*VFAST Transactions on Software Engineering*
*http://vfast.org/journals/index.php/VTSE@ 2016 ISSN(e): 2309-3978;ISSN(p): 2411-6246*
*Volume 4, Number 1, January-December, 2016*

*pp. 76-89*

# MINIMIZING DENIAL OF SERVICE ATTACK FOR MULTIPLE BASE STATIONS IN WIRELESS SENSOR NETWORK

JAFFER WAZIR[1], OMAR BARUKAB[2], ALAA OMRAN ALMAGRABI[3]

[1]Department of Computer Science, Abdul Wali Khan University Mardan
Jafferwazir85@gmail.com
[2]Faculty of Computing and Information Technology, Department of Information Technology, King Abdul Aziz University, Rabigh 344, Saudi Arabia.
Obarukab@kau.edu.sa
[3]Faculty of Computing and Information Technology, Department of Information Systems, King Abdul Aziz University, Rabigh 344, Saudi Arabia.
aalmagrabi3@kau.edu.sa

Revised September 2016

ABSTRACT: *Wireless sensor network* (*WSN*) *is a network communication technology that is characterized by its small size; low power consumption and limited memory capacity. It provides communication in a broadcast manner. These sensor nodes have no specific infrastructure and they are placed randomly throughout the network. The use of WSNs is to collect data from physical environment and in real time. Error in the collected data or malfunctioning of the sensors can create problems on large scale. There are few ways and methods through which WSNs can be attacked. One of them is the Denial of Service Attack* (*DoS*), *which captures the nodes and takes its important data, modifies it or halt it from responding to a bona fide user. Various techniques are used to tackle DoS attack on WSNS. By using the multiple base station approach we can reduce and minimize the drastic effect of DoS attack on WSNs and makes our network secure and functioning in its normal conditions.*

**Keywords**: WSN, Layered architecture of WSN, NS2, Denial DoS, DDoS.

1. **Introduction.** Wireless sensor networks is a technology that is gaining growth rapidly. It consists of sensors and these sensors spread on Ad hoc manner in the wireless environment. These sensors are characterized by their small size, low power consumption and limited memory capacity. They provide communication in a broadcast manner. Nodes of WNS network are grouped for well monitoring to achieve reliable communication through redundancy. Every sensor has its specific range in which it can sends and receives messages as well as communicating with other nodes in its vicinity in the network. Wireless sensor network's nodes are cheap and cover a specific geographical area. The topology changed continuously, therefore they are often susceptible to a number of attacks, such as Denial of Service attack, Black hole attack etc. The dynamic nature of wireless sensor network makes it easy for Denial of Service attack to capture the network data during transmission [1].

The addition and removal of nodes means that WSN is subjected to attacks. The openness of WSNs makes it possible for the attacker to penetrate the network easily and makes it possible to launch the Denial of Service (DoS) attack. The purpose of DoS attack is to block all the available services provided for the legitimate users on the network by causing an enormous number of messages to be destined to the victim machine which lead to the blockage of its services it provides. Sometime such type of attack destroys the node on the network and captures important information of a compromised node. Symptoms of DoS can be notices as a delay in data delivery of packets destined from source to destination, wastages of the available bandwidth and a reduction in the battery life

of a node in WSN. The DoS attack can be minimized by using multiple base stations which tolerate the failure of the base station of nodes in the network [2].

Wireless sensor networks mainly face two categories of attacks: invasive and non-invasive types of attacks. Invasive attacks targets the services, transmission of data packets, and routing etc. Non-invasive attacks attempts on timing of WSN nodes, their frequency and channel's power. The DoS attacker tries to suspend the services and make them inaccessible for the legitimate user of WSN. There are different conditions of DoS attack on WSN according to the layer of the WSN [3]. Figure 1-a depicts a simple WSN architecture while Fig. 1-b shows an WSN that includes a base station. The structure of the paper is as follows. Section 2 presents the literature review. Section 3 discusses the layered architecture of the wireless sensor network. Section 4 shed the light on the denial-of-service attack while section 5 dealt with the distributed denial-of-service attack. Next, section 6, presents the defense strategies to mitigate the denial-of-service attack. Section 7 illustrates the simulation parameters used in this conducted study. Conclusion and future work is presented in section 8.

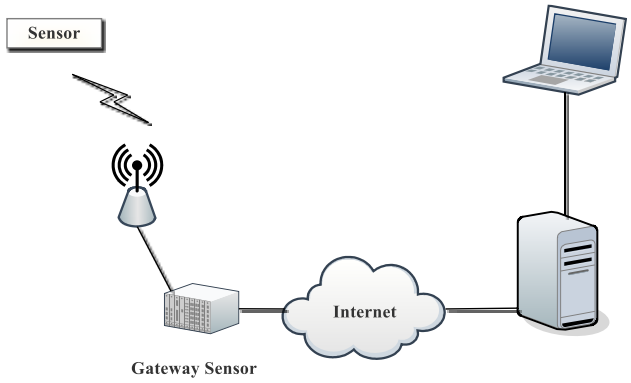


Figure 1-a: A simple WSN architecture.

