ISSN: 1832-5505

Applied GIS

Vol-8 Issue-03 July 2020

An Analysis of Denial-of-Service Attacks Wireless sensor networks are under attack.

Amirthasaravanan.A, Rajasekar S , Rajasekar S

Assistant Professor[1,2,3]

CK College of Engineering & Technology, Tamilnadu, India

ABSTRACT

A Wireless Sensor Network is a network of several low-cost sensors made possible by the simple improvement of hardware engineering processes and efficient software operations. Wireless sensor networks (WSNs) provide a potential network architecture for a variety of uses, including the supervision of household appliances, ecological monitoring, and medical care. Moreover Since WSNs are both practical and simple to set up, they are often used in homeland security and monitoring scenarios in war zones. However, securing WSN against devastating assaults is now a major challenge. Organization of sensor nodes in a desolate area renders network systems vulnerable to a wide range of powerful attacks, while the memory and power constraints of sensor nodes make the conventional security configurations impractical. This article presents a comprehensive review of the security dangers posed by Denial of Service (DoS) attacks on WSN and the fundamental characteristics of sensor network devices that render them vulnerable to such assaults.

Keywords*:* Warzone, Denial-of-Service Attack, Wireless Sensor Network.

1. INTRODUCTION

Commonly, people think of a WSN as a collection of sensors and actuators that work together to facilitate communication between electronic devices and their immediate physical environment. Wireless sensor networks (WSNs) may be used for many different kinds of services and applications, many of which have stringent safety requirements. This security includes massive number of issues vary from the surroundings of wireless communications, deployment type of the network, unattended milieu, big and thick network, incoherent network, occurrence of physical stimuli, etc. Moving-object tracking, intruder detection in a sensitive location, hospital patient monitoring where patient data must remain confidential, military scouting, disaster management and warning system, volcano monitoring, etc. are all examples of security-sensitive WSN applications. Soft communication over the network is required for these applications, along with assurances of privacy and data integrity. This means that the network will continue to function normally and all of its resources will be accessible at all times.However, the sensors that make up a WSN are often inexpensive gadgets with spartan memory, radio, processor, and battery capacities. With current technology, it is also challenging to magnify the capabilities of sensors under the current conditions of low-cost deployment of WSN and tiny size of sensors.Therefore, in WSN, it is important to ensure the most promising use of sensor resources for each given activity if the network is to remain operational for as long as feasible. In contrast to this critical goal of sensor network management, a Denial of Service (DoS) attack aims to interrupt the network's essential functions and put at risk the efficient use of its resources. DoS attacks might be seen as one of the most significant risks to WSN security due to the variety of techniques that can be utilized to produce a denial of service situation in the network.

2. CHARACTERISTICS OF WIRELESS SENSOR NETWORK

Compared to other networks, sensor networks are rather unique. Wireless sensor networks are distinguished from conventional communication systems by their unique properties. In terms of interfaces and components, wireless sensor nodes have a lot in common with extremely basic computers. Typical components include a small amount of storage and processing power, a few or no sensors, a radio transceiver for limited communication, and a battery or other limited power source. These features include the capacity for energy storage, resilience to failure, mobility, failure, heterogeneity, scalability, and sensitivity environmental management. Because of these inherent weaknesses, DDoS assaults may easily overwhelm a WSN.

One major drawback shared by all wireless technologies is the difficulty in securing the wireless medium. Jamming the network and listening in on communications is possible for any enemy within radio range. If sensors are installed in insecure locations, they might be physically tampered with or destroyed. Given the unprotected nature of WSNs and the volatile nature of DoS assaults, it may be difficult to distinguish between the two.

