
ACADEMY JOURNAL OF SCIENCE AND ENGINEERING
Available online @ www.academyjsekad.edu.ng
AJSE 16 (1) 2022
Original Research

Prevention Technique against Denial of Sleep Attack in Wireless Sensor Networks

[1] Saidu, I.R., [2]Shu'aibu, M. and [3]Hamman, G.E.

[1]Department of Cyber Security, Faculty of Military Science and Interdisciplinary Studies, Nigerian Defence Academy, Kaduna, Nigeria

[2]Department of Computer Science, CST, Kaduna Polytechnic, Kaduna, Nigeria

Abstract

Wireless sensor networks are unique sort of network in which mobile nodes are linked together via wireless interfaces to form a network. They don't require permanent infrastructure, because of the increased mobility of the nodes and the dynamic architecture of the Wireless sensor networks (WSN), the energy (power) of the nodes is a major concern. There are many factors which effect the proper functioning of a Wireless sensor networks but that of the attacker is fundamental because they intrude the network and attack a victim node and deplete the battery of such node which affect the performance of the network in the long run. Usually, sensor node transit to standby mode from time to time due to the Adaptive Time-out of the protocol but when such node could not enter into sleep mode, it is termed sleep deprivation or Denial of Sleep Attack. This study mitigate this attack using an algorithm at the Network Organization stage of the Wireless sensor networks which hinders intruder from penetrating into the network. Simulation was utilized to assess the algorithm's performance on a node, and the simulator was OMNET ++. The results suggest that the proposed strategy can decrease the consequences of Denial of sleep attacks in Wireless sensor networks.

Keywords: Denial of Sleep Attack; Network Organization Algorithms; Sink Node; Wireless Sensor Networks.

1. INTRODUCTION

Wireless sensor network belong to the family of ad hoc networks and it inherits the characteristics of ad hoc networks according to Bhattasali and Chaki, (2011). The sensor nodes face security difficulties due to the nature of the wireless environment. Intruders may gain access to the network and interrupt its usual operation (Boubiche and Bilami, 2012). Nodes normally carry energy-saving

Corresponding author's e-mail: jesani@nda.edu.ng

mechanisms which allow them to switch to standby (sleep) mode regularly. However, malicious node can join the network and prevent nodes wishing to enter standby mode from turning off their radio. This can be considered as sleep deprivation torture, also called Denial of sleep attacks. It is performed by convincing the victim node that data is being transferred or that it only needs to stay awake for monitoring purposes. Much overhead is generated as a result which leads to poor performance (Gelenbe and Kadioglu, 2018).

1.1 Background to the Study

Wireless Sensor Network (WSN), is a collection of so many dispersed nodes connected to one or more sensors, which examine a large physical environment. The nodes (wireless devices) are typically undersized and capable of performing sensing, on-board processing, communication and storage (Fotoli and Bari, 2020). Chan et al. (2003) WSNs provide cost-effective solutions for a variety of applications, including current monitoring of plant instruments, pollution levels, freeway traffic, and building structural integrity. Climate sensing and control in business buildings, as well as home environmental sensing systems for temperature, light, moisture, and motion, are some of the other applications. According to Dargie and Poellabauer (2011), the development of wireless sensor networks stemmed primarily from military applications such as battlefield monitoring. The Distributed Sensor Nets Workshop was held in 1978 by the Defense Advanced Research Projects Agency (DARPA), and it focused on sensor network research issues such as networking technologies, signal processing approaches, and distributed algorithms. (Farooq et al., 2014). In the early 1980s, DARPA also ran the Distributed Sensor Networks (DSN) initiative, which was followed by the Sensor Information Technology (SensIT) program. WSN is currently regarded as one of the most essential technologies for the twenty-first century (21 Ideas for the Twenty-First Century). WSN is becoming a more common place and can be found in research projects and civilian applications as well as defence projects. The sensor nodes are often deployed to remote and inaccessible areas and thereby increase their exposure to malicious intrusions and attacks (Brownfield et al., 2005). WSN is therefore faced with several security challenges when deployed to remote areas. One of the most challenging security threats is a Denial of Service Attack (DoS) which is the result of any action that prevents any part of a WSN from performing correctly and in a timely manner (Wood and Stankovic, 2002). It can be seen as a malevolent attempt to make network resource unavailable to genuine users, thus is considered one of the most general and dangerous attacks endangering network security. Desnitsky et al., (2018), Desnitsky et al., (2019), it was discovered from practice that attacker required minimum basic technical knowledge, tools and resources to carry out depletion attacks which they are effective on. The attacker can deplete the device's energy entirely and rapidly, causing the attacked device to become completely disabled. The Wireless Sensor Network sensor nodes are normally strengthen with the help of the batteries even with that it still suffer energy depletion (Gunasekaran and

Periakaruppan, 2017). This is caused due to collisions, overhearing, idle listening and control packet overhead.