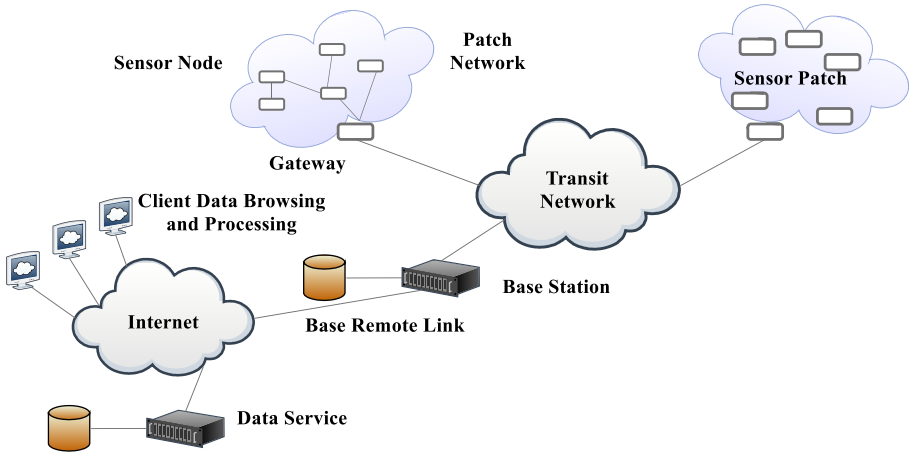


Figure 1-b: Base Station with WSNs.

**2. Literature Review.** Wireless Sensor Network is a technology that is widely used nowadays. Due to its mobility, it is widely used. It is less expensive compared to the traditional wired network. It is characterized by its

limited memory capacity and a very weak processing power. The security problem commonly faced by WSN is DoS attack. A very little task done in the prevention of DoS attack against WSN such as using cryptographic primitives and digital signature to mitigate the risk incurred by DoS [8].

The DoS attacker causes misdirection of packets which lead to a change in the routing information in the routing tables of the router and this leads to a reduction in the throughput and increase in the latency. In the case of WSN, the sensor nodes collect data and then send it towards the base station for processing. Due to the limited functionalities of WSN network, it is easily susceptible to access by the attacker. This halts the network resources from being accessed by a legitimate user. The DoS attack injects fallacy packets into the network which result in keeping the target node busy from functioning well. If the DoS attack is accomplished by a single agent, then it is called DoS attack, while if it is accomplished by multi agents then it is recognized as distributed denial-of-service attack (DDoS) [9]. Anthony D. Wood et al. [7] in their research work stated that DoS attack is very harmful for the wireless sensor networks, because it not only disrupting the communication between base stations but creates coordination problem among WSN nodes. The DoS attack affects the availability of the needy resources for the requesting node, and causes loss of energy of those nodes during data transmission. The DoS attack is very cheap and very hard to detect in the wireless sensor network. DoS attack affects the data in the network in different layers of the network ranging from physical, network and transport layer, etc . as a consequence, this may lead to jamming , tampering, collision, exhaustion , homing and flooding. Mitigating DoS attack ranges from authentication, node hiding and using redundant paths etc. L. Lilienet al. [10] analyzed that DoS attack can capture information from the networks in order to jeopardize the base station or the entire sensor network. because nodes will be visible for access by the DoS attacker. Measures against DoS attack can be classified as preventative and detective measures. In the case of preventative measures, one can employ cryptographic primitives, such as authentication , integrity and confidentiality for the users. Detective measures are based on monitoring the network while in its normal conditions and then being able to compare the network status when the DoS took place and then apply the counter measures required for the ramification of such attack. Deng et.al. [11] in their study focused on security of the wireless sensor networks to prevent the sensor nodes from being accessed by un bona fide users. A single node is not allowed to broadcast due to which DoS attacks (flooding) are prevented. Only base station is loosely authenticated through the using a one-way sequence number so that nodes will not be able to spoof the intended base station. Sensor nodes can unicast a packet only to the base station. The peer-to-peer sensor communication is not only directly supported; however the tunneling is accomplished through the base station that allows indirect sensor-to-sensor communication. To control routing information, the WSN needs authentication to prevent the false injection in the routing table of the sensor nodes. The symmetric key cryptography is used for confidentiality between a base station and a node instead of the computationally intensive public key cryptography technique due to the speed of the former one. Base station is in charge for the computation of the routing table to other peer base stations. Raymond et.al. [12] focused on the DoS sleeping attack. This is a special type of attack, which commonly focuses on the battery power of the sensor base station. If a number of nodes are working together for such type of attack, this will reduce the life time of the battery up to few days. The DoS attack creates problems not only for the sensor nodes but for the entire network. When it continuously sends packets to such a system, DoS attack shuts down the battery of the system, therefore the researchers attempting to protect the network from this attack. Zhou et.al. [13] analyzed that there are commonly two types of attacks on the network, passive and active. In the case of passive attack, the eavesdroppers tampers the communication channels and at the end the result shows that which type of data packets are transferred from source to destination. The attacker has the ability to listen to the channel while hiding its identity from the network administrator and silently gather data and modify the packet's content. In the case of active attack, the attacker exploits the protocol's security during the communication between nodes. This consumes and ultimately exhausts the limited power of the sensor nodes. These DoS attacks bring a great effect on the wireless sensor networks such as noticeable degradation of the performance that can be noticed by a legitimate user. At the physical layer, DoS attack can jam the network traffic and no signal can pass in the transmission medium because the straight forward nature of the wireless sensor network attacks are very effective. To defend against jamming and tampering of network signals, authentication and cryptographic algorithms are employed.

**3. Layer Architecture of WSN.** Wireless Sensor Network is using layered architecture as shown in Fig. 2. Each layer of the network with its characteristics and its associated functions is described briefly in this section as follows:

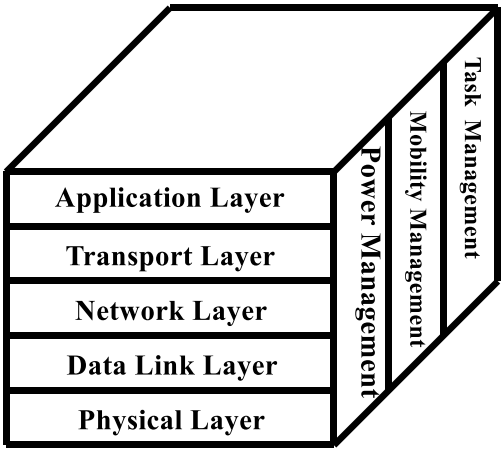


Figure 2: Layers of Wireless Sensor Network.

