Denial of Services Attack on Wireless Sensor Network using Different Technique: A Survey

Shubham Kumar[1], Yogesh Kumar[2]
[1]M. Tech Scholar, [2]Assistant professor
Department Of Computer Science Engineering, School Of Engineering & Technology
A Unit of Ganga Technical Campus, Soldha, Bahadurgarh M. D. University, Rohtak, Haryana (India)

Abstract **-** This makes WSN vulnerable to multiple attacks. One of them is a denial of service (DoS) attack. Each layer has different types of DoS attacks. Dealing with this type of attack requires an understanding of the types of DoS and the various defence mechanisms used to overcome them. This article introduces the introduction of DoS attacks and their countermeasures. Some of the defence mechanisms provided have some limitations, which can be defeated by the attacker counterattack, but further investigations to extend their efficiency to make it specific. Wireless sensor networks are computer networks commonly used for environmental monitoring and military observations. Wireless sensor networks are subject to both sabotage and broadcast attacks. Protecting the WSN is a difficult task. A notable attack in wireless sensor networks is a denial of service (DoS) attack. DoS attacks are triggered by interference with a single node or group of nodes are achieved by interrupting communication. This article discusses various types of DoS attacks. It also details the methods used by multiple researchers to detect DoS attacks.

Keywords **-** WSN, DDoS, DoS, Jamming , Attack

I. INTRODUCTION

Wireless Sensor Network (WSNs) is an innovative large network of distributed, autonomous, low-power, low-cost, small devices that use sensors to gather information over a low infrastructure ad hoc wireless sensor network. The development of wireless sensor networks was initially driven by military applications such as battlefield surveillance. However, wireless sensor networks are currently used in many residential applications such as environmental and habitat monitoring, healthcare applications, home automation, traffic control and more. Security plays an important role in many wireless sensor network applications. Due to the unique challenges presented by sensor networks, the security techniques used in traditional networks cannot be applied directly to wireless sensor networks because of their unique characteristics [2].

The wireless sensor network includes sensor nodes for detecting real time events. They can sense temperature, sound, vibration, and pressure. Sensor nodes consist of sensing, drive and power components integrated on one or more boards to form an embedded system. Sensors are small, low cost devices that have limited energy and transmission capabilities. Sensor node weaknesses lead to various attacks on the WSN. One such attack is the Denial or Service (DoS) attack. There are various types of DoS attacks, from the physical layer to the application layer.

II. CLASSIFICATION OF DDOS ATTACKS

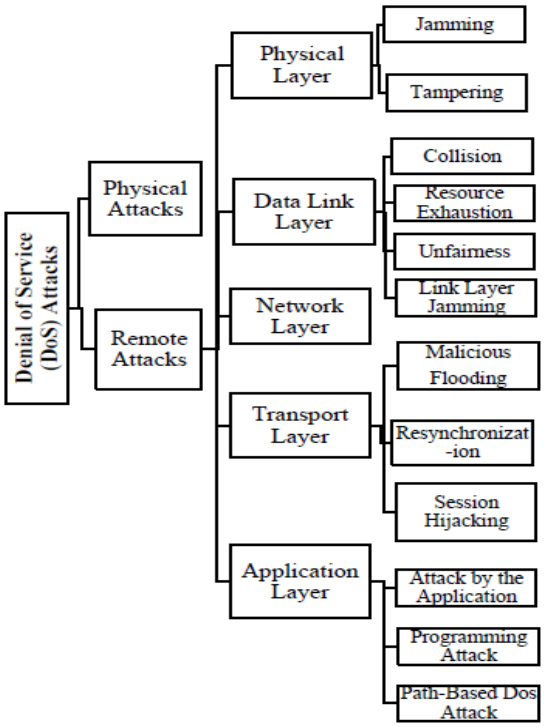

Figure 1: Classification of DoS Attacks

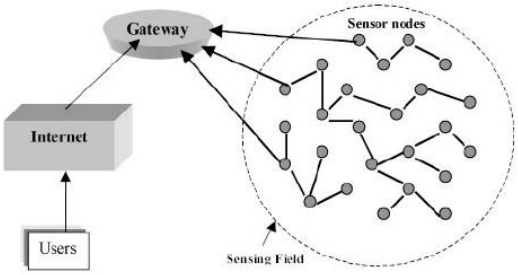

Figure 2: Simple network of WSN.