ISSN: 1832-5505

Applied GIS

Vol-8 Issue-03 July 2020

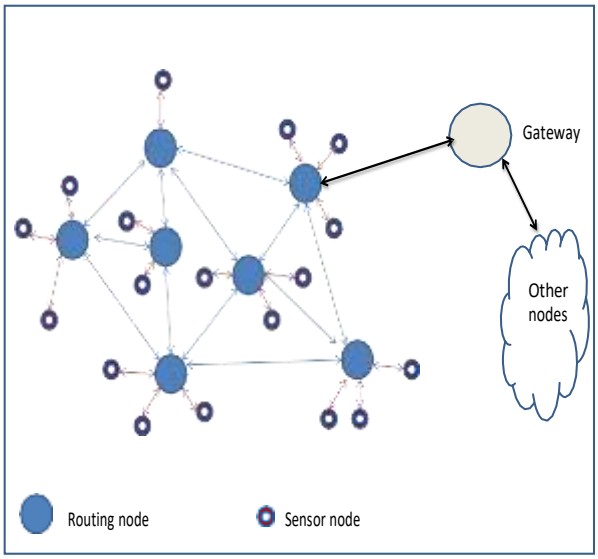

Figure 1. Simple Network of WSN Structure

3. ATTACKS

In this section of the paper, different types of attacks have been conferred. First, attacks have been sorted as an invasive i.e. (unrelenting) or non-invasive i.e. (non-persistent). The Invasive attacks are habitually considered more frequently in the literature [2] and they are better recognized attacks than the non-invasive ones. Few of the well-known Invasive attacks have been conversed in the section below, collectively with non-invasive attacks with the side channel attacks based on timing, frequency and power.

4. ATTACKS ON SENSOR NETWORK ROUTING

The majority of the WSN's routing protocols are simple and straightforward. Because of these grounds they are weak to attacks. There are different types of network layer attacks in WSNs which can be classified as following:

a) False routing Information, replayed routing information, Spoofed, or Altered

b) Sybil attacks,
c) Wormholes,
d) Selective forwarding,
e) Sinkhole attacks

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

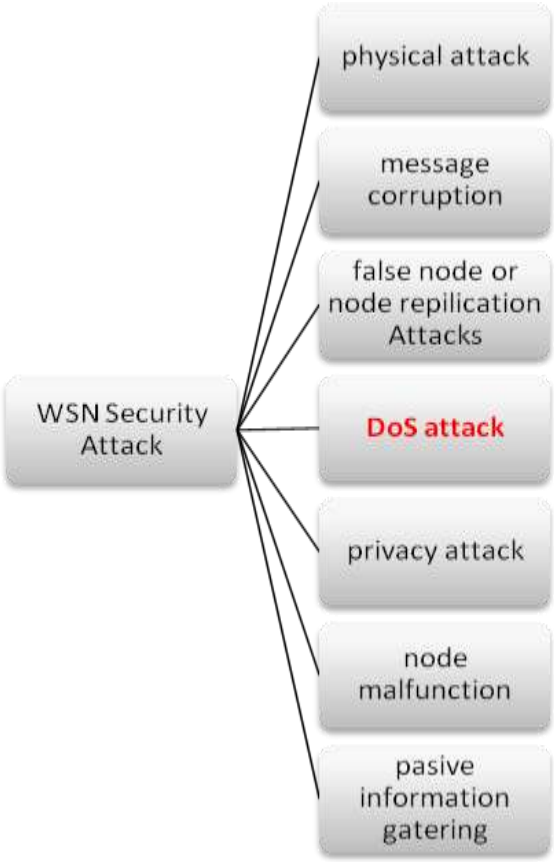

Figure 2. Types of Attack on WSN

5. STATISTICAL DETAIL

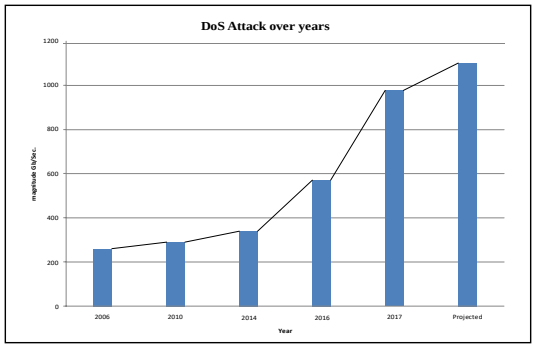

Figure.3.Statistical Analysis of DoS Attack

The statistical detail given above on DoS attack for time period stipulate that, DoS not only an emerging security issue, but when WSN is inherited to IoT technologies in near future then its effect will be severe on sensor expertise.

6. DENIAL OF SERVICE ATTACKS

A Denial of service attack is a clear effort to prevent the lawful user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legal traffic. As a outcome, it makes the service or system unavailable for the user. The fundamental types of attack are: consumption of processor time or consumption of bandwidth, obstructing the communication between two

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters DoS attacks, the attack slowly but surely reduces the functionality as well as the overall recital of the wireless sensor network. Projected use of sensor networks in responsive and vital applications makes the prospect of DoS attacks even more alarming.

