data to their environment and communicate with each other wirelessly. The purpose of this network is to accomplish a certain task such as environment monitoring. Each node is sending their sensing data to a center node (or sink node).The collected data is used in different domains as surveillance and monitoring habitat.

Denial-of-Service (DoS) attacks where unnecessary packets are sent causing services to appear unavailable and thus these services are denied to the legitimate sensor nodes.

Detecting Denial-of-Service (DoS) attacks and reducing the energy consumption are two important and frequent requirements in WSNs. Detecting phenomena such as forest fires or seismic activities implies to keep watch over wide areas. Wireless sensor networks (WSNs) are often used to achieve this watch. In WSNs, we have a large number of sensor nodes which sensing their environment and sending the collected data to the base station (BS).

Because of their limited size, the sensors have very limited resources: memory, computing capability and energy must be spent with care [7, 13, 15].

Other uses of WSNs include activities such as preventing chemical, biological, or nuclear threats in an area, or collecting data on a military field [8, 9].

In such sensitive domains, the deployment of a WSN brings out strong requirements in terms of security.

Various works deal with ways of preventing unauthorized access to data or with the necessary precautions to guarantee data authenticity and integrity inside the network [10, 17, 18, 12].

DoS attacks are prevent the source node to deliver its data to the destination. So confidentiality and authentication are of poor use if DoS attacks exist in the network.

II. DENIAL OF SERVICE IN WSNs

A DoS attack is an attempt by an adversary to degrade the network's services. In DoS attacks, malicious nodes can degrade the services provided by legitimate nodes, by flooding the legitimate nodes with requests (RTS).

One of the characteristics of WSNs is that they are based on carrier sense multiple access with collision avoidance (CSMA/CA) mechanism.

This CSMA/CA mechanism relies on the exchange of ready-to-send (RTS) and clear-to-send (CTS) control packets. When a source node has data to send, it initiates the process by sending an RTS packet. When an RTS packet is heard by any node, the node will respond by sending a CTS packet.

Therefore when an RTS is travelling the WSN it silences all passing nodes until it reaches its target node, and thus only one CTS packet is returned. Like the RTS packet, the CTS packet silences the nodes in its immediate vicinity. Once the RTS/CTS exchange is complete, the source node transmits data without worry of interference from any other nodes. The data packets are positively acknowledged.

Denial-of-service (DoS) attacks indeed aim at reducing or even annihilating the network ability to achieve its ordinary tasks, or try to prevent a legitimate agent from using a service [11, 14].

Due to limited resources of sensor nodes in WSNs. WSNs tend to be rather vulnerable to DoS attacks.

A compromised sensor node is used to send the corrupted data at a high rate to other nodes in the network. Due to this corrupted data sensor nodes lost their energy faster.

III. OVERVIEW OF VARIOUS DETECTION AND PREVENTION MECHANISMS IN WSN

To deal with DoS attacks in WSNs, various research studies have been conducted. In [1], the authors proposed a DoS detection method based on deployment of special control nodes in the sensing field: this is, specific nodes that are responsible for monitoring the throughput of traffic of specific part of the sensing field and signaling the presence of suspected attacked nodes in case anomalies are detected. Control nodes election is a crucial aspect of DoS mechanisms. In this paper the authors presented a dynamic method of election of control nodes. cNodes (control nodes) are periodically elected among normal sensors. Detection takes place whenever a cNode observes that at least one among the sensor nodes under its controlled perimeter sends data at a rate that is note with in "regular behavior" thresholds. In that case, the cNode sends a warning message to the Cluster Head (CH).Once the CH has received warnings from a sufficiently large number of distinct cNodes, it starts ignoring the packets coming from the detected compromised sensor. cNodes may also monitor output traffic of the CHs and warn the Base Station (BS) if they come to detect a compromised CH. The guarding functionality of cNodes may lead to energy consumption higher than that of "normal" (i.e. sensing) nodes. In order to maximize the repartition of the energy load, the author propose a scheme by which a new set of cNodes is periodically established with an election period shorter than the length of a LEACH round(i.e. the period between two consecutive CH elections).

