ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 6, June 2014*

# Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey

**Annie Jenniefer[1], John Raybin Jose[2]**

M.Phil, Scholar, Department of Computer Applications, Bishop Heber College (Autonomous), Trichy[1]

Asst. Professor & Head, Department of Information Technology, Bishop Heber College (Autonomous), Trichy[2]

**Abstract**: Wireless Sensor Networks is a type of computer network, which is commonly used for environmental monitoring and military observation. Wireless sensor networks are frequently affected by jamming attacks and broadcast attacks. Securing WSN is a challenging task. The prominent attack in WSN is Denial of Service (DoS) attack. DoS attack is caused by jamming single or group of nodes and there by disrupting the communication. This paper depicts the different types of DoS attacks. It also elaborates the techniques adopted by several researchers for Detecting DoS attacks.

**Keywords:** Wireless Sensor Networks, Denial of service attacks, Monitor Node, Gateway Medium Access Control, Evasion, Multi Dataflow, Lightweight Medium Access Control, Weighted Centroid Localization.

## I. INTRODUCTION

Presently wireless sensor networks have gained universal attention and mainly spread in Micro-Mechanical System (MEMS) technology which has facilitated the growth of advanced sensors. These sensors are tiny, with narrow dealing out and computing resources and they are of low-cost compared to conventional sensors. These sensor nodes can intellect, evaluate and congregate information from the surroundings and based on some local conclusion methods. WSNs have immense possibilities for applications in scenarios such as armed intention tracking and scrutiny, natural disaster relief, biomedical health monitoring, dangerous surroundings investigation and seismic sensing. In military target tracking and surveillance. WSN can also support in invasion finding and credentials. Natural disasters, sensor nodes can intellect and distinguish the environment to predict disasters before they arise. In biomedical applications, surgical implants of sensors can help to screen a patient's health. Sensors along the volcanic area can perceive the maturity of earthquakes and eruptions. The applications of WSNs include environmental control, habitat monitoring, object tracking, nuclear reactor control, fire detection and traffic monitoring. There exists various security attacks in wireless sensor networks such as: (i) Denial of Service attack (ii) Sink hole attack (iii) Black hole attack (iv) Worm hole attack (v) Selective forwarding attack (vi) Sybil attack (vii) Node replication attack.

The types of WSNs are structured WSN and unstructured WSN. Sensor nodes may be deployed in an ad hoc method into the field. WSN offer a bridge between the real physical and virtual worlds and posses the capability to monitor the wide range of possible applications to industry, science, transportation, civil infrastructure, and security. Wireless sensor networks present the capability for applications to scrutinize and respond to actions, but their isolation introduce challenges and vulnerabilities for network manage and energy consumption. Wireless networks are deployed in open RF communication link, and communication happens in the same frequency band. So radio snooping or spying is very easy. The sensor nodes are low-cost and use minimal resources like power, bandwidth, and storage. It is difficult to add strong security algorithms as those are complex to implement. As a result, sensor networks adopt low-cost modest security protocols. WSN is deployed in extreme climatic conditions and terrains. It is difficult to continuously to monitor these networks for potential attacks.

The main objective of this paper is to give an overview for researchers and developers on different techniques available to prevent Denial of Service attack. The paper is organized as follows: Section 2 presents the overview of Denial of Service attack, Section 3 classifies the previous works on Denial of Service attack, Section 4 gives the future research direction and the final section concludes this paper.

## II. DENIAL OF SERVICE (DoS) ATTACKS

Any type of intentional activity that can disrupt, subvert or even destroy the network is known as a Denial of Service (DoS) attack. Basically, DoS attacks can 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.

DoS attack target the network resources. The hardware of sensor nodes is typically constrained and attackers can try to overload them. The DoS attack is one of the major energy consumption attacks in a WSN. DoS attacks are dependent on the vulnerabilities of each layer in the layered architecture of wireless networks. The physical layer being the lowest layer and the first to be attacked by jammers. This physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. As an outcome of DoS attack, the sensor node fails to function when the energy is exhausted. Sensor nodes are vulnerable against this type of physical attack. DoS attacks are very critical such as jamming attack and tampering attack. Jamming is the deliberated interference of the wireless communication channel. Tampering is another type of physical attack, which targets the actual hardware of the sensor nodes. In this attack, it is difficult to know whether any particular DoS situation is caused intentionally or unintentionally. [1] The WSN's denial of sleep attack is a subset of the Denial of Service class of network attacks. Stajano and Anderson first mention denial of sleep attacks in 1999 as "sleep deprivation torture". Energy –limited system designers often incorporate power management mechanisms to monitor active processes and power down non-essential subsystems when feasible. A denial of sleep attack penetrates a device's power management system to reduce the opportunities to transition into lower power states.