Table.1. DoS Attacks and Defenses by Protocol Layer [11]

PROTOCOL LAYER	ATTACKS	DEFENCES
Physical	Jamming attack	Sleep stage
	Node devastation	Hide nodes or tamper proof packaging
MAC (Medium access control) Denial of Sleep, authentication and anti-replay Network Spoofing, anti-replay, replaying Authentication	Denial of sleep	Sleep,, authentication and anti-replay
Network	Spoofing attack	anti-replay, Authentication
	Hello floods	Geographic routing
	Homing	Header encryption
Transport	SYN flood	SYN cookies
	De-synchronization	Attack Packet authentication
Application	Path based DoS	Authentication and anti-replay protection
	Reprogramming attacks	

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

6.1 MAC Layer

Data link layer is classified into two sub layer Link layer and MAC layer. The link layer manages the access to the physical medium linking a simple network node. The link layer chooses when the radio should transmit frames; [9] listen to the channel to receive data and sleep to preserve energy. MAC protocols function at link layer and these protocols are used for sensing denial of sleep attacks because they direct the functionality of the transceiver, which devours extra energy than any other components.

The MAC protocol is conscientious for super-visioning the radio of sensor, and radio is focal source of power consumption. To design a secure MAC layer it is vital to know the normal and malicious sources of energy loss, which is necessary to design the power control system.

6.2 Denial of Sleep Attack

It is a procedure which averts the radio from going into sleep mode. Many procedures initiated its impact on battery –powered mobile devices. An attacker might uses jamming attack to devour the energy and battery of the sensor but it would take about many months to completely reduce the targeted devices whereas denial of sleep attack is a intellectual attack that keeps the sensor nodes radio ON that drainpipe the battery in only few days.

Numerous solutions have been projected to solve these types of attack but each has restricted feature which are only concern to the fussy layer. In this study the denial of sleep attack which is type of denial of service attack on data link layer.

7. RELATED WORKS

7.1 Neutralizing Denial-of-Sleep Attacks in Wake-up-radio-based Sensing Systems

Angelo T. Capossele et al. [2] present AntiDoS, a practical framework to counteract sleep deprivation attacks in wake-up-radio-based sensing systems. This approach influence on a easy yet proficient idea: the WuR address of every node should be produced and restructured in a pseudo-random fashion, based on key material recognized only by authorized peers. In this method, an attacker cannot wake up a node unless he/she identifies a shared secret key used to produce legitimate WuR addresses. To manage the exchange of the secret key among legal nodes, a sturdy and secure Key Management Protocol (KMP) is essential. To be versatile in large-scale deployments, the KMP has to presume supple and lightweight approaches that can maintain the dynamic nature of the IoT and of WSNs. A core ingredient of AntiDoS is thus a robust, supple and lightweight Key Management Protocol based on Public Key Cryptography.

This KMP is balanced leveraging on the Fully Hashed MQV protocol [3], an authenticated key contract scheme that offers key materials used to produce secure WuR addresses. A core component of this system is a key exchange protocol inherited from Elliptic Curve Cryptography (the Fully Hashed MQV protocol), which is used in conjunction with inherent certificates.

7.2 Denial of Sleep Attack in Wireless Sensor Network

Brownfield et al. [1] proposed new MAC protocols which alleviate a lot of the effects of denial of sleep attacks by centralizing cluster organization. MAC has some energy saving characters which not only lengthen the network duration, but the centralized architecture makes the network duration more defiant to denial of sleep attacks. Other than distinct period and synchronization message, it has two contention period and dissimilar networks for sending the message within the clusters and outside the cluster by the gateway node. The MAC protocol Performance Results show that G-MAC achieves significantly better than other protocols in every traffic circumstances. [1]The empty network case confirm the protocol overhead and inactive listening effects determined by the duty cycle-MAC has 94% duty cycle is weighted average of duty cycle of gateway node and other nodes. Attacker can get access to network by gateway node. But attacker can only influence one node at a time, because nodes exchange the gateway responsibilities based upon incremental boost in battery levels

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

7.3 Consequence of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols

David R. Raymond et al. [9] categorize sensor network denial-of-sleep attacks by an attacker's acquaintance of the medium access control (MAC) layer protocol and capacity to bypass authentication and encryption protocols. Attacks from each categorization are then modelled to demonstrate the impacts on four sensor network MAC protocols, i.e., Sensor MAC (SMAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC). Implementations of particular attacks on MAC, T-MAC, and B-MAC are illustrated and analyzed in detail to authenticate their effectiveness and analyze their efficiency. And it illustrate that the most proficient attack on S-MAC can keep a cluster of nodes awake 100% of the time by an attacker that sleeps 99% of the time. Attacks on T-MAC can keep sufferers awake100% of the time while the attacker sleeps 92% of the time. With acquaintance of protocol because of dissimilarity exist in packet structure and timing between WSN MAC protocols, and even without capability to penetrate encryption; all wireless sensor network MAC protocols are vulnerable to a full control attack, which decrease the network duration to the minimum possible by maximizing the power utilization of the nodes' radio subsystem. Even without the capacity to penetrate encryption, slight attacks can be launched, which reduce the network duration by orders of magnitude. If sensor networks are to meet present opportunities, they must be strong in the face of network attacks to include denial-of-sleep. This approach also amplifies the network overhead.

