# Denial of Service Attacks and Their Countermeasures in WSN

Mian Ahmad Jan[1],

[1]Department of Computer Science
Abdul Wali Khan University
Mardan, Pakistan
mianjan@awkum.edu.pk

Muhammad Khan[2]

[2]Department of Computer Science
Bacha Khan University
Charsadda, Pakistan
knmuhammad@gmail.com

**Abstract**

Wireless Sensor Network consists of tiny miniaturized motes which gather information about their vicinity and collaborate with each other through wireless link.These motes are mostly deployed in a harsh environment and left unattended for the duration of their lifetime. Hostility of the environment and physical intervention possess various threats to these energy-thirsty sensor motes which results in severe catastrophic affects. In this paper we have provided a brief overview of denial of service attacks at various layers and proposed countermeasures available in literature and our proposed solutions in Wireless Sensor Network.In Denial of Service attack, a sensor node is deprived of resources in one way or another. Also, security is classified into four major classes in this paper. Tabular form of these security threats is provided to depict the severity and calamitous nature of these attacks.

**Keywords:**Wireless Sensor Network, Denial of Service Attack, Base Station, Sensor Node, Security

## 1. Introduction

Latest development in Micro-Electro-Mechanical Systems (MEMS) has enabled the development of low cost, miniaturized sensormotes or nodes [1]. All necessary circuitry along with memory and processing modules are fabricated on a single chip due to MEMS technology. With the advancement of research, the size and cost of sensor nodes is minimizing without compromising the standard and quality of the nodes. The nodes are becoming smarter in terms of intelligence and conscientious.Wireless Sensor Network (WSN) [2] is a promising technology, well adapted to meet a growingneed for environmental data collection. Implementation allows spatial and temporal monitoring which yields information for solving complex environmental problems. Applications of WSN are numerous and can be broadly classified into two categories: Monitoring [3, 4] and Tracking [5, 6].

Due to small size, these nodes are constraints on energy, data rate,communication bandwidth, computation power, storage etc. These nodes are equipped with AAA batteries as the major source of power supply. Data rate ranges from 20kbps to 250kbps using Zigbee protocol stack. Available RAM is on the order of few kilobytes (normally 4kB depending on the type of node) and flash memory ranges are in order of few Megabytes. One of the major differences between traditional networks and WSN is that the latter is capable to operate in harsh and remote locations which expose the nodes to various types of threats and attacks. Attacks ranges from environmental vulnerabilities and human interference to sophisticated intruders and malicious nodes presence in the network. In WSN, attackers can either temper the nodes or data in

transit.Traditional security mechanisms do not fit well with these networks due to their resource-constraint nature. Researchers have proposed various mechanisms keeping in mind these constraints. In this paper we have provide a brief overview of various form of Denial of Service (DOS) attacks in Wireless Sensor Network ranging from physical layer to network layer. DOS attacks deprive a legitimate node of various resources like available bandwidth, available channels, energy etc. by providing it with false network information, bogus acknowledgement messages, excessive connection requests, interfering with its signals etc.

This paper is divided into six sections: In Section II, we presented security requirements in WSN. In Section III, security is classified into four major classes. In Section IV, various types of DOS attacks and vulnerabilities are discussed follow by their countermeasures in Section V. Section VI concludes the paper with future directions.

## 2. Security Requirements in Wireless Sensor Network

WSNneeds to ensure to protect communication between nodes and network resources from potential threats. WSN must ensure to meet the following major requirements along with many others.

*Data Confidentiality:* Any security mechanism in place should ensure that data should be delivered to the right recipient intact. In WSN, communication is mostly multi-hop. As thedata passes from various nodes till it reaches the intended recipient, hence it should not be understood by these nodes except the final destination of the data.

*Data Integrity***:** The data should not be altered on its way to the receiver.

*Availability:* WSN should provide services even in every situation. Presence of security threats should not affect the capabilities of WSN: Availability

*Data Freshness:*Any security mechanism intact should ensure that data is recent. It is possible that attacker replays old data which is of no use. This is the case during refreshing security Keys, during which attacker replay old data using old key. Counter need to be attacked to each packet to determine its freshness.