2. Sensing is simply an art used for obtaining information about a physical object or process such as changes in temperature, pressure and so on. Any object that can perform this very task is called a Sensor. When several sensors jointly observe large physical environments, they form what is known as a Wireless Sensor Network (Dargie and Poellabauer, 2011), Samir, A., (Djallel and Azeddine, 2013).. The sensor nodes communicate with centralized control called base stations, which is also refer to as a sink nodes. A base station normally allows transmission of information to another network, a powerful data processing or storage centre, or an access point for human interface. According to Chaudhari and Kadam, (2011) communication with the base station could either be single-hop, where the nodes transmit data directly to the base station or multi-hop, where some nodes operate as relays for other sensor nodes, assisting in the transmission of sensor data to the base station. In WSN, the level of expertise in sensor processing and communication varies. Depending on their configurations, some may be classified as simple nodes, while others may be classified as complicated nodes. (Chen et al., (2009). Data dissemination (sending data/queries from sinks to sensor nodes) and data collection are the two most important functions of a WSN (send sensed data from sensor nodes to the sinks). In a sensor network, the architecture can be either flat, where each node performs the same sensing duty and there is no global identification, or hierarchical, where each node performs different sensing tasks and there is a global identifier. (Li et al., 2007).

1.2 Problem

WSNs rely heavily on Media Access Control (MAC) protocols for energy efficiency, especially because these networks include resource-constrained devices that are largely powered by batteries. The radio is the primary source of energy consumption in these devices, and the MAC layer regulates radio access. As a result, one of the ways that MAC protocols save energy is by putting nodes to sleep when they are idle and only waking them up when they need to transmit or receive data but intruders invade the MAC protocols by observing the adaptive timeout (TA) of the protocol and send meaningless control traffic and constrain affect node from entering standby mode thereby depleting the energy of the node which in the long term affect the overall performance of the network.

1.3 Aim and Objective

The aim is to develop a technique for detecting, mitigating and isolating intrusion which occurs at the MAC protocol of the Data Link layer in wireless sensor network in an efficient way.

The objectives are to:

i. Develop a model that will address energy depletion in WSN.

ii. Evaluate the efficiency of the model in order to determine its accuracy in detecting intruders in the network.

1.4 Organization of the paper

This work is structured in the following ways. Section 1 talks about the introduction, problem and aim of the work. In Section 2 related works are cited. Section 3 deals with the method used in achieving the set objectives. Section 4 provides the suggested Network Organization technique. The parameters for evaluating the performance are studied and simulation outcomes were discussed. Section 5 outlined the conclusion and future work.

2. Related Works

2.1 General literature

It is important to highlight that while there are a variety of approaches to preventing these assaults in the context of DoSL, most of them are strategies that do not consider energy efficiency, and even when they do, throughput becomes a trade-off that could be counter-productive in the long term (Hsueh, et al., 2015). External and internal attacks are the two types of attacks that can be classified according to Kalnoor and Agarkhed (2018), Shakhov et al., (2017).

i. External attacks: These attacks are usually initiated by nodes outside the logical network. The nodes do not have internal information such as cryptographic information about the network.

ii. Internal attacks: These assaults are carried out by either compromised sensor nodes running malicious code or adversaries who have stolen the crucial material, code, and data from genuine nodes and then attack the network with one or more laptop-class devices.

A study from Cakiroglu et al., (2006) and Raymond et al., (2009).show that in Jamming (attacks in which malicious nodes block legitimate communication by causing intentional interference in networks), the radio frequencies used by the sensor nodes are interfered in this type of attack. The entire network or just a portion of the network could be disrupted in this attack depending on the power of the jamming nodes around the network. Attacking just a portion of the network is enough to bring down the whole network. Jamming could be initiated in various ways, Reactive jammer constantly check the medium and send multiple RTS/CTS or data packets if the medium is found to be busy. Random jammers switch between sleep and active state thereby reducing their power dissipation. Constant jammers on the other hand send packets repeatedly without delay once the medium is available. Deceptive jammers send out multiple legal Request To Send (RTS) packets so as to always receive Clear To Send (CTS) packets from the nodes thereby exhausting the energy of the legal nodes.

The Data link layer is divided into the MAC layer and Link layer. WSN MAC protocols are designed to establish cooperation between the nodes to use the communication medium making them particularly vulnerable to DoSL attacks. These protocols, on the other hand, work at the link layer. When the radio transmits frames and listens to the channel, the link layer decides. The MAC protocol is in charge of controlling the sensor's radio, which is the primary source of power consumption. The transceiver

consumes more energy. (Raymond and Midkiff, 2008).