7.4 Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks

Raymond D. R. et al. [8] illustrated the host based lightweight intrusion detection method, Clustered Adaptive Rate Limiting (CARL) based on rate restraining approach at MAC layer is projected to defeat denial of sleep attacks. The main weakness of above method is that the period during which nodes are awake is not synchronized, so if a node has packet to send, there is no assurance that other nodes will poll at correct time to eavesdrop a segment of preamble and wait awake for the data packet. The technique used in B-MAC increases latency in multi hop networks and if bursts of network traffic are produce at a higher rate than is sustained by rate- limiting policy, network traffic is lost. So in adaptive rate restraining, network traffic is limited only when malicious packets have been sensed at a rate enough to expect the attack. It can be used to retain network duration and better throughput at a time even in face of sleep denial attack.

7.5 An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks

Chen C. et al. [3] depict a scheme is proposed employing fake schedule switch with RSSI measurement aid. This system spotlight on earlier attack and initiates fake schedule. The sensor nodes can decrease and weaken the damage from exhaustion attack and on the converse make the attackers lose their energy rapidly so as to die. Simulation results illustrate that at a bit price of energy and delay, network health can be assured and packets drop ratio has been reduced when compare with original circumstances without this scheme. This system considers only S-MAC protocol with duty cycle 10%. If packet failure is not caused by the attack, then fake schedule switch is dangerous. Due to which RSSI is used as a value consigned to each node and node having attacker one hop away has well-built RSSI value.

7.6 Sleep Deprivation Attack Detection in Wireless Sensor Network

Tapalina Bhattasali et al. [11] illustrated a hierarchical framework based on distributed collaborative method for sensing sleep deprivation torture in wireless sensor network efficiently. In heterogeneous sensor field, sensor nodes are categorized into an assortment of roles such as Sector-in –charge (SIC), sink gateway (SG), sector monitor(SM) and leaf node (LN) based on their battery power. Here leaf node is used to detect the data, SIC is used to accumulate the data and SM sense the data as valid data and invalid data. Sink Gateway is used to access all other networks. If leaf nodes are openly affected by intruder, node cannot spot it. As a end result battery of affected node may be short or exhausted completely. This can affect data transmission for network due to which it is done in authenticated way.

7.7 Optimal Dynamic Sleep Time Control in wireless Sensor Networks

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

Ning et al. [6] illustrated d the dynamic sleep time sooner than fixed sleep time which reduce the energy wasted in inactive channel i.e. energy to broadcast and receive the message. This paper has used the dynamic programming (DP) algorithm rather than differential equations (ODE) to find the global best possible solution. Problem with this approach is that there are some cases where it is not possible to find global best possible solution using DP therefore ODE has to be used which is difficult to implement and is complex.

Table.2.Comparative Scrutiny of Sleep Deprivation Attack Detection Techniques

DETECTION TECHNIQUES	STRENGTHS	WEAKNESS
EllipticCurve Cryptography (the Fully Hashed MQV protocol)[2]	wake-up-radio-based sensing systems outperforming competing security schemes in terms of both computation and communication overhead	Complex Structure and Scalability issue in teams of key handling.
Sensor MAC (S-MAC) [1] Timeout MAC (T-MAC) [1] Berkley MAC (B-MAC) [1] Gateway MAC (G-MAC) [9]	Simple energy-efficient protocol extends WSN network lifetime.	(i) Fixed sleep cycle makes it vulnerable to broadcast as well as uni-cast attack. (ii) Inflexible in responding to network traffic fluctuations or network scaling. (iii)It is more vulnerable to a broadcast attack.
Random Vote Scheme [11] Round Robin Scheme [11] Hash based Scheme [11]	(i) Dynamic sleep cycle makes network flexible and scalable. (ii) Energy saving is comparatively better. (iii) It works well in ultra-low traffic networks.	Performance significantly decreases because each passive node has to wake up and receive every message.
Clustered Adaptive Rate Limiting (CARL)[3]	It performs significantly better than the other in every traffic situation.	All cluster nodes entirely dependent on gateway node.
RSSI Measurement Aid[11] Markov Decision Process (MDP)[6]	It reduces probability of selecting adversary cluster head; so that exhaustion of sensor nodes by cluster head is reduced.	(i) It requires more iteration to complete the algorithm. (ii) When number of compromised nodes within a cluster increases, For large cluster, each node requires an unrealistic amount of per-node storage, which enhances the overhead.