*Authentication:* The sender of the data must be the one who it claims to be. It is possible that an attacker hijacks another node identity or fabricates packets. Attacker not only has the capabilities to change packets but can also inject packets in the network. Hence it is very important that a security mechanism should be intact to make sure that packets are authenticated sender.

## 3. Security Classes In Wireless Sensor Network

Pfleeger [7] has identified four major classes of security threats in any computing systems. These four threat classes can be integrated in Wireless Sensor Networks [8.Tanvir Zia]. In any computing systems, hardware, software, and data are the main assets. Our goal in WSN is to protect the network, nodes and communication among the nodes. In Figure 1, these major classes of threats are illustrated which exploit the vulnerability of any security goal.

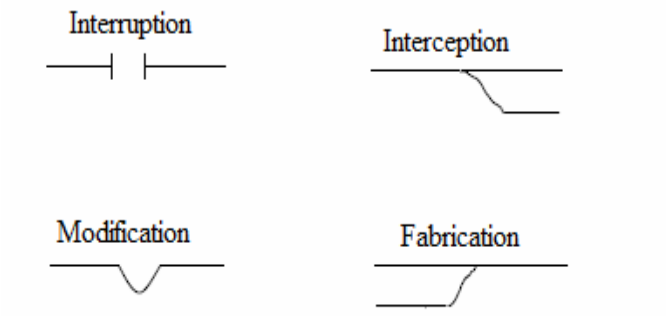



Figure 1: Pfeeger's Four Classes of Systems Security Threats

In*interruption*, the communication link among the sensor nodes in WSN is lost or unavailable. Well known examples of interruption are message corruption, fabrication of malicious code, node capture, etc.

In *interception*, WSN is compromised by an adversary where the attacker gains unauthorized access to the node or its data. For example node captures.

In *Modification*, unauthorizedintruderfirst access the data and then tamper it before injecting it in the network. For example, modifying the data in transit which has severe consequences in applications where the network flow is based on flooding.

In *fabrication*, an adversary injects false and fabricated data packets and hence compromises the

sensitive information which is supposed to be trustworthy.

All these types of attacks adversely affect the network in one way or another, not only compromising the nodes but also the data in transit.

## 4. Denial of Service Attacks in Wireless Sensor Network

Wireless sensor networks are vulnerable to various types of security threats. These attacks are classified into three classes [12].

- Denial of Service (DOS) Attacks
- Attacks on Secrecy and Authentication
- Stealthy attacks against Service Integrity

The scope of this paper is restricted to denial of service attack as it's in itself a very broad area. Any event which diminishes or eliminates Network's Capabilities to perform its expected functions is known as DOS attack [9]. Denial of Service occurs in one way or another in various forms: Resource exhaustion, software bugs, hardware failure, environmental conditions etc. DOS attacks are so diverse in nature that they exist at each layer of sensor network architecture. In this section we will explore the various types of security threats and vulnerabilities at each layer of WSN architecture.

### 4.1 DOS Attacks at Physical Layer

Physical layer is responsible for frequency selection, modulation, carrier frequency generation, link quality indication, clear channel assessment and tuning the transceiver. Attacks at Physical Layer are *Jamming* and *Tampering*

In *jamming*, the attackers interfere with the frequencies of the nodes. Malicious nodes of the attackers use the same set of frequencies as the nodes in the network. Jamming the whole network will completely destroy the network and is a classic example of DOS attack. However, in a very large sensor network, it becomes very difficult to jam the whole network.

Another attack common at physical layer is tampering. As sensor nodes are left unattended after deployment, it is quite obvious that an intruder would either capture the node by modifying its programming code, tampering its circuitry or injecting fabricated code in a legitimate node.

### 4.2 DOS attacks atMAC Layer

The link or media access control (MAC) layer is responsible for channel access control and collision avoidance using Carrier Sense Multiple Access with Collision avoidance (CSMA/CA) protocol. Functionality of MAC varies depending on the type of protocol deployed. In case of Zigbee nodes and protocol stacks, apart from collision avoidance and channel access control functionality, the MAC layer is also responsible for Beacon frames management and super frames definition. The most common types of vulnerable situation at this layer are *collision* and*exhaustion*[9].