In collision attack, the attacker node, known as the jammer, continuously checks the communication channel to know if the channel is busy. If found busy, the jammer assumes that some packets such as RTS, CTS or data packets are in the medium and thereafter sends some jamming packets to collide with the real packets. This could prevent receivers from getting the expected number of packets after sending out CTS to the sender (Bhullar et al., 2016).

An ideal jam should have a high energy efficiency, a low chance of discovery, and the ability to interrupt communications to the intended or maximum extent achievable. For example, the jammer can use strategies that are consistent with MAC layer behaviours to maintain a low probability of detection. This attack however consumes less energy of the attacker but causes disruptions to the operation of the network, (Pelechrinis et al., 2011), (Bhattasali et al., (2012).

2.2 Review of the Anchor papers

Fotoli and Bari, (2020) proposed and Algorithms using Firefly and Hopfield Neural Networks (HNN) Algorithms, a novel countermeasure technique to protect WSN against Denial of Sleep Attacks, the algorithms combine Firefly, Hopfield Neural Networks (HNN), and RSA optimization techniques, a DoSA-immune schema was proposed. The proposed WSN-FAHN is made up of nodes that are spread at random. The network has a multi-channel mobile sink and n primary energy sensor nodes. Members of the cluster communicate with CH in a single hop. Furthermore, each CH only has to speak with the sink once. The transmission radius of nodes can be adjusted. The network activity cycle is also separated into multiple rounds. The sleep cycle of the sensors are arranged by using S-MAC protocol in sensor networks. S-MAC protocols work by sending synchronize signals to set the sleep cycle of the nodes. These protocols work with using control messages such as Request to Sent(RTS) and Clear to Send (CTS) that are known as synchronization packets. Repeating control packets as RTS message is one of the effective ways to prevent sleep deprivation attack. This cause the nodes not to fall to sleep. Therefore, their power loses. When these messages are sent over a short period of time, network nodes will not have enough opportunity to go to sleep mode and come back again. This leads to lose of battery power, this lose can occur for all nodes at attackers transmission time. Naika and Shekokarb (2015), Conservation of energy in wireless sensor network by preventing denial of sleep attack, in their approach they use a base station with clusters and each cluster has a cluster head and the attack was implemented on SMAC protocol, the attack approach was replay attack using Selective Local Authentication for detection of denial of sleep attack; hashing and interlock protocol was used for key exchange and Zero Knowledge for authentication of base node. Gunasekaran and Periakaruppan, (2017) GA – DoSLD: Genetic Algorithm Based Denial-of-Sleep Attack Detection in WSN. Proposed an Algorithm for generating DoSL attack profiles from multiple sensor nodes such that the attacker nodes can be prevented from the communication process. They simulated the WSN with 100 numbers of static sensor nodes; then the BS performs the operations

such as key pair generation and behaviour monitoring in parallel. The base station monitors the behaviour of the sensor nodes and initializes every behaviour as a chromosome. The MRSA algorithm was implemented in the base station for generating and distributing the key pair among the sensor nodes. Before initiating the communication between the sensor nodes, the AODV routing protocol estimates the optimal route. To validate the trustworthiness of the relay nodes in the route, the fitness value is estimated for every chromosome. If the chromosome is determined as unusual, it is validated against the existing attack profiles. If there does not exist a match, the pair of chromosomes is subjected to the crossover and mutation operations. The resultant chromosomes are added to the existing chromosomes. Finally, the BS determines the attacker nodes broadcasting the blocked information to all the sensor nodes in the network.

Desnitsky et al., (2019) in their work, Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems they developed a special software for Arduino platform based legitimate nodes. The task of such firmware (sketches) is to ensure correct reading of GPS data, their timely sending according to the model of normal network operation. A sketch for the attacking node has been written also, to model the normal operation of the network and the messaging process, the software of one of the legitimate nodes was modified. In addition to a standard option of the sending messages with GPS coordinates on some nodes request with a text message "GPS", the messaging between the attacking module and the potential victim node is also modelled. Packets are sent in bunches, i.e. in a sequence of a specified number of messages with a specified time intervals (interval inside bunches and interval between bunches). The variability of the modelled normal traffic is provided by using parameters, taking into account some maximum possible deviation defined on the basis of a random number sensor.

2.3 Research Gap

From the literature reviewed they established authentication method on the SMAC and TMAC, but there was still energy consumption in the long run because all the nodes are active during the network organization and when an intruder is sensed, the node need to be trace down to the root as a result much overhead is generated.

3. Methodology

To prevent all nodes from sending information to the Base Station, we adopt the network Organization approach so that each node stores the identification of its parent (the node it can send data to) and the identification of child nodes (nodes one hop away that it can receive data from).