III. BACKGROUND

Some researchers use different techniques to detect DoS attacks and identify malicious nodes that cause denial of service attacks in wireless sensor networks. These techniques are categorized and described in Figure 3 below.

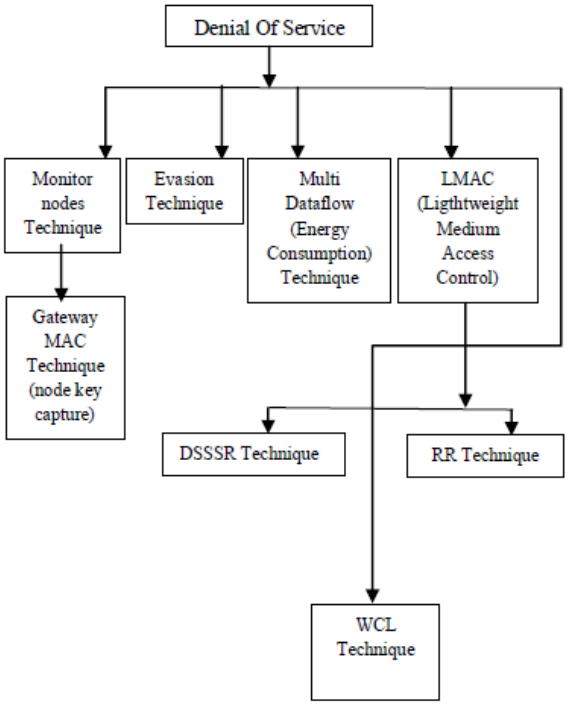

Figure 3: Classification of Denial of Service attacks

The wireless sensor network consists of small and lightweight wireless nodes with limited storage space and limited communication bandwidth. This includes small battery-powered wireless devices with sensing capabilities and limited processing power. Provides on-board processing. It is a network of autonomous devices designed to jointly monitor physical and environmental conditions. Large WSNs consist of thousands of nodes that require a shared key for secure wireless communication. Key distribution should also be used securely. In addition to the sensors, each node has a wireless transceiver, a small microcontroller and an energy source. In sensor networks, centralized control uses base stations (also known as receivers). Data streams from all nodes end at BS. Through the base station, the sensor network can be linked to other networks to propagate sensing data. As such, they can also be considered as gateways to other networks. BS is more powerful than sensor nodes.

This review provides the main points of security issues associated with WSNs networks and describes the different types of attacks in the network. When deployed to form a wireless sensor network operating under control of a central authority (i.e., base station), it is interesting to note that sensor nodes may be deployed ubiquitously in a harsh and ubiquitous environment we can show the use but for the same reason, security is a major concern for these networks. The purpose of this white paper is to analyze threats to wireless sensor networks and identify different research activities to investigate different routing attacks on the network layer. Particularly destructive attacks are worm attacks and denial of service attacks, where an attacker creates a low latency link between two network points. By studying existing wormhole detection methods, researchers have identified and described important search challenges for detecting wormhole attacks at the network layer [1].

In [3], we consider optimal attack scheduling for remote condition estimation on wireless channels. We demonstrate that successive attacks maximize the expected mean error covariance. It also shows that if attacks are evenly separated, they have the least impact on the quality of estimates. When a special intrusion detection mechanism in the estimator is available, we further propose the best attack plan. We finally saw the best offensive schedule when both the sensor and the attacker have energy restrictions. A closed-form solution for finding the best attack schedule in a high-loss network environment is interesting but challenging. This is reserved for future work. We will also develop an infinite time attack model and consider the best future attack schedule. It is also interesting to consider the best defense strategy, assuming that the sensor knows the presence of the attacker. We use several physical experiments to further validate the results, to consider the best attack scheduling for feedback control, and to evaluate the corresponding effectiveness.

Recently, a lot of literature has taken into account the security issues of Wireless Network Control Systems (WNCS). However, because of the lack of energy on the attacker side, there is little work for the attacker to optimize the attack plan to maximize the impact on system performance. This paper fills this gap in terms of control system performance. We consider the optimal interference attack maximizing the linear quadratic Gaussian (LQG) control cost function under energy constraints. After analyzing the nature of the cost function under any attack plan, we derive the optimal interference attack plan and its corresponding cost function. System stability under this optimal attack plan is also considered. In addition, WNCS examined optimal attack plans using multiple subsystems. Different examples are provided to demonstrate the effectiveness of the proposed best denial of service attack plan [4].