In *Collision*, adversaries induce a collision in one octet of a packet in order to disrupt an entirepacket. Change of a single bit in a packet makes the packet damages and need to be retransmitted.The reason isthat the trailer in a frame at the receiver end would not match and results in a checksum mismatch. Also, it is possible that a corrupt Acknowledgment (ACK) packet is being transmitted by the sender which causes costly exponential back-off in some MAC protocols.

Another vulnerable situation which arises at MAC layer is *exhaustion*. It can either be imposed by the intruder or by a legitimate itself by compromising it. A sensor node can sacrifice itself by continuously transmitting join-request message to affiliate itself with the network and hence consume all or major portion of its own energy. It is mostly because that an intruder modifies the program code in a sensor node to act in a malicious way. Another form of resource exhaustion is, when an intruder node sends numerous join-requests or by the sending too many acknowledgment frames.

### 4.3 DOS attacks at Network Layer

Network layer is responsible for routing, route discovery, connection setup, neighbor discovery and link recovery from failure etc. The most common

types of attacks at this layer is Interception attacks in which information in transit is being compromised. Some of the most common attacks at this layer are *Spoofing, altered and replay attacks,Sybil, Sinkhole, Black hole, Wormhole, Selective Forwarding, homing* etc.[10].

In *Spoofed, Altered and Replay attack,*routing information in transit between nodes is being targeted. Packets in transit can be spoofed, modified and also can be replayed. Once these packets are modified, Data Integrity is lost and replaying modified version of the data will cause malicious data to arrive at the sink node (Base Station). Some of the consequences of this attack are: Attracting or repealing traffic, generating routing loops, increasing end to end latency, generating false error messages etc.

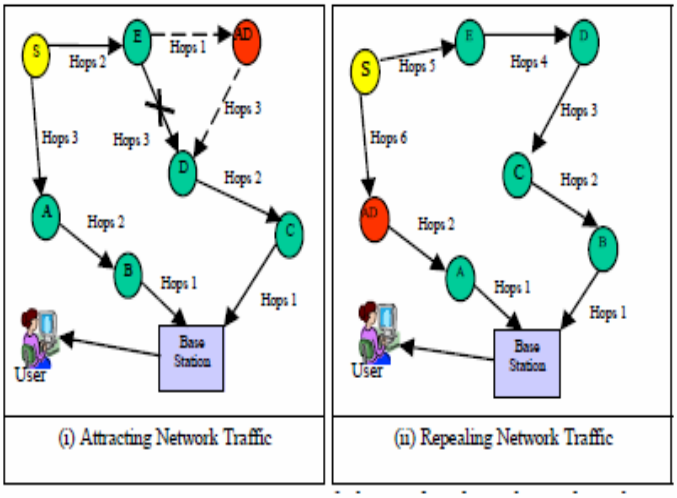
In *Selective Forwarding,* malicious nodes will drop packets on its way to the base station. Ideal location for adversary is near the base station. Adversary can either drop all the packets or follow selective drop and forward Policy. In former case, neighboring nodes will realize that the adversary has failed since it drops all data. So adversary uses *selective forwarding* by dropping some packets and forwards the rest.

In *Worm Hole* attack, malicious nodes receive data in one part of the network and tunnel it to the other part of the network and replay them over there. Simplest form of Worm hole is, when a malicious node forward packets between two nodes in the network. However, *Worm Hole* is more than it. Worm hole is created when a High Power Laptop class adversary convinces neighboring nodes that they are one or two hops neighbor of the sink node. This can be done by advertising very high quality routes to the sink node. Surrounding nodes forward their packets to this node as this route is attractive to the nodes instead of other link. In this case *wormhol*e can create Sinkhole and Selective Forwarding attacks as well.

In most sensor networks, some of the nodes have special responsibilities, For example, Cluster Head node in a specific Cluster as in most clusters based routing protocols. Also, there are more powerful nodes which might serve as managers for cryptographic keys, query monitoring or network uplinks. Since these nodes play special role, so it is natural for the attackers to have more focus on them as compare to ordinary sensing nodes. This is where the concept of *homing* comes into play.