**3.1 Physical Layer:** The main aim of physical layer is to minimize the loss of path and to increase the reliability of the network. The physical layer has the capability to provide connectivity for data communication and increases the data rate of the link. It is also responsible for secure communication through using data encryption primitives. Physical layer is used for saving the bandwidth of the link and generating a specific frequency which provides a smooth communication between source and destination nodes.

**3.1.1 Data Link Layer:** Data link layer is commonly used for interoperability between nodes, error detection, and collision avoidance of packets during transmission. This layer is also responsible for security through using key distribution algorithm.

3.1.2 **Network Layer:** The main objective of the network layer is routing of packets. The data is transferred from source to base station, node-to-node, source-to-destination by using the shortest and best path for data routing. Therefore this layer has the ability to increase the battery's life. Wireless sensor networks use broadcast mechanism, but this layer secure the data by using safe (secure) routing.

3.1.3 **Transport Layer:** Transport layer facing a number of challenges in WSN because the network is communicating in open environment. The entire network is communicated with external world (internet).

3.1.4 **Application Layer**: This layer displays the last information, because application layer collects the data, manages and then process the data by using application software for reliable information [4].

**4. Denial of Service (DOS) Attack.** Denial-of-service attack (DoS) has a drastic impact on the availability of nodes in the network as well as it wastes various resources available in the same network. denial-of-service attack is hard to detect and it disables the target devices from responding to a legitimate user. It can interrupt and jam the radio signal. In addition, it can capture data packets and modifies them which may cause incorrect entries in the nodes' routing tables. As a consequence, this may lead to shutting down the whole wireless network [5]. Fig. 3 depicts a simple DoS attack mechanism.

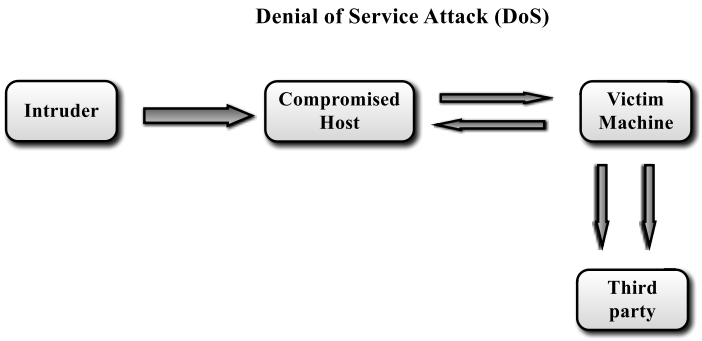


Figure 3 : Simple DoS Attack on WSN.

**4.1. DOS Attack on Different Network Layers.** Denial-of-service attack disrupts the network from being functioning in its normal conditions and this causes legitimate users deprived from accessing the available resources. Moreover, it consumes bandwidth, battery life and keep processors busy all the time. Table 1 shows the different types of DoS attacks on the WSN as well as the countermeasures to mitigate them.

Table 1: DoS attack on different layer and respective defense.

| Layer | DoS attack | Defense from attack |
|---|---|---|
| ***Physical layer*** | Jamming and tampering | Sleep the nodes and use tamper proof packages |
| ***Link layer*** | Denial of sleep | Authentication, anti replay and sleep |
| ***Network layer*** | Spoofing , homing, replaying and flooding | Authentication, routing, anti replay and header of the packet secure from attacker. |
| ***Transport layer*** | Flooding, and de synchronization | SYN cookies, and authentication |
| ***Application layer*** | Path based, and reprogramming | Authentication and anti replay |

**4.2. Physical Layer Attack**. In physical layer, the DoS attack uses jamming mechanism which jams the signals by wasting the power of a node and sending traffic randomly. It has the ability to jam the forwarded traffic of the medium towards the target node. In jamming attack the channel is occupied with unwanted signals due to which the authorized user cannot use these unwanted signals in the network. The WSN uses a classic limited spectrum which is easy for DoS attack to gain access to the wireless spectrum and jams it during data transmission on the network. The detection and sleeping mechanisms are commonly used mechanisms to defend such type of attack on the physical layer. Tampering is another type of attack on the physical layer of the network in which the target nodes are deployed into the unsecure areas where they face a number of difficulties on the network. To secure the network against the tempering attack, WSN uses tempering proof packaging and tamper reaction.

**4.3. DOS Attack on Link Layer.** The denial-of-service attack creates more collisions in the network and constantly sends request messages on the network to jam the node's link and reduces the battery life of the. This attack can be defended by using anti-reply and jamming detection. With authentication, the authorized node can be trust on the communication network and checked that the sending and receiving of packets is safe and secure.

**4.4. DOS Attack on Network Layer.** The DoS attack on the network layer halts the routing protocols between nodes from normally functioning by flooding various nodes of the network by generate a number of

hello packets which traverse the wrong hops on the WSN, and break down the network routes. This type of DoS attack can be mitigated through using pair wise authentication between different nodes. In the network layer attack, the attacker creates itself a cluster head node and captures a number of packets and drop them out of the network. Flooding is a network layer attack which commonly jeopardizes the communication resources and then hide away from the network. Figure 4 shows the network layer attack where in Fig. 4-a the service is flooded with many inputs which make the network not working properly while in Fig. 4-b an attacker catches all the data from the nodes then disappears from the network.