In [2], the authors proposed a novel intrusion detection scheme for cluster-based WSNs. The proposed scheme adopts the energy prediction method to detect malicious nodes. In this paper the author believe that malicious nodes have to use additional energy to launch DoS attacks. In this paper, Markov chains model is adopted to periodically predict energy consumption of sensor nodes. The difference between the predicted and the real energy consumption of sensor nodes can be used to detect malicious nodes. The energy dissipation in sensor nodes depends on the energy consumption in different working states and the time they operate in each state. The sensor nodes have five operation states: sleeping state, sensing state, calculating state, transmitting state and receiving state. The author believed that the energy dissipation mainly focuses on the last four states. The nodes with abnormal energy consumption are regarded to be malicious.

In [3], the author design a novel MoM in the hierarchical WSN based on spatiotemporal correlation, to detect and defense the DoS attack. In MoM, the author store several representative normal messages and abnormal messages as referential data sets. The MoM is usually deployed in the cluster head (CH). MoM includes the two types of lists normal message list (NML) and abnormal message list (AML)

which distinguish forge messages and redundant messages (replayed attack) based on the lists and frequency, also present a MoM to judge the new event to avoid the adversary's tampering with packets. Based on the spatiotemporal correlation, MoM utilizes the similarity function to identify the content attack as well as the frequency attack. And then the Mom adopts rekey and reroute countermeasures to isolate the malicious node.

In [4], In this paper, the authors proposed a new method to defend against DoS attacks in WSN using the ideas of Shield and sShield that are DoS attack defense techniques using traffic deflection for the existing wired networks. Out of the wireless sensor network routing algorithms, this paper focused on the location-based routing protocol for the sensor network environment since it is simple and easy to implement and install. The proposed method was systematized with three phases of DoS attacks fit for each risk circumstance, and the administrator was made to select nodes to make traffic deflection when judging a DoS attack. Then, by changing the location parameter of location-based routing protocol only for nodes selected, it is possible to for the selected nodes to make traffic come to themselves, by which a DoS attack could be blocked out. Besides, the number of nodes to deflect path was confirmed by experiments. By using the results, it will be possible to make judgments about the appropriate number of nodes depending on various sensor network conditions. This paper proposed a method to defense DoS attack effectively in WSN (wireless sensor network) environment by using traffic diversion method.

In [5], the author present a novel countermeasure for TDMA protocols to defend against energy efficient link layer jamming attacks, this countermeasure targets the power consumed by the jammer, the main idea of the countermeasure is to separate the data packet into two parts. This separation results in misleading the jammer to estimate the slot size smaller than it actually is and to jam at higher rate hence, lose power faster. The defence is also equipped with a means to reduce slot size randomization effect on the throughput of the network by having all slots equal in duration by applying Round Robin slot assignment techniques. Typically, slot size randomization results in a reduced network throughput due to randomized slot sizes among nodes resulting. Applying Round Robin quarantines fairness among nodes by ensuring that all nodes get the same amount of time to transmit.

In [6], in this paper authors proposed a new security scheme to provide confidentiality and DoS-resistance in a multi-hop WSN code dissemination protocol. The authors proposed the use of session keys derived from hashing data packets to encrypt these same data packets. The re-keying process between one sender and multiple receivers can be done in this way on the reception of the data packets without requiring any additional energy expensive mechanisms. the author also described a Cipher Puzzle as a weak authenticator to integrate confidentiality for the first session key with a countermeasure against signature based and request-based DoS attack, which we believe is the first security scheme to do so in a multi-hop code dissemination protocol.

IV.CONCLUSION

As per study of many papers, many techniques are used by various researchers for detection of denial-of-service (DoS) attacks in WSNs. But in this paper we only considers, the detection techniques which are efficient in detection of DoS attack and also reduce the power consumption in the Wireless Sensor networks. Our Study is only focuses on some latest detection mechanisms which are design taking scarce resources of Wireless Sensor Network as consideration. A large number of detection mechanisms are exists. But in WSNs, we have limited power and processing capability of sensor nodes thus to reduce the power consumption in WSNs. We need to design an energy preserving DoS detection mechanism in WSNs.