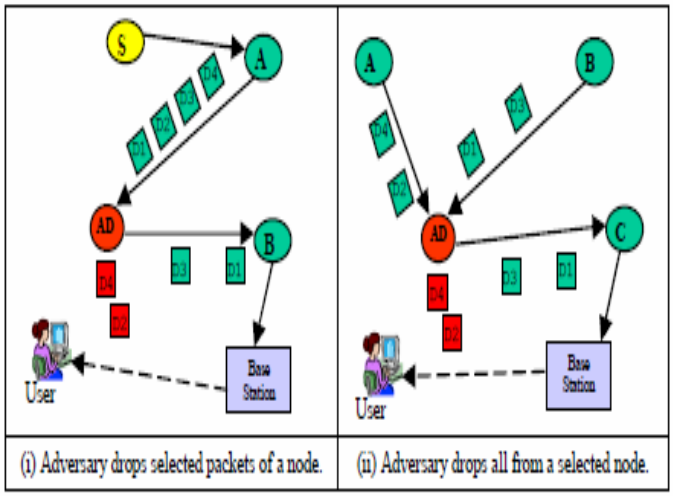
In *Sybil* attack[10], an attacker possesses multiple identities at the same time at a single point. Sybil attack give rises to many other attacks like resource exhaustion, unfairness, selective forwarding etc. By posing multiple identities, a single attacking node obtains multiple network resources which cause scarcity for others. In worst case scenario, these Sybil nodes participate in voting conducted by the base station on the integrity and identity of a legitimate node and hence declare them mischievous nodes and illegitimate during voting.

Figure 2: Various types of DOS attacks



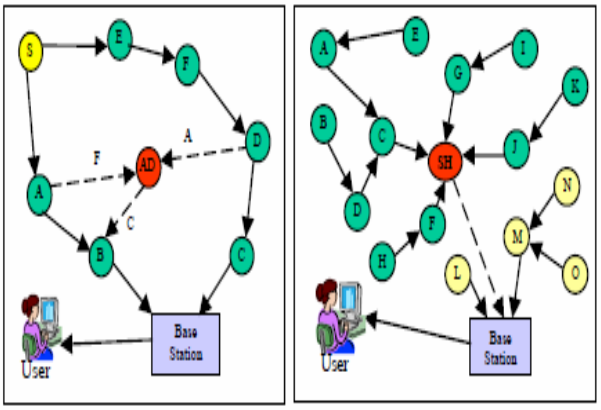

Spoofed, Altered and Replay Attack

(a)




Selective Forwarding

(b)




Sybil Attack Sinkhole Attack

(c)

Figure 2: Various DOS Attacks

In *Sinkhole* attack, the attacker attracts almost all the traffic to a specific compromised node. The compromised node is placed in an area which has more scope and vision of the network traffic. Ideal location for such nodes is "Near Base Station or Sink ". Hence these intruders' node form a "Sphere of Influence" by attracting almost all the traffic destined for the sink node [11]. This malicious node poses to be the sink node which in reality is not. Figure 2 shows these various types of attacks in WSN.

## 5. Defense Mechanism against Denial of Service Attacks

In this section, we have provided a brief overview of defense mechanism to combat various threats and vulnerabilities at different layers in WSN architecture.

Frequency hopping spread spectrum or Code spread spectrum is used to combat *jamming*loopholes [9]. However, code spread spectrum is not feasible for sensor networks because it requires complex circuitry and high power which is not feasible with tiny sensor nodes. In Frequency hopping spread spectrum, nodes switches carrier among the available band of channels. It becomes very difficult for the attacker to attack unless the attacker has an idea about the frequency selection sequence or attack a wide range in the frequency band. Another defense mechanism is that the nodes experiencing jamming signal especially those on the boundary of the jamming area and their neighbor generate high power, prioritize packets which need to be transmitted to the base station/sink immediately. However it is only possible if jamming is intermittent in nature. It is the responsibility of the nodes to send these packets sincerely to the sink. Also the nodes can buffer if in case Jamming starts again during transmission of this packet. Another option is to route packets around jamming area by avoiding the nodes which are affected by the jamming signal.