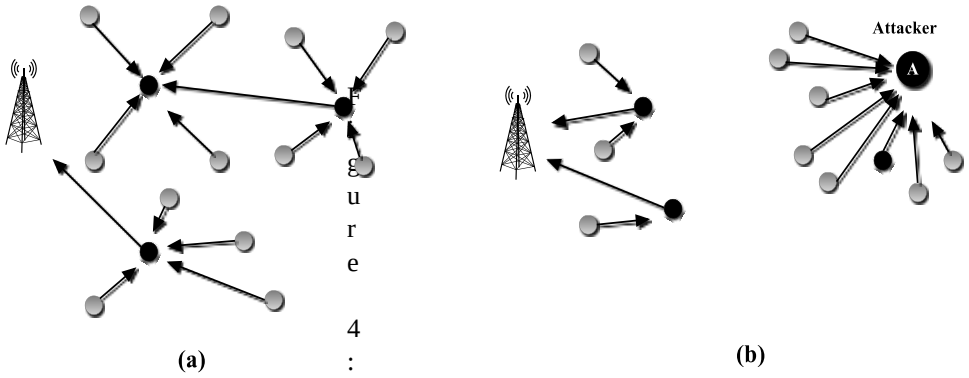


Figure 4. Network Layer Attack.

Homing is another type of attack on the network layer which analyzed the data traffic for cluster head node and shut down the entire network for communication process. This type of attack can be mitigated by using encryption techniques for the packet's header. Black hole is also a network layer attack which establishes a number of routes for data packets by sending and then dropping all those packets on the way. Black hole attack can be mitigated by using authentication and anti- reply mechanisms.

**4.5. Transport Layer Attack**. The most common DoS attack is the SYN flood attack which has the ability to use the Transport Control Protocol's three-way handshaking policy for generating flood in the network. In the transport layer the Transport Control Protocol (TCP) is responsible for end-to-end reliable connectivity, where it is a connection-oriented protocol. In wireless sensor network a number of connections are opened at the same time in which a buffer overflow is occurred which as a consequence leads to a flood in the network. Reducing flood attack from the transport layer is achieved by using SYN cookies. De-synchronization is also a transport layer attack which sends a number of malicious sequence numbers to destination nodes. This type of attack can be counter measured by using authentication mechanisms.

**4.6. Application Layer Attack.** In the case of application layer attack, a large number of stimuli packets are on the network and produce an immense amount of traffic. These stimuli can jeopardize all the applications from running on the network. This type of attack can be coutermeasured by using filter-data alerts. Reprogramming is another type of application layer attack which sends fallacy programs to a node. Reprogramming attack can be defended by dividing the whole program into modules and one module is a hash algorithm for the next program module and so on. Path-based DoS attack is also another application layer attack in which a node sends packets to the base station by using the entire possible routes towards the base station. Path- based attack wastes the link bandwidth and consumes greater amount of node energy and resources. The path-base DoS attack can be mitigated by using authentication and anti-replay messages between nodes. This attack hinged other nodes from sending data to the existing base station. Fig. 5 depicts the path-based DoS attack [7].

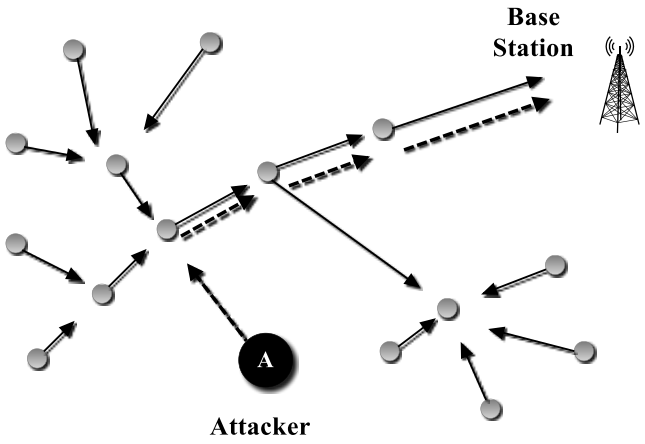


Figure 5: Path Based DoS Attack.

**5. Distributed Denial-of-Service Attack (DDOS).** Distributed denial-of-service attack (DDoS) holds network resources from being utilized and uses them in accordance to the attacker's intended plans. When DDoS attack occurs, a network user or a node is denied from accessing the available resources. It has the ability to control thousands of computers (zombies) on the network and be able to conduct this type of intended attack through these machines. Distributed denial-of-service attack has the capability of generating enormous amount of traffic on the network and affects multiple resources. Figure 6 shows DDOS attach on WSN.

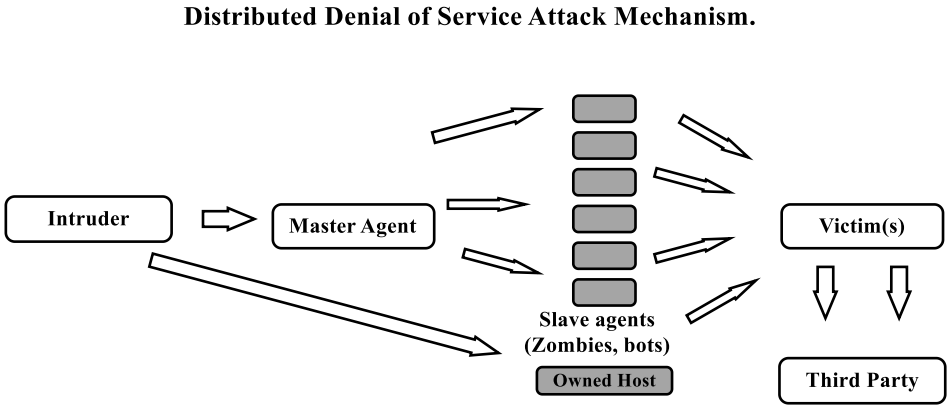


Figure 6 : DDoS Attack on WSN.