REFERENCES

[1] Paolo Ballarini, Lynda Mokdad and Quentin Monnet 2013.Modeling tools for detecting DoS attacks in WSNs. Security Comm. Networks 2013; 6:420–436.

[2] Wen Shen, Guangjie Han, Lei Shu, Joel Rodrigues, Naveen Chilamkurti. A new energy prediction approach for intrusion detection in cluster-based wireless sensor network.

[3] Zhang yi-ying, Li xiang-zhen, LIU yuan-an 2012. The detection and defence of DoS attack for wireless sensor network. ScienceDirect 19(Suppl. 2): 52-59.

[4] Ho-Seok Kang, Sung-Ryul Kim1, Pankoo Kim 2013.Traffic Deflection Method for DOS Attack Defense using a Location-Based Routing Protocol in the Sensor Network. ComSIS, Vol. 10, No. 2, Special Issue.

[5] Ahemed R. Mahmood, Hussein H. Aly, Mohamed N. El-Derini 2011. Defending against energy efficient link layer jamming denial of service attack in wireless sensor networks. AICCSA, 978-1-4577-0476-5.

[6] Hailun Tan, Diethelm Ostry ,John Zic Sanjay Jha 2013. A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks. ScienceDirect 36-55.

[7] Anastasi G, Conti M, Di Francesco M, Passarella A 2009. Energy conservation in wireless sensor networks: a survey. Ad Hoc Networks; 7:537–668.

[8] Li B, Batten L 2009. Using mobile agents to recover from node and database compromise in path-based DoS attacks in wireless sensor networks. Journal of Network and Computer Applications; 32:377–387.

[9] Claycomb WR, Shin D. A novel node level security policy framework for wireless sensor networks. Journal of Network and Computer Applications 2011; 34:418–428.

[10] Simplicio MA Jr., De Oliveira BT, Barreto PSLM, Margi CB, Carvalho TCMB, Naslund M. Comparison of authenticated-encryption schemes in wireless sensor networks, 36th Annual IEEE Conference on Local Computer Networks, Bonn, Germany, 2011.

[11] Hu F, Sharma N 2005. Security considerations in ad hoc sensor networks. Ad Hoc Networks; 3:69–89.

[11] Yahya B, Ben-Othman J 2010. Energy efficient and QoS aware medium access control for wireless sensor networks. Concurrency and Computation: Practice and Experience; 22(10):1252–1266.

[12] Ben-Othman J, Yahya B 2010. Energy efficient and QoS based routing protocol for wireless sensor networks. Journal of Parallel and Distributed Computing; 70(8):849–857.

[13] Fouchal H, Habbas Z 2011. Distributed backtracking algorithm based on tree decomposition over wireless sensor networks. Concurrency and Computation: Practice and Experience. DOI: 10.1002/cpe.1804.

[14] Dessart N, Fouchal H, Hunel P, Vidot N 2010. Anomaly detection with wireless sensor networks. The 9th IEEE International Symposium on Network Computing and Applications (NCA 2010), IEEE CS Press, Cambridge, MA, USA, July 2010.

[15] Bernard T, Fouchal H 2010. A low energy consumption MAC protocol for WSN. IEEE ICC, Ottawa, Canada, June 2012.

[16] Yahya B, Ben-Othman J 2010. Energy efficient and QoS aware medium access control for wireless sensor networks. Concurrency and Computation: Practice and Experience. 22(10):1252–1266.

[17] Ben-Othman J, Bessaoud K, Bui A, Pilard L. Selfstabilizing algorithm for efficient topology control in Wireless Sensor Networks. Elsevier, Journal of Computational Science (JOCS) In press.

[18] Ben-Othman J, Saavedra Benitez Y. IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s. In Concurrency and Computation: Practice and Experience. Wiley, In press.