Our proposed solution suggests switching the aggregator node on regular basis based on the amount of energy. Jamming has catastrophic affects in case the attacker jams nodes near the base station (aggregator nodes). Aggregator nodes are normally one-hop neighbor of the sink. There should be enough one-hop neighbors of the base station and base station must switch between them. Also, there should be enough distance between aggregator nodes because in case if one of the aggregator nodes is compromised, base station should switch to the other aggregator node. Distance between aggregator nodes is needed because attacker doesn't only jam the node but also its surrounding nodes.

Our proposed solution against *Tampering*at physical layer is to raise an alarm whenever a node is being touched by unauthorized party. Though, it will come with expense of overhead. Also nodes are possibly exposed to intense heat, which can harm their circuitry, Plastic/Heat proof coating is solution for it.

Possible solution for *Collision* avoidance at MAC layer is to use Error-correcting codes in the frames trailer which provide a flexible mechanism to detect corruption in messages at any layer of WSN.

To avoid *Exhaustion* at MAC layer, admission control *rate limiting*is used. In this mechanism, network ignores excessive requests and hence avoids transmitting expensive radio transmissions. However, rate limit cannot drop below the expected threshold data rate supported by the network in order to maintain an acceptable level of Quality of service for example queuing delay, throughput, packet drop probability, latency etc.

Appending Message Authentication Code (MAC) with the message will help to verify if the message has been *spoofed or altered* at the network layer. MAC is generated by using MAC algorithm. MAC algorithm takes Message and Secret Key (K) as input to generate MAC.

*Replay* attack at network layer can be avoided by introducing Counter or Timestamp to the message which will determine whether the data is recent or not. Appending Sequence Number/Counter in each packet will tackle replay attacks.

*Sybil* attack can be prevented by validating the identity of each node in order to ensure that the each node identity is the only identity presented by each physical node of the network. Identity validation can be performed either by Direct or Indirect validation. In direction validation, a node directly tests the legality of another node to ensure if it is valid or not. In indirect validation, those nodes which have already been identified and validated as legitimate are allowed to vouch for or repudiate other nodes.
Another defense mechanism against Sybil attack is Radio Resource Testing (RRT).Any physical device has only one radio and is incapable of simultaneously sending or receiving on more than one channel.
A node assigns each of its *n*neighbors a different channel.By challenging a neighbor node on the exclusively assigned channel, a sensor node can detect Sybil nodes with a certain probability.

Packet Leashes is a solution for *Worm Hole* attack. Leash is a piece of information which is used to restrict the maximum distance a packet can flow. Packet Leash can be either geographical or temporal. Geographical leash insures that the recipient of the packet is within a certain distance from the sender.Temporal leash ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).

*Selective Forwarding* can be prevented by using multiple disjoint paths: Nodes on disjoint paths must also be disjoint. Also checking sequence number of the packets can avoid this threat. If sequence number is altered, this means that there is malicious node in the middle.

Table 1 gives a brief overview of various types of attacks and their countermeasures [12]. The table includes a wide variety of attacks existing at various layers.

| **LAYER** | **ATTACKS** | **DEFENSE** |
|---|---|---|
| Physical | Jamming | Spread-spectrum, PriorityMessages, Lower Duty Cycle, Region mapping, Mode Change, SwitchingAggregator Nodes |
| | Tampering | Plastic/Heat proof coating, Raising Alarm |
| MAC | Collision | Error-Correction Code |
| | Exhaustion | Rate Limiting, Rejecting Excessive Connections Request. |
| | Unfairness | Small Frames Transmission |
| Network | Spoofed, Altered and Replay | Message Authentication Code, Monitoring, Time Stamps |
| | Selective Forwarding | Multiple Disjoint Paths, Egress Filtering, Authentication, Monitoring |
| | Sinkhole | Redundancy Checking |
| | Sybil | RTT, Authentication, Monitoring, Redundancy |
| | Wormhole | Authentication, Probing |
| | Hello Flood | Authentication, Packet Leashes |
| | Acknowledgment Flooding | Authentication, Bi-directional Link authentication |
| | Sniffing Attack | Encryption Techniques |
| | Data Integrity Attack | Asymmetric Key for Encryption |
| | Node Replication Attack | Base Station Computed Data Gathering Paths. |