During the network organization stage, a node can transit to sleep mode upon receipt of Hello Response from all child nodes and when the network organization is completed, all nodes wake up to begin synchronization.

The algorithm was developed and implemented using simulation frameworks such as OMNeT++ to provide experimental analysis on the behaviour of the nodes.

To minimize the rate of energy consumption while trying to organize the network, the

algorithm is design such that the nodes can transit to sleep mode once Hello packet has been sent and Hello Response packet received. With this, the rate of energy consumption was reduced. An attack is suspected if a node receives a SYNC packet from node(s) not listed as its child, then the packet is simply discarded. the Network Organization algorithm is presented below.

Steps (Network Organization):

i. The Base-station (Sink) broadcasts Hello Packets with ID and RSSI value

ii. Node a hop away from the sink receives packets and replies with Hello Response with its ID and RSSI value, and thereafter broadcasts Hello Packet with its ID.

iii. The Node which receives Hello Packet includes the sender as its parent only if it has no parent.

iv. The node updates its child list on the arrival of hello Response packet.

v. The node(s) then transits to sleep after receiving hello response packet.

Algorithm: Network Organization

```
BEGIN:
        HELLO ⇐ generate Packet with ID
        Broadcast HELLO Pack ⇐ Wait for Packet from the Network ();
        IF Pack is HELLO {
                IF Parent==NULL {
                        Parent= ID in HELLO
                        HELLO_RES⇐create Response packet with ID
                        Send HELLO_RES to Parent
                }
        }
        ELSE Pack is HELLO_RES {
                Child list⇐{ID in the Hello_Res}
               Go to sleep and wake up after network organization
       }
        END IF
END
```

After the network organization is over, the synchronization phase for the MAC protocol is initiated. Only valid nodes are able to synchronize with neighbours. Then, network is built in a tree-like structure as shown in Figure 3.1.

From Figure 3.1, the Sink Node (Base station) broadcast hello packet to all the child

nodes that are one hop way from it, and wait for response from all the child nodes, the same child nodes after responding to the parent broadcast hello packet to all the nodes that are one hop away from it and the process continue until all the nodes in the network are included and connected.