In the DDoS attack a large number of zombie machines are used in attacking one or more target machines. The DDoS attack uses the client-server architecture to launch the attack. The DDoS attacker installs a master program on a computer of stolen account, this master program has specific time in which it has the ability to communicate with any number of agent machines to trigger them to initiate the attack. These machines are called slave agents or zombie machines. The master program has the ability to initiate thousands of agent programs in a very short period of time in order to launch the attack. Some popular agent programs are Trinoo, Tribe Flood Network, TFN2K, stacheldraht (barbed wire) etc [6].

In the DDoS attack, the nodes are divided into a number of categories such as attacker node, master nodes, slave agents, and victim node.

Attacker node works like administrator for the attacker nodes, it issues a number of commands to the master nodes. The master node then sends the instructions to the slave agents to execute the commands according to the attacker's instructions. Slave agents are controlled by the master nodes and these nodes execute the commands

for the attacker on the network and at last the victim's node is jeopardized from being functioning well by several hosts on the network during communication.

## 6. Defense Strategies Against DOS in WSN

Wireless sensor networks are commonly protected against the DoS attack by using authentication and identification mechanisms. Recently, the following mechanisms are often in used to defend the WSN from the DoS attack which are:

a) ***Watchdog scheme*:** This scheme works with two ways to defend against the DoS attack. Firstly, it has the ability to monitor constantly forwarded packets of the neighbor nodes on the network. Secondly, it provides path rater facility for reliable transmission and covers all the alternative routes toward the destination, but this scheme is only used for source routing protocol, and ignore the general routing protocols.

b) ***Rating scheme***: According to this scheme, the neighbors of any single node on the network collaborate. It shows that how the function is executed for the rating but this is very rarely used.

c) ***Virtual currency***: This scheme introduces selfish node on the network which is also called nuglet. This selfish node captures all the information running on the network by the attacker during communication. The disadvantage of virtual currency scheme is that it cannot prevent malicious flooding on the network.

d) ***Route DoS prevention***: In this mechanism the DoS attack is defended in the routing layer by cooperating a of number of nodes.

**7. Simulation Parameters.** In this study the simulation area of the network is chosen to be 2500 m x 2500 m and the wireless medium is used. The number of nodes in the wireless sensor network is 200 sensors and the access points are the base stations for data monitoring and controlling. The bandwidth used for this simulation is 2 Mbps, and the packet's size is 128 bytes. There are a number of simulation topologies that were randomly created in search for the sake of finding the optimum results. Table 2 shows the simulation parameters of interest while Fig. 7 depicts a screenshot of the simulation environment used under NS2 simulator [14].

Table 2 : Simulation Parameters.

| No. of Stations | PARAMTER | SPECIFICATIONS |
|---|---|---|
| 1 | Access point | Base station |
| 2 | Medium | Wireless networking |
| 3 | Area of network | 25000 m x2500 m |
| 4 | Number of nodes | 200 |
| 5 | Type of traffic | CBR(constant bit rate) |
| 6 | Bandwidth | 2 Mbps |
| 7 | Simulation time | 100 seconds |
| 8 | Packet size | 128 bytes |
| 9 | Speed (data rate) | 32 bits/sc |
| 10 | Antenna | Two way |
| 11 | Number of attacker | One |

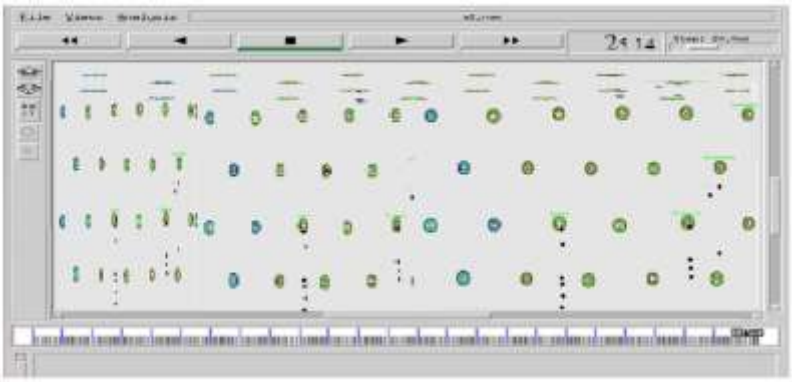

Figure 7: Simulation Environment.

**7.1. Securty of the Base Station.** The wireless sensor network consists of gateways which are also called the base stations of the network. These base stations have the ability of providing powerful computation, high storage capacity and long life as compared to other nodes on the network. The base stations are used in both types of networks (wired and wireless network). A base station may be a computer or powerful mobile device that provides connectivity for the entire network to the Internet. There are three strategies that are shown in Fig. 8, which show that how to secure sensor network against base station failures. These strategies are as follows:

- In part (a) of the figure, the source node designated by the letter S sends data packets to two base stations using multipath. The first path is toward the base station B1 and the other one to the base station B2. This mechanism is used for both route discovery and data routing phases. If the number of base stations is increased then this will enhance the resiliency of the network.
- Part (b) shows that the address and identification fields of the header are commonly used by the attacker for finding the location of the base station and thereby introducing threats from the passive attack observer's point of view who is trying to eavesdrop the source and the destination node headers to find the location of the base station.
- Part (c), focuses on the relocation of the base station in the network and tries to analyze the traffic to the point where the base station reveals its mobility status to the attacker.