Table 1: DOS Attacks and their Countermeasures

## 6. Conclusion

In this paper we have provided a brief overview of various types of Denial of service attacks at various layers in Wireless Sensor Network and also proposed various type of defense mechanism in order to combat them along with presenting the already existing defense solutions present in literature. Denial of Service attacks severely affects the functionality of the nodes and Wireless Sensor Network in general. These attacks deny the functioning of the network by either jamming its signal or intercepting packets in transit or by fabricating malicious codes and data into the network. We provided a brief introduction of these attacks followed by various types of such attacks at different layers. These attacks are evaluated and provided with various defense mechanisms in tabular form.
Currently, we are working on Sybil attacks detection and its various forms and the level of severity it poses to the network. Various defense mechanisms are to be proposed based on a conceptual model and later to be evaluated in OPNET modeler.

## Acknowledgement:

This work is fully supported by Abdul Wali Khan University, Mardan, Khyber Pakhtun Khwa (KPK), Pakistan and Bacha Khan University, Charsadda, Khyber Pakhtun Khwa (KPK), Pakistan. Besides, the authors of this paper are greatly thankful to the Vice-Chancellor of Abdul Wali Khan University, Professor Dr. Ahsan Ali for his support and craven for Research and Development. These driving forces have enabled Abdul Wali Khan University and Bacha Khan Universityas the leading Universities of the Pakistan in a short span of time.

## Authors Biography

**Mian Ahmad Jan**

I am Lecturer at the Department of Computer Science Abdul Wali Khan University, Mardan Pakistan. I have completed my Master degree in Mobile Computing from University of Bradford, United Kingdom in 2007. I am currently pursing my PhD Studies at University of Technology, Sydney Australia under Abdul Wali Khan University Overseas PhD Scholarship Programme. My area of Research is Wireless Sensor Network, Adhoc Network, Internet of Things, and IEEE 802.15.4 WPAN.

**Muhammad Khan**

I am Lecturer at the Department of Computer Science Bacha Khan University, Charsadda, Pakistan. I am currently pursuing my Master degree in Computer Science from Institute of Management Sciences, Peshawar. I am specifically interested in Wireless Sensor Network and Adhoc Network

## REFERENCES:

[1]. Akyildiz, I.F., Su W., Sankarasubramaniam Y., Cayirci, E.: Wireless sensor networks: a survey. Elsevier Computer Networks 38 (2002) pp. 393–422.
[2]. J. Yick et al., Wireless sensor network survey, Comput.Netw. (2008), doi:10.1016/j.comnet.2008.04.00
[3] Kirk Martinez, Jane K. Hart, and RoyanOng. "Environmental sensor networks" *IEEE Computer*, 37(8):50–56, 2004
[4] I. Johnstone, J. Nicholson, B. Shehazad, J. Slipp, Experiences from a Wireless Sensor Network deployment in a petroleum environment, in: IWCMC, Honolulu, Hawaii, 2007
[5] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai, K. Frampton, Sensor network-based counter sniper system, in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD, 2004
[6] P. Zhang, C.M. Sadler, S.A. Lyon, M. Martonosi, Hardware design experiences in Zebra Net, in: Proceedings of the SenSys'04, Baltimore, MD, 2004
[7] Zia. T, Zomaya, A.: "Security Issues in Wireless Sensor Networks", Proc.ICSNC 2006
[8]. C.P. Fleeger, Security in computing, 3rd edition, Prentice-Hall Inc. NJ. 2003
[9]. Wood,A.D, Stankovic , J.A: "Denial of Service in Sensor Networks", Proc. IEEE 2002. pp 54-62
[10].Newsome, J., Shi, E., Song, D.,Perrig, A.: "The Sybil Attack in Sensor Networks: Analysis & Defenses." Proc. ACM, *IPSN'04*, April 26–27, 2004.

[11]. Mohanty.P., Sangram. P., Sarma. N., Satapathy.S.S: "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Proc. Journal of Theoretical and Applied Information Technology, 2010.
[12] Sen, J.: "A Survey on Wireless Sensor Network Security", Proc. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009.