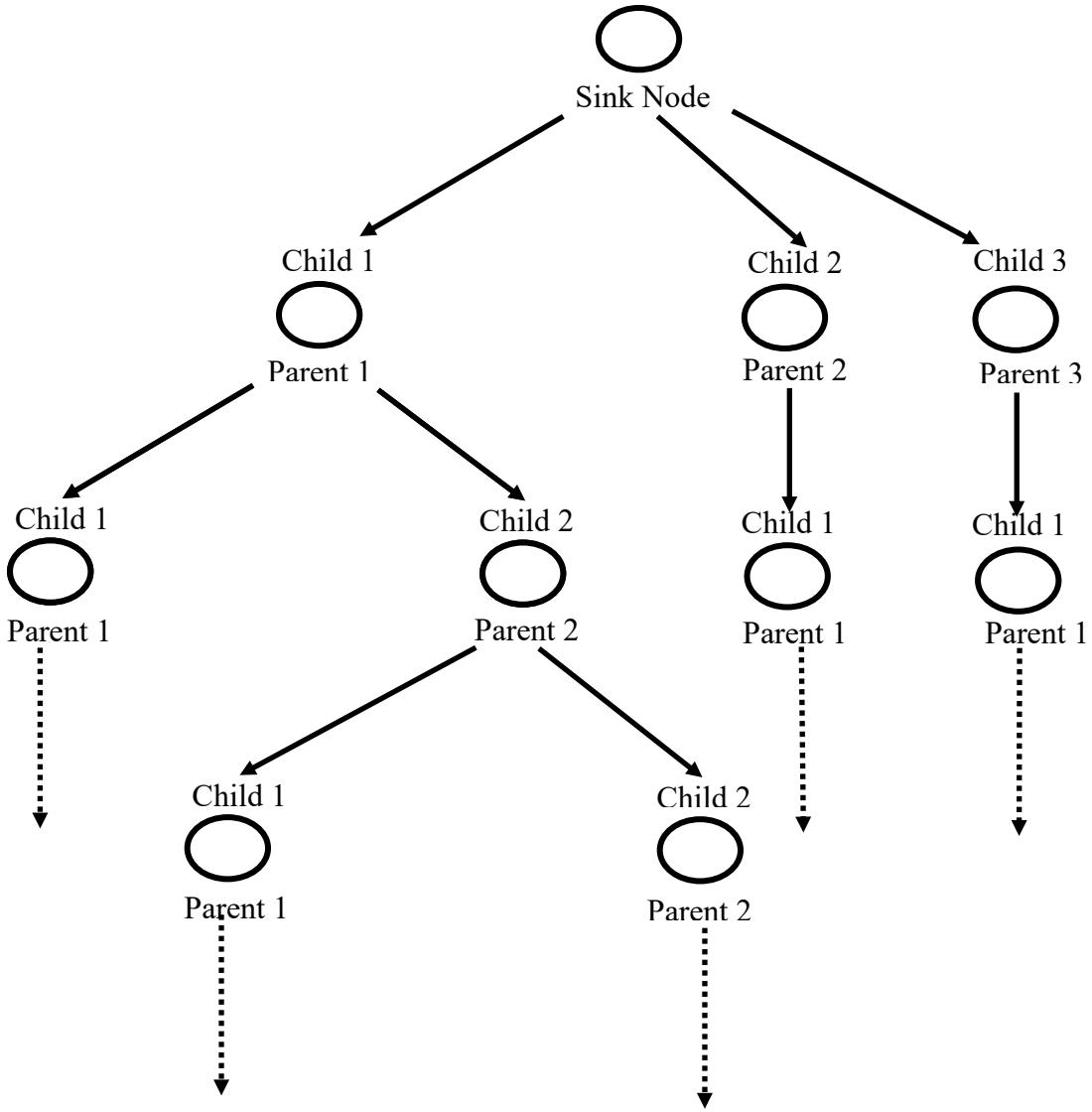

Figure 3.1: Sink Node (Base station) Broadcast Hello Packet to all the Child Nodes

4. Results and Discussion

During the simulation we increased the network size and record the performance of the nodes. We did this simulation for 1,450 milliseconds. Readings were taken for different network sizes (50, 100 and 120 nodes). From the result, it is evident that the attackers continuously send fake packets at different rates at an interval lower than the adaptive timeout value. We implement a security mechanism on TMAC protocol and the analysis of the performance of our intrusion detection was carried out using OMNet ++. The Model is constructed on various number of nodes with diverse field sizes and deployment types.

4.2 Assumption

a) Attackers are external.

b) No attack at deployment stage.

4.3 System specifications

We used the TMAC protocol, with transmission power of 60.15MW (MegaWatt), and the receiving power of 73MW (MegaWatt), the RTS – is the request to send packet send from a transmitter to receiver, while CTS – is the clear to send packet send to a transmitter from a receiver and ACK is acknowledgement packet send upon receipt of a RTS or CTS. Then, the adaptive timeout for the nodes to transit to sleep mode on the protocol TMAC is 20millisecons and packet spacing is 12milliseconds. All these are necessary because we want to know the amount of energy consumed under attacked and secured network.

Table 4.1 General Simulation Parameters and values

Parameters	Values
3MAC Layer protocol	TMAC
Transmission Power	60.15Mw
Receiving Power	73MW
RTS, CTS, ACK size	15Bytes
Adaptive Timeout	20ms
Packet Spacing	12ms

4.4 Simulation Results

Intruder constantly send fake packet at interval less than the TA. We test the algorithm with various number of nodes, varying the simulation time. The energy consumption of all the nodes in the network is shown on the graph. The algorithm is compared with when the nodes are working under attack. On the Graphs, we have;

a) Attacked signifies when intruders invade the nodes on the network.

b) Secured signifies the system working under normal condition.
c) Improved signifies our algorithm on TMAC protocol
.

1st Case with 50 nodes on the network

Table 4.2 Parameters for 50 Nodes

Parameters	Values
Number of Nodes	50
Number of attackers	7
Field size	40X40meters
Deployment Type	"10X5"