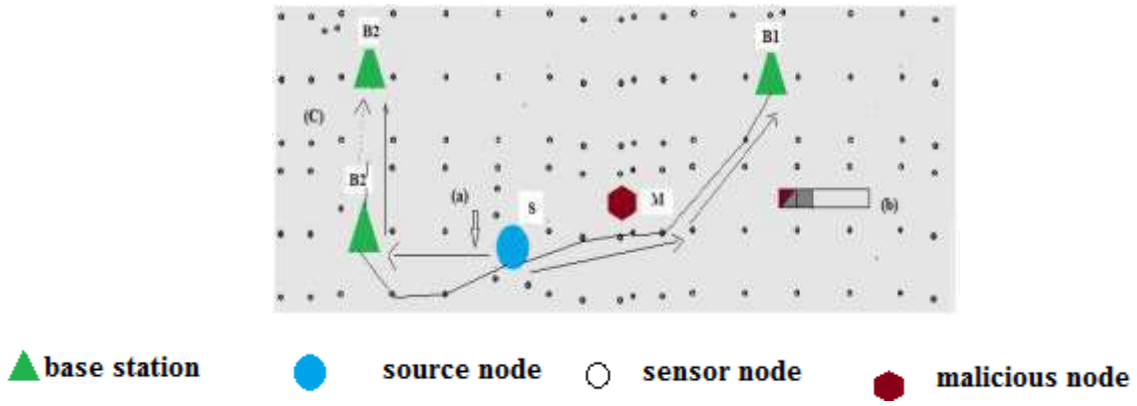


Figure 8: Multi Base Stations.

**7.2. Erformace of Route Discovery**. There are two types of attacks mainly occur in WSN: passive and active attack.

- In passive attack, the attacker captures the feedback messages and dropped them from the routing path or modify them which causes changes in the routes or neighbor information of nodes. Due to this passive attack on the network the legitimate nodes will not be able to provide their correct information to the base stations and where some nodes are disappeared from the network. This will create problems in the network topologies.
- Active attack, the malicious nodes lunch their attack on the feedback messages which are received by base stations from different nodes on the network. Figures 9 and 10 show the results of both passive and active attacks on the wireless sensor network. The horizontal axis illustrates that the number of malicious nodes in the network while the vertical axis displays the number of nodes which are compromised by a single attacking node. Active DoS attack disconnected only 8 nodes while 39% nodes are functioning properly, if there are three base stations used for monitoring the nodes. In passive attack this damage is found by calculating all the nodes which are downstream from the malicious nodes that cannot be connected with the respective base station, but in active attack calculation of damage is displayed by counting the downstream malicious neighboring nodes, and downstream of the neighbor nodes which cannot get hold by any base station on the network.

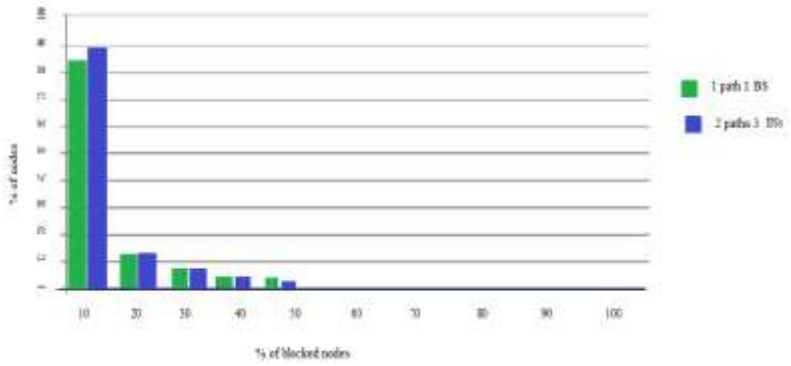


Figure 9: Results of Passive Attack.

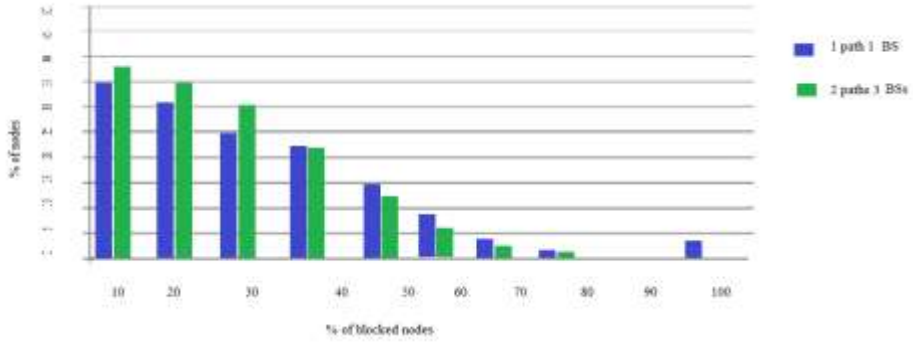


Figure 10 : Results of Active DoS Attack.

According to the above figures there are a number of observations, such as active attack jeopardizes more nodes from functioning in the normal conditions as compared to the passive attack, and the multi-base stations have the capability that improve the resiliency of wireless sensor network protocols from both active and passive attacks. In the case of single base station the malicious nodes have the ability to block a number of nodes and affect the

communication process. When the number of base stations are increased then the malicious node will not be able to have enough power to blockage the nodes from every base station in the network. According to the two figures above, there is a catastrophic scenario when there is only one base station in the network, because some nodes in the entire network were working down the network and such nodes are not basically part of the network, which actually causes the DoS attack to take place. When a network consists of multi-base stations, then the DoS attack will b e reduced to a peak point because multi-base stations helps to provide fault-tolerance that will help in avoiding this catastrophic scenario from being executed on the network.