In this paper [4], we consider an optimal DoS attack strategy considering energy constraints to maximize LQG cost function. We first developed an optimization problem from the perspective of a DoS attacker. Attackers may block transport channels with limited activity during any activity. Next, we analyze the characteristics of the LQG cost function under the given viable attack plan. Determine the optimal attack schedule and the corresponding expected cost. This indicates that it is best to group limited attacks by active session. We further studied the stability of the system under an optimal attack schedule.

This paper [5] proposes a new method to detect denial of service attacks. In particular, attention has been paid to sleepless attacks, such as malicious nodes that use flooding techniques. Our approach is based on Wireless Sensor Network (WSN) clustering. This includes recursive clustering sensors until reaching the desired granularity (selected by the expert). We use two different clustering

algorithms to apply our method. In fact, we use the general clustering WSN algorithm low energy algorithm adaptive clustering hierarchy and the general clustering method fast and flexible unsupervised clustering algorithm (FFUCA) based on hyper parameter characteristics. We will use two algorithms to illustrate the behavior of this method.

In [5], we propose a new method to detect denial attacks in wireless sensor networks. This method is based on recursive clustering. Clustering allows detection of homogeneous groups and monomers (possibly generating an attack). Grouped homogeneous groups indicate optimal management based on energy consumption. Approved two clustering algorithms on 100 sensor networks. In fact, we use LEACH and FFUCA algorithms. The results were compelling in the test group. In addition, FFUCA allows you to better manage energy, thus extending the life of your network. In this paper, we propose a classification method to study DoS attacks that affect the availability of wireless sensor network resources and their countermeasures.

This paper [7] presents a multi-step analysis of DDoS attack problems. Eight solutions were defined using two security levels (encryption/no encryption) and various numbers of damaged devices (50, 75, 100 and 150). A series of simulations were performed to investigate receiver performance and power consumption under DDoS attacks. A new distributed denial of service attack, DDoS attack, was identified by examining the results of the created simulated collection. Analysis shows that the packets traversing the network are not encrypted (the performance of the aggressor node should be less harmful from a performance point of view), but still dangerous and silently reducing the entire network without knowing it I can. Create valuable energy resources. Depending on the type of DDoS attack, you can adjust the security level to prevent different types of attacks. Our simulations show that, in some cases, DDoS can be avoided or delayed by lowering the security level.

This paper [8] formally defines WSN and DoS attacks. The purpose of these specifications is (i) to define the attacks individually as there is not enough detail in the general attacker model, and (ii) to present various DoS attack specifications in an accurate and formal way. The specification is expressed from the grassroots level, so Z is used as a formal mathematical symbol for a detailed explanation. By using widely recognized programming/modeling techniques (such as Z), researchers who agree on the same and readable and acceptable specifications so that DoS attacks are detected on the same basis. You get the benefits. Solution it also enables research to annotate DoS specifications in a structured way to achieve future modifications.

In this paper [9], we propose a method to detect and prevent denial of service attacks in wireless sensor networks. The detection method we considered is based on the use of a special control node that monitors the traffic throughput in a cluster. Control nodes (cluster heads) are selected using a recursive LEACH clustering algorithm. We introduced it through a series of experiments using the Siemens simulator. The numerical results obtained show that our method gives significant results in detection rate and time detection. Future work will improve the approach by introducing additional parameters to detect DoS attacks and will consider other security protection systems to protect wireless sensor networks.

In this article [10], we aim to minimize the stealth denial of service (S-DoS) attack. Visibility may the same time be as harmful as other attacks on the resource usage of wireless sensor networks. The impact of Stealth Denial of Service (S-DoS) attacks includes not only denial of service but also resource maintenance costs related to resource usage. Specifically, the longer the detection delay, the higher the cost incurred. Therefore, we need to pay special attention to secret DoS attacks in WSN. In this paper, we propose a new attack strategy to slowly increase or decrease the exploit of application vulnerability under Constrained DoS Attack Strategy (SIDCAS) in order to reduce the base station performance in WSN. Finally, we analyze the characteristics of S-DoS attacks against existing Intrusion Detection Systems (IDS) running at the base station.