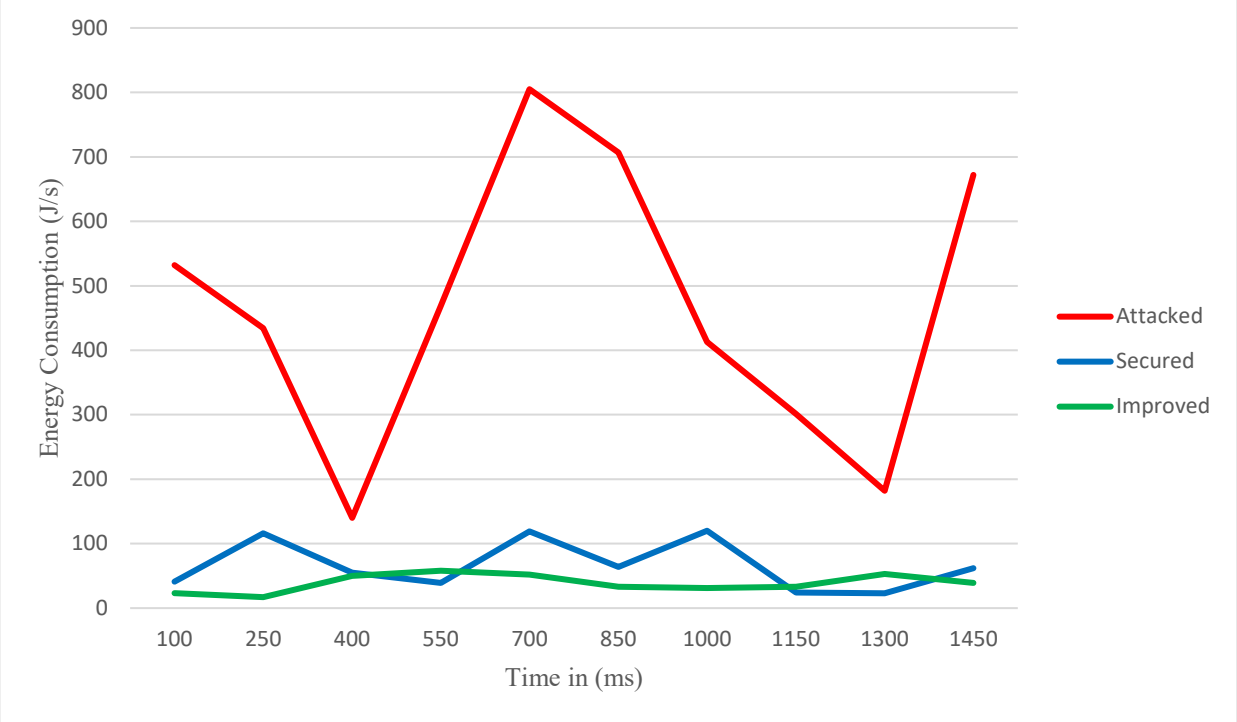

Figure 4.1: Energy consumed with 50 nodes

From Figure 4.1 it shows that our improve mechanism helps to preserve more energy with attackers on the network.

2nd Case with 100 nodes on the network

Table 4.2 Parameters for 100 nodes

Parameters	Values
Number of Nodes	100
Number of attackers	10
Field size	50X50meters
Deployment Type	"20X5"

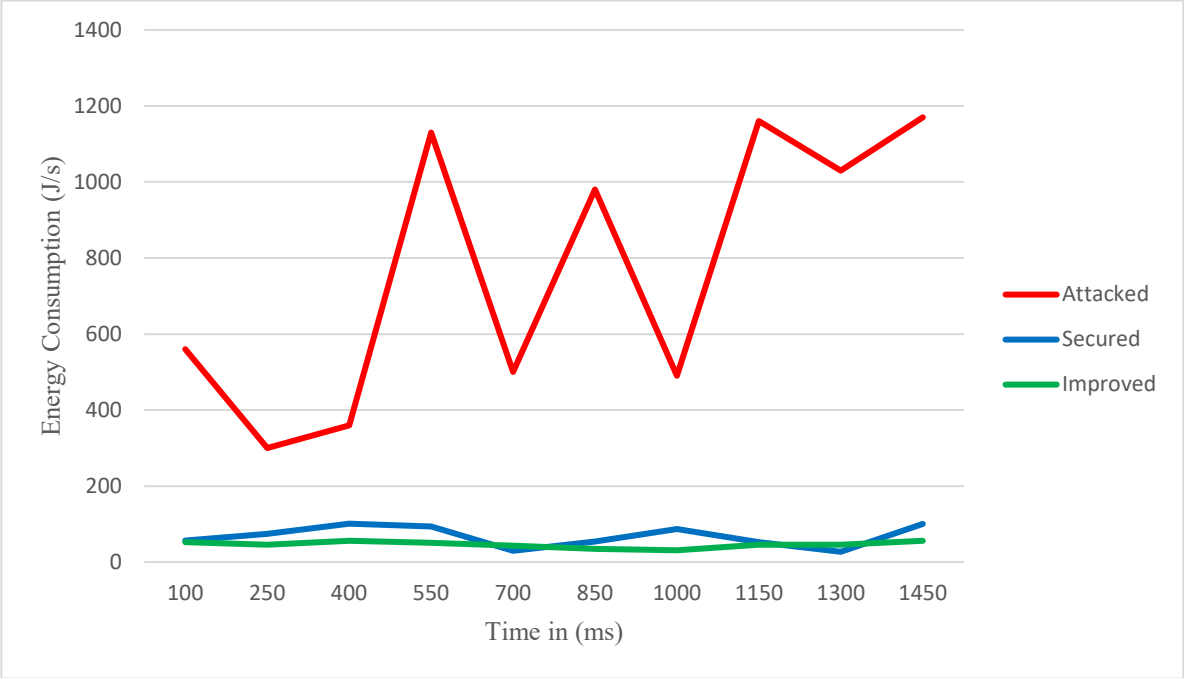

Figure 4.2: Energy consumed with 120 nodes

From Figure 4.2 with ten attackers on the network the energy consumed tend to increase but with our improve method in place, it help to reduce energy depletion.