**7.3. Performance of Multi Paths Lunching DOS Attack.** The Figure 11 show that the damage of malicious may cause DoS attack. We have noticed that malicious nodes can send packets continuously to block their neighbors but with multiple base station the results shows that DoS attack can be reduced if the random topology is used. The total number of nodes used in this simulation study is 200. The following scenario displays five different outputs. The x-axis of the Figure 11 shows that the percentage of blocked nodes using a single malicious node by lunching DoS attacks while the y-axis displays the percentage of malicious nodes in the network. Some observations can be drawn from the figure such as: multi- base station with multiple redundant paths can provide greater resiliency against DoS attack. The second observation shows that a multi-redundant paths provide more security that of a single path.

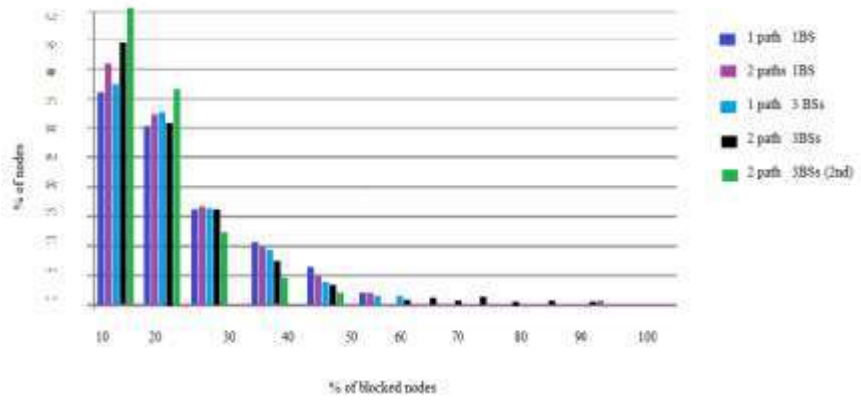


Figure 11 : DOS Attack on WSN.

In a single base station scenario there is a chance that the number of malicious nodes can shut down the entire network, and these nodes are in the vicinity of the base station and if they are left as such, they can launch DoS attack. In WSN such type of compromised nodes become the source for DoS attack. In the case of multiple base stations network, it is apparent that the network performs better.

**7.4. Failure of Base Station.** Multiple base stations provide a number of merits to the network such as if one base station failed, the network can tolerate the failure of such base station failure. For example if nodes are not able to reach to any base station in a network, it results that one or more base station are failed. According to Fig.12 as shown below, there are five base stations in the network that are using two redundant paths. There are four different scenarios such as 2, 3, 4and 5 base stations respectively which provide two vital observations. In the first observation, there are multiple paths using multiple base stations which provide strong resiliency to the network downstream. When the failure occurs in one base station, the other two base stations will take over causing only 22 nodes to be disconnected from the network.

In the second approach, if there are number of base stations in a network and failure occurs in one base station then these base stations have the ability to provide high resiliency. In the case of five base stations in the network, only one node is disconnected. Using the same method if four stations are failed

in the network, more than half of the nodes will have connectivity in the network. It means that the numbers of base stations contribute to supporting network's resiliency automatically.

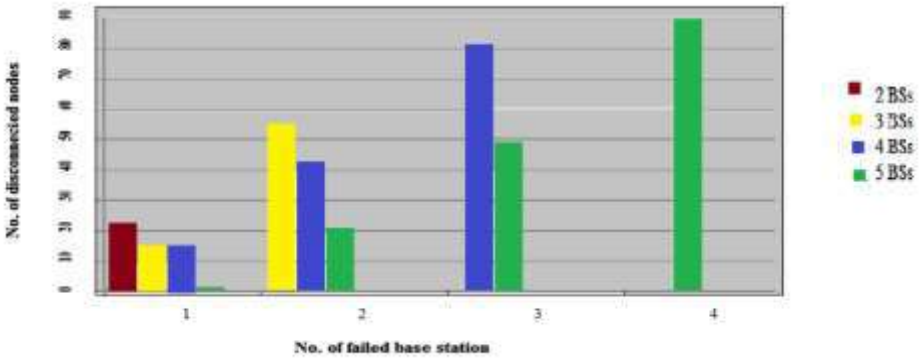


Figure 12: Impact of Failure of a base station.

When the number of base stations is greater in numbers then it will have the ability to minimize the DoS attack in a wireless sensor network. According to the results depicted in table 3 below, in the first scenario the number of connected stations are four and only one station failed due to which a very few (22) nodes are disconnected while a greater number of nodes are providing services to other nodes. In the second scenario, two stations are failed due to which the number of disconnected nodes reaches up to slightly high numbers as compared to first scenario. It means that when the number of base station failure increases, it follows that the number of disconnected nodes is also increases.

Table 3 : Number of Stations and Disconnected Nodes During DoS Attack.

| **No. of base stations** | **Number failed BS** | **Number of (Max) Disconnected nodes** |
|---|---|---|
| 1 | One base station | 22 nodes |
| 2 | Two base stations | 54 nodes |
| 3 | Three base stations | 81 nodes |
| 4 | Four base stations | 90 Odes |

**7.5. Scalability of Base Station.** The performance of the WSN is basically depends on the number of base stations in the network. If the number of base stations are increased in number, then the performance and security are automatically improved. Using the same simulator, a number of experiments were conducted and it is observed that if the number of base stations are increased, then the average number of blocked (disconnected) nodes are decrease. Figure 13 shows that if the number of base stations are increased in network, then it follows that the average of blocked nodes is decreased.