## III. **RELATED WORK**

Several researchers have worked with different techniques to detect DoS attack and to identify the malicious nodes that source Denial of Service attack in wireless sensor networks. Those techniques are classified and depicted below in Fig 1.

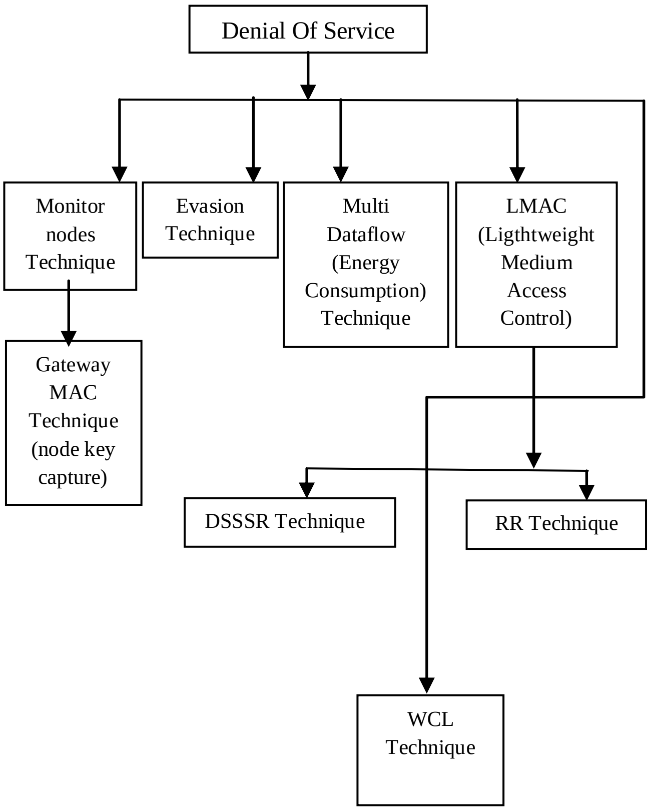
Denial Of Service
Monitor nodes Technique
Evasion Technique
Multi Dataflow (Energy Consumption) Technique
LMAC (Ligthweight Medium Access Control)
Gateway MAC Technique (node key capture)
DSSSR Technique
RR Technique
WCL Technique

Fig 1. Classification of Denial of Service attacks

### A. Monitor Nodes Technique

Monitor nodes supervise whether there occurs any jamming or misrouting of information through other remaining nodes. Manju V.c and Sasi Kumar M [2] has proposed a technique for identifying jamming attack in the wireless sensor networks. Based on residual energy of nodes some of the existing nodes are marked as monitor nodes. These nodes collect the Receiver Signal Strength Indicator and packet delivery ratio from all the other nodes. Based on this metric, they compute a weight value of each node. The computed weight value is compared against the threshold value. When the estimated weight value goes beyond the threshold value, the corresponding node is marked as jammer and it is isolated from data transmission. This technique significantly improves system performance.

### B. Gateway MAC Technique

G-MAC is an energy efficient sensor medium access control technique designed to coordinate transmission within a cluster. Michael Brownfield, et al., [1] has described the energy resource vulnerabilities of Wireless Sensor Networks. They also proposed a new MAC protocol which mitigates many of the effects of denial of sleep attacks. G-MAC has several energy-saving features. It shows guarantee in extending the network existence and also the centralized architecture makes the network more resistant to denial of sleep attacks.

### *C. Evasion Technique*

Wenyuan Xu, et al., [4] has proposed two different but complementary approaches. First approach is to simply retreat from the interferer, which may be accomplished by either spectral evasion (channel surfing) or spatial evasion (spatial retreats). The second approach aims to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, for achieve communication in the presence of the jammer. These techniques are important areas for studying and classifying the scenarios where one defense strategy is advantageous over another.

Mingyan Li, et al., [3] have derived solutions to the optimization problems, optimal attack and network defense strategies. They also found alternatives for modeling lack of knowledge for the attacker and the network.

### D. Multi Dataflow Technique

Multi dataflow is a topologies scheme that can effectively defend the mobile jamming attack. Hung-Min Sun, et al., [5] have multi dataflow topologies scheme to reduce the affected area caused by the mobile jamming attack. Mobile jamming attack not only causes the energy consumption but also breaks the routing on WSN and also shows that the existing defense mechanism is unable to withstand this attack.

### E. WCL Technique

The low complexity, the fast calculation and the minimal resource requirements recommend WCL as localization algorithm in wireless technique. Jan Blumenthal, et al., [6] has introduced Weighted Centroid Localization technique to make it fast and easy for the algorithm to locate devices in wireless sensor networks.WCL algorithm is derived from a centroid determination which calculates the position of devices by averaging the coordinates of known reference points. They summarized the basic theoretical and practical facts concerning the analysis of RSSI measurements.