3rd Case with 120 nodes on the network.

Table 4.3 Parameters for 120 nodes

Parameters	Values
Number of Nodes	120
Number of attackers	15
Field size	60X60meters
Deployment Type	"30X4"

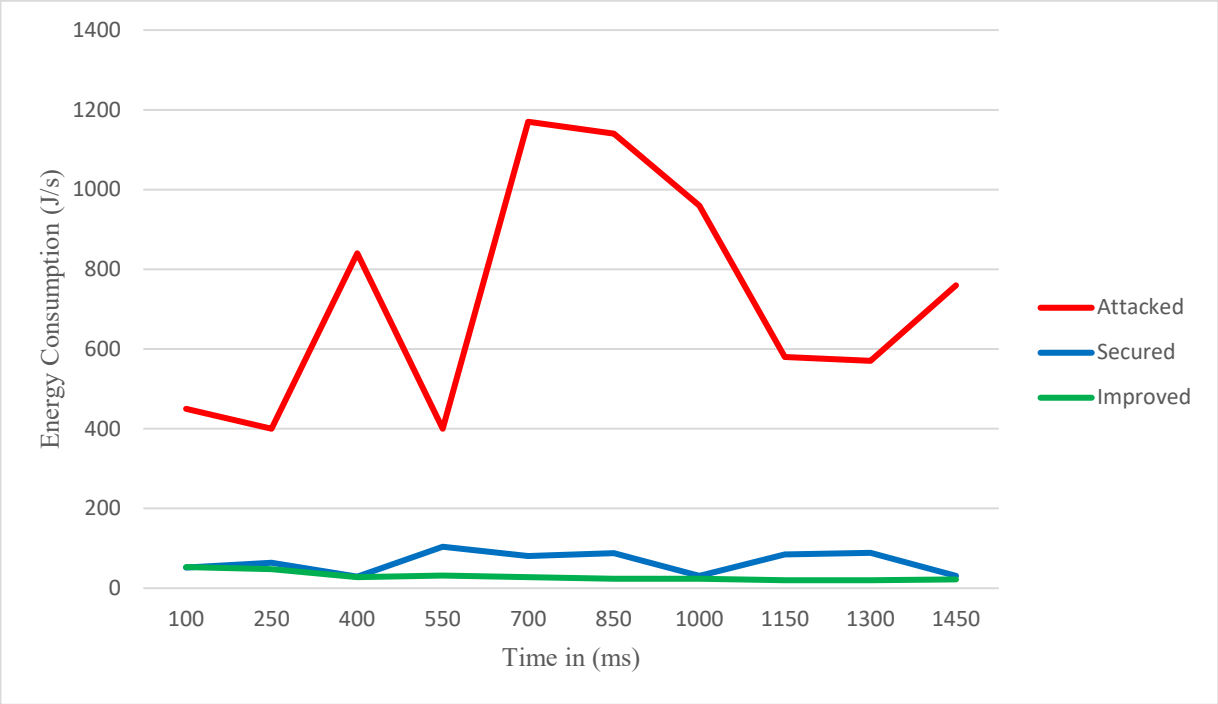

Figure 4.3: Energy consumed with 120 nodes

From Figure 4.3 with fifteen attackers on the network the energy consumed tend to increase but with our improve method in place, it help to reduce energy depletion.

5. Interpretation of Results

We applied the same transmission and receiving power on all the nodes, the intruder constantly broadcasts invalid packets at interval of 18ms just below the adaptive timeout to prevent the node from transiting to standby mode, all through the simulation time. Our graphs shows the average energy consumed on the victim node increases with increase in simulation time. The graph also shows that our algorithm works better in all the cases even with an increase in the number of nodes. It also goes further to state that the mechanism on the TMAC could efficiently mitigate denial of sleep attacks.

5.1 Conclusion

We initiate a method by using network organisation and was able to design an algorithm to prevent DoSL attacks. We simulate broadcast attacks on TMAC protocol. With our method it was discovered that the algorithm performed better and a large amount of energy was conserved as the nodes goes to sleep after the network organisation and also an intruder is detected immediate a node receives packet from a node which is not listed as it parent or child and it is discarded, with this method there is no need to trace an intruder to the root.

5.1 Future work

There is need to test this Simulation with more deployment and also using uniform distribution approach. The following are also recommended:

(a) To test the algorithm with the other classes of denial of service attacks.

(b) To test the algorithm on larger field sizes.

REFERENCES

Bhattasali, T., & Chaki, R., (2011). Lightweight hierarchical model for HWSNET, *ArXiv Prepr. ArXiv11111933*.