In this paper, we propose a new strategy to implement stealth attack mode in WSN, which reveals hidden behavior that may not be recognized by the proposed technology for DoS attacks in existing intrusion detection systems. To exploit target base station or access point vulnerabilities in the WSN, intelligent attackers can organize custom or dynamic access streams that are indistinguishable from legitimate access requests. In particular, the proposed attack mode is not designed to make access unavailable, but to exploit resources so that the system consumes more resources than necessary. In our future work, our goal is to develop a method to detect stealth attacks in wireless sensor network environments [10].

The recent surge in the development of underwater acoustic networks (UAN) has led to the rapid acceptance of this technology in scientific, commercial and military applications. However, only limited work has been done in developing secure communication mechanisms and technologies to protect these networks. Security mechanisms are widely studied in terrestrial networks, and various defense mechanisms are being developed as protective measures. Due to differences in communication media and physical environment, existing terrestrial network solutions cannot be applied directly to UAN. This white paper uses real-world field tests to investigate the impact of a DoS interference attack on UAN. We develop proprietary jamming hardware and signals to analyze the characteristics of different jamming attack models on the network. Our tests were conducted on several commercial brand acoustic modems and prototypes of orthogonal frequency division multiplexing modems. We demonstrate that UAN can be easily blocked using energy efficient timing attacks [11].

This paper proposes an immune system against DoS attacks on WSN, which will improve the accuracy of attack

defense, reduce false positive rates and identify different Dos attacks [12].

IV. DDOS ATTACK ON DIFFERENT LAYERS

Table 1: Denial of Service attacks and defences to combat at different protocol layers

Protocol layer	**Attacks**	**Defenses**
Physical	Jamming	Sleep
	Node destruction	Hide nodes or tamper proof packaging
MAC	Denial of sleep	Sleep, authentication and anti-replay
Network	Spoofing, replaying	Authentication, anti-replay
	Hello floods	Header encryption
	Homing	Header encryption
Transport	SYN flood	SYN cookies
	De synchronization attack	Packet authentication
Application	Path based DoS	Authentication and antireplay protection.
	Reprogramming attacks	

V. CONCLUSION

In this paper, DoS attacks in wireless sensor networks are studied in detail and comprehensively, and they are classified according to their basic techniques. Protected transactions are cumbersome in wireless sensor networks. This paper examines many effective denial of service attack detection techniques in wireless sensor networks proposed by various researchers in space. There are many other technologies that can be used to detect DoS attacks. By using the above techniques we can communicate securely in a wireless sensor network.

VI. REFERENCES

[1]. Pawar, M., & Agarwal, J. (2017). A literature survey on security issues of WSN and different types of attacks in network. Indian J. Comput. Sci. Eng, 8, 80-83.

[2]. Parno, B., Perrig, A., & Gligor, V. (2005, May). Distributed detection of node replication attacks in sensor networks. In IEEE symposium on security and privacy.

[3]. Zhang, H., Cheng, P., Shi, L., & Chen, J. (2015). Optimal denial-of-service attack scheduling with energy constraint. IEEE Transactions on Automatic Control, 60(11), 3023-3028.

[4]. Zhang, H., Cheng, P., Shi, L., & Chen, J. (2016). Optimal DoS attack scheduling in wireless networked control system. IEEE Transactions on Control Systems Technology, 24(3), 843-852.

[5]. Fouchal, S., Mansouri, D., Mokdad, L., & Iouallalen, M. (2015). Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks. International journal of communication systems, 28(2), 309-324.

[6]. Osanaiye, O. A., Alfa, A. S., & Hancke, G. P. (2018). Denial of service defence for resource availability in wireless sensor networks. IEEE Access, 6, 6975-7004.

[7]. Mazur, K., Ksiezopolski, B., & Nielek, R. (2016). Multilevel modeling of distributed denial of service attacks in wireless sensor networks. Journal of Sensors, 2016.

[8]. Saghar, K., Farid, H., Kendall, D., & Bouridane, A. (2016, January). Formal specifications of denial of service attacks in wireless sensor networks. In 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)(pp. 324-333). IEEE.

[9]. Mansouri, D., Mokddad, L., Ben-Othman, J., & Ioualalen, M. (2015, June). Preventing denial of service attacks in wireless sensor networks. In 2015 IEEE International Conference on Communications (ICC) (pp. 3014-3019). IEEE.