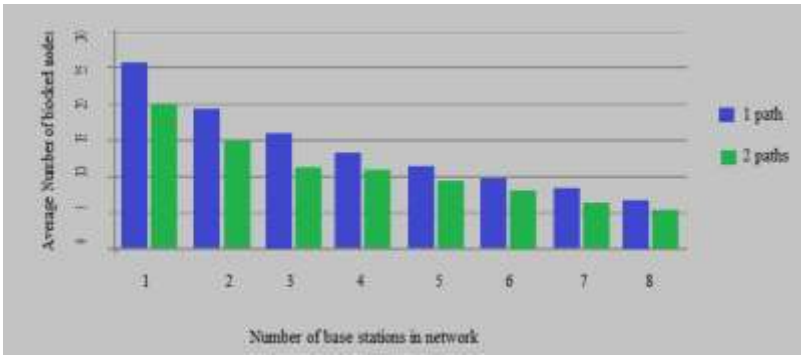


Figure 13 : Scalability of Base Station in WSN.

For 200 nodes in the scenario, there will be eight base stations providing significant results when using two redundant paths. In the above figure the average blocked nodes are decreased with time and it is also depends upon the number of the available routing paths. Table 4 below shows that if the numbers of base stations are increased then the number of blocked nodes in the network are decreased in both single and two paths in the network.

Table 4 : Minimizing the DoS Attack By Multiple Base Stations.

| No. of Stations | Average blocked node in 1 path | Average blocked nodes in 2 paths |
|---|---|---|
| 1 | 26 | 19 |
| 2 | 20 | 17 |
| 3 | 16 | 12 |
| 4 | 13 | 11 |
| 5 | 12 | 9 |
| 6 | 11 | 8 |
| 7 | 9 | 7 |
| 8 | 8 | 5 |

## 8. Conclusion and Future work

Wireless sensor networks is commonly used technology today. Similar to wired network, wireless sensor networks are susceptible to denial-of-service (DoS) as well as Distributed Denial-of-Service attacks DDoS. This paper dealt with the minimization as well as mitigation of Denial-of-Service attack in wireless sensor networks. A technique of multiple base stations is employed to defend against such kind of attacks. The NS2 simulation environment is used to curry-out the simulation process. A 2500m × 2500 m working area is chosen augment ted with 200 nodes. Packet size was selected to be 128 Bytes. The bandwidth used was 2 Mbps. The use of multiple base stations helps in enhancing the performance of the WSN and its resiliency against DoS and DDoS attacks. As a consequence security is improved by using cryptographic primitives and authentication which leads to keeping the pillars of network security in place which are confidentiality, integrity and availability of the functioning network. This can be demonstrated by the above obtained results. Future work will include the usage of Fault-tree analysis in

analyzing and studying WSNs such as in [15]. Further study will investigate the effect of changing different parameters of interest in order to provision the proper way to deal with the DoS and DDoS attacks on WSNs. In addition, clustering and segmentation of nodes based on their importance in computation and how to protect them will be another area of investigation where nodes can be self-organized to minimize such type of attacks. This will include the development of different types of protocols to deals with this type of WSN environments.

## REFERENCES


[1]. Alazemi, A. R. (2013). Defending WSNs against jamming attacks. *American Journal of Networks and Communications*, *2*(2), 28-39.

[2]. Kumar, S et. al. (2013). Mitigate the Impact of DoS Attack by Verifying Packet Structure, International Journal of Advanced Research in Computer Science and Software Engineering. 3(8): 289-294.

[3]. Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. *IJRET: International Journal of Research in Engineering and Technology*, *3*, 2319-1163

[4]. Pandey, A., & Tripathi, R. C. (2010). A survey on wireless sensor networks security. *International Journal of Computer Applications*, *3*(2), 43-49.

[5]. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2), 293-315.

[6]. Dittrich, D. (1999). The DoS Project's 'trinoo'distributed denial of service attack tool.

[7]. Wood, A. D., & Stankovic, J. A. (2004). A taxonomy for denial-of-service attacks in wireless sensor networks. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, 739-763.

[8]. Di Francesco, M., Das, S. K., & Anastasi, G. (2011). Data collection in wireless sensor networks with mobile elements: A survey. *ACM Transactions on Sensor Networks (TOSN)*, *8*(1), 7.

[9]. Sher, A. (2015). *Simulation of Attacks in a Wireless Sensor Network using NS2* (Doctoral dissertation, Texas A&M University-Corpus Christi).

[10]. Lilien, L., Kamal, Z. H., Bhuse, V., & Gupta, A. (2006). Opportunistic networks: the concept and research challenges in privacy and security. *Proc. of the WSPWN*, 134-147.

[11]. Deng, J., Han, R., & Mishra, S. (2003). A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *Information Processing in Sensor Networks* (pp. 349-364). Springer Berlin Heidelberg.

[12]. Raymond, D. R., Marchany, R. C., Brownfield, M. I., & Midkiff, S. F. (2009). Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE transactions on vehicular technology*, *58*(1), 367-380.

[13]. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE network*, *13*(6), 24-30.

[14]. NS2 Web Site. (2015, March 1) NS2. Retrieved From NS2 website: http://www.isi.edu/nsnam/ns.

[15]. Rushdi, A. M., & Ba-Rukab, O. M. (2005). Fault-tree modeling of computer system security. *International Journal of Computer Mathematics*, *82*(7), 805-819.