Bhattasali, T., Chaki, R., & Sanyal, S. (2012). Sleep Deprivation Attack Detection in Wireless Sensor Network, *ArXiv Prepr. ArXiv12030231*.

Bhullar, R., K., Pawar, L., & Kumar, V. (2016). A novel prime numbers based hashing technique for minimizing collisions. In *Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on IEEE:* 522-527.

Boubiche, D., & Bilami A. (2012). Cross layer intrusion detection system for wireless sensor network. International Journal of Network Security and Its Applications, 4(2), 35.

Brownfield, M., Gupta, Y., & Davis, N. (2005). Wireless sensor network denial of sleep attack, in *Information Assurance Workshop, IAW'05. Proceedings from the Sixth Annual IEEE SMC*, 356–364.

Cakiroglu, M., Özcerit, A., T., Ekiz, H., & Çetin, O. (2006). "MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey," in *ICWN*, 45–48.

Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks, in *Security and Privacy, Proceedings. Symposium on*, 197–213.

Chaudhari, H., & Kadam, L. (2011). Wireless sensor networks: security, attacks and challenges, *International Journal of Networking*, 1(1), 4–16.

Chen, C., Hui, L., Pei Q., Ning, L., & Qingquan, P. (2009). An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," in *Information Assurance and Security, IAS'09. Fifth International Conference on*, 2009, vol. 2, pp. 446–449.

Dargie, W., & Poellabauer, C. (2011). *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons.

Desnitsky, V., Kotenko I., & Rudavin N. (2018). "Ensuring Availability of wireless Mesh Networks for Crisis Management," Intelligent Distributed Computing XII. Studies in Computational Intelligence Springer-Verlag. Vol.798. Proceeding of 12th Internaltional *Symposium on Intelligent Distributed Computing (IDC2018)*. Bibao, Spain, Springer-Verlag. 344-353.

Desnitsky, V., A., Kotenko I., V, & Rudavin, N., N. (2019). Protection Mechanism against Energy Depletion Attacks in Cyber-Physical System. *2019 IEEE conference of Russian Young Researchers in Electrical and Electronic Engineering (ELconRus); Saint Petersburg and Moscow, Russia, Russia*. DOI 10:1109/ElconRus. 8656795.

Farooq, N., Zahoor, I., Mandal, S., & Gulzar, T. (2014). Systematic Analysis of DoS Attacks in Wireless Sensor Networks with Wormhole Injection. International *Journal of Information*

and Computation Technology. ISSN 0974-2239, 4(2), 173-182.

Fotoli, R., & Bari, S., F. (2020). A Novel Countermeasure Technique to Protect WSN againt Denial-of-Sleep attacks using Firefly and Hopfield Neural Network (HNN) algorithms. The Journal of Supercomputing. 76(6). DOI: 10.1007/S11227-019-03131-X.

Gelenbe, E., & Kadioglu Y., M. (2018). Bettery Attacks on Sensors, International Symposium on Computer and Information Sciences, Security Workshop, Springer International Publishing.

Gunasekaran, M., & Periakaruppan, S. (2017). GA – DoSLD: Genetic Algorithm Based Denial-of-Sleep Attack Detection in WSN, Security and Communication Networks, 1-10, Doi: 10.1155/2017/9863032.

Hsueh, C., T., Wen, C., Y., & Ouyang Y., C. (2015). A sesure scheme against power exhausting attacks in hierarchical wireless sensor networks. *IEEE Sensor journal, 15(6*), 3590-3602.

Kalnoor, G., & Agarkhed, J. (2018). Detection of Intruder using KMP Pattern Matching Technique in Wireless Sensor Networks. Procedia Computer Science, 125, 187 -193.

Li, Y., Thai, M., T., & Wu, W. (2007). *Wireless Sensor Networks and Application.* Springer – Verlag, Berlin Heidelberg. ISBN: 978-0-387-49591-0.

Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S., V. (2011). Denial of service attacks in wireless networks: The case of jammers, *Commun. Surv. Tutor. IEEE*, 13(2), 245–257.

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.

Raymond, D., R., & Midkiff, S., F. (2008). Denial-of-service in wireless sensor networks: Attacks and defences, *Pervasive Comput. IEEE*, 7(1), 74–81.

Samir, A., Djallel, E., B., & Azeddine, B. (2013). Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs. *2013 World Congress on Computer and Information Technology (WCCIT),* **DOI:** 10.1109/WCCIT.2013.6618693

Shakhov, V., Koo, I., & Rodionov, A. (2017). Energy exhaustion attacks in wireless networks, *Engineering, Computer and Information Sciences (SIBIRCON), International Multi-Conference on IEEE,* 1-3.

Wood, A., & Stankovic, J., A. (2002). *Denial of service in sensor networks, Computer,* 35(10),