8. CONCLUSION

This study evaluate about WSN and some of the types of denial of sleep assault. This study also illustrates various existing solutions, allowing you to learn about their advantages and disadvantages and to compare them with one another. When deciding how to protect the sensor nodes, researchers might look to this paper as a possible resource. DoS is not merely a new security risk, but will have far-reaching consequences as WSN is inevitably adopted by IoT technology in the not-too-distant future. In near future a vital solution of protecting the sensor nodes in the clusters, so that it can make sure sensor nodes is able to handle with assaults.

REFERENCES

1. M. Brownfield, Yatharth Gupta and N. Davis, "Wireless sensor network denial of sleep attack," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 2005, pp. 356-364.doi: 10.1109/IAW.2005.1495974.

2. Capossele, Angelo & Cervo, Valerio & Petrioli, Chiara & Spenza, Dora. “Counteracting Denial-of-Sleep Attacks in Wake-up-based Sensing Systems",13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2016.

3. C. Chen, L. Hui, Q. Pei, L. Ning and P. Qingquan, "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," Fifth International Conference on Information Assurance and Security, Xi'an, 2009, pp. 446-449. doi: 10.1109/IAS.2009.33.

4. Giuseppe Ateniese, Giuseppe Bianchi, Angelo T. Capossele, Chiara Petrioli, Dora Spenza, "HELIOS: Outsourcing of Security Operations in Green Wireless Sensor Networks", 85th IEEE Vehicular Technology Conference (VTC Spring) 2017, pp. 1-7.

5. Jia-Ching Wang, Chang-Hong Lin, Ernestasia Siahaan, Bo-Wei Chen, Hsiang-Lung Chuang, "Mixed Sound Event Verification on Wireless Sensor Network for Home Automation", IEEE Transactions on Industrial Informatics, 2014, vol. 10, pp. 803-812, ISSN 1551-3203.

6. X. Ning and C. G. Cassandras, "Optimal Dynamic Sleep Time Control in Wireless Sensor Networks," 2008 47th IEEE Conference on Decision and Control, Cancun, pp. 2332-2337, 2008. doi: 10.1109/CDC.2008.4738768.

7. Pirretti M., Zhu S., Vijaykrishnan N., Mcdaniel P.,Kandemir M., Brooks R., “The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence”, International Journal of Distributed Sensor Networks,2006, Vol.2,no.3,pp.267-287.doi: 10.1080/ 15501320600642718.

8. Rajeev Piyare, Amy L. Murphy, Csaba Kiraly, Pietro Tosato, Davide Brunelli, "Ultra Low Power Wake-Up Radios: A Hardware and Networking Survey", Communications Surveys & Tutorials IEEE, 2017, vol. 19, pp. 2117-2157.ISSN 1553-877X.

9. D. R. Raymond, R. C. Marchany, M. I. Brownfield and S. F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," in IEEE Transactions on Vehicular Technology, Jan. 2009,vol. 58, no. 1, pp. 367-380. doi: 10.1109/TVT.2008.921621.

10. D. R. Raymond and S. F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-of-Sleep Attacks in Wireless Sensor Networks," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-7.doi: 10.1109/MILCOM.2007.4455251.

11. Tapalina Bhattasali, Rituparna Chaki, Sugata Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network", International Journal of Computer Applications, February 2012,vol.40, no.15. Pp.19-25. doi: 10.5120/5056-7374 10.5120/5056-7374 10.5120/5056-7374 10.5120/5056-7374.

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

12. Wei Ye, J. Heidemann and D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks," in IEEE/ACM Transactions on Networking, June 2004,vol. 12, no. 3, pp. 493- 506. doi: 10.1109/TNET.2004.828953.

13. Wei Ye, J. Heidemann and D. Estrin, "An Energy-efficient MAC Protocol for Wireless Sensor Networks," Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 2002, pp. 1567-1576, vol.3.doi: 10.1109/INFCOM.2002.1019408.

14. S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?," in IEEE Communications Magazine, vol. 39, no. 6, pp. 130-137, Jun 2001.doi: 10.1109/35.925681.