### F. LMAC Technique

LMAC has proven to be the most resistant protocol against energy efficient attack. LMAC is a good representative of the TDMA category. In LMAC time is divided into frames, which are further divided into time slots. David R. Raymond and Randy C [7] have classified the Lightweight Medium Access Control (LMAC) technique. Initially, it classified denial-of-sleep attacks on WSN medium access control protocols based on an attacker's knowledge of the MAC protocol and ability to penetrate the network. Next, it explored potential attacks from each attack classification. The impacts on sensor networks running for leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks. Finally, it proposed a framework to defend against denial of- sleep attacks and provides specific techniques that can be used against each denial-of-sleep vulnerability.

Ahmed R. Mahmood, et al., [8] has proposed and evaluated two modifications to the Lightweight Medium Access Control (LMAC) [3] protocol. The first is Data Packet Separation Slot Size Randomization (DSSSR) and the second is Round Robin (RR) slot size assignment. Enhancing the attack and applying it to other types of protocols is also a potential future work because the war between the attacker and defender never ends.

Saman Taghavi Zargar and James Joshi [9] in their work have explore the scope of the DoS flooding attack problem and attempts to combat it and categorize the DoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DoS flooding attacks.

## IV. FUTURE RESEARCH DIRECTION

The denial of sleep vulnerabilities for leading Wireless Sensor Networks medium access control protocols and models the catastrophic effects. These attacks can have on a deployed network. Gateway MAC establishes an effective denial of sleep defense by centralizing cluster management. Future work in WSNs protocol research includes analyzing other security vulnerabilities such as physical layer jamming, node key capture containment and network layer misrouting. To providing solutions for these resources constrained networks requires delicate tradeoffs in security, performance and usability.

## V. CONCLUSION

The paper have provides a detailed and comprehensive study on DoS attacks in Wireless Sensor Networks and classifying them according to their underlying techniques. Protected transaction is very tricky in wireless sensor network. This paper researched many efficient detection techniques for denial of service attacks in wireless sensor network proposed by various researchers around the universe. There are many other techniques for detecting DoS attack. By using the above techniques we can make secure communication in wireless sensor network.

## ACKNOWLEDGEMENT

This work was supported by my guide *John Raybin Jose. J* Assistant Professor and Head of the Department of information Technology from Bishop Heber College.

## REFERENCES

[1] Michael Brownfield, Yatharth Gupta "Wireless Sensor Network United Denial of Sleep Attack" Proceedings of the 2005 IEEE Workshop on Information Assurance States Military Academy, West Point, NY June 2005

[2] Manju V.c, Sasi Kumar M "Detection of Jamming Style DoS attack in Wireless Sensor Network" IEEE International Conference on Parallel Distributed and Grid Computing 2012

[3] Mingyan Li, Iordanis Koutsopoulos, Radha Poovendran "Optimal Jamming Attacks and Network Defense in Wireless Sensor Networks" IEEE Transactions on Mobile Computing August 2010

[4] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang "Jamming Sensor Networks: Attack and Defens Strategies. IEEE Network. May/June 2006

[5] Hung-Min, Shis-Pu, Chien Ming Chen, "Mobile Jamming Attack and its countermeasure in Wireless Sensor Networking and Applications" Workshops 21 st International conference on Advanced Information Networking and Applications Workshops, 2007.

[6] Jan Blumenthal, Ralf Grossmann, Frank Golatowski and Dirk Timmermann, "Weighted Centroid Localization in Zigbee-based Sensor Networks", IEEE International Symposium on Intelligent Signal Processing, (WISP 2007), pp-I-6, 2007

[7] David R. Raymond, Randy C "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols "IEEE Transactions on Vehicular Technology, Vol 58, hNo.I January 2009.

[8] Lodewijk van Hoesel,Yee Wei Law, Jeroen Doumen, Pieter Hartel, Paul Havinga "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Networks MAC Protocols". Proceedings of 3rd ACM workshop on security of ad hoc and sensor networks. March 31, 2006.

[9] Saman Taghavi Zargar, James Joshi, David Tipper, "Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks" IEEE communications surveys 2013

[10] Shivangi Raman"Wireless sensor networks: A Survey of Intrusions and their Explored Remedies" International Journal of Engineering Science and Technology Vol.2(5), 2010.

## BIBLIOGRAPHY

**ANNIE JENNIEFER CHRISTOPHER** received M.C.A degree with distinction from Holy Cross College (Autonomous) Affiliated to Bhatathidasan University Nationally Accredited ($3^{rd\ Cycle}$) with 'A' Grade by NAAC in 2013. Currently pursuing M.Phil degree in Bishop Heber College (Autonomous) Affilliated to Bharathidasan University.