IMPLEMENTATION OF A MITIGATION STRATEGY FOR DENIAL OF SLEEP ATTACK AT NETWORK ORGANIZATION LEVEL IN WIRELESS SENSOR NETWORKS

M. Shua'ibu[1], I. R. Saidu[2], A. Jegede[3, 4], A. Oloyede[5], M. Magaji[3] and J. Mazadu[6]

[1]Department of Computer Science, Kaduna Polytechnic, Nigeria
[2]Department of Cyber Security, Nigerian Defence Academy, Kaduna, Nigeria
[3]Department of Computer Science, University of Jos, Nigeria
[4]Africa Centre of Excellence on Technology Enhanced Learning, National Open University, Abuja, Nigeria
[5]Department of Computer Science, Lagos State University, Ojoo, Nigeria
[6]Department of Computer Science, Federal University, Wukari, Nigeria

Corresponding Author's Email:[2]jegedea@unijos.edu.ng

Article History: Received 15 August 2022; Revised 28 October; Accepted 29 November 2022

ABSTRACT: Wireless sensor networks are special types of networks which use wireless interfaces to connect mobile nodes. These networks do not need fixed infrastructure. Due to high mobility in nodes and dynamic infrastructure of wireless sensor network, the energy (power) of the nodes is an important factor. There are many factors which affect the proper functioning of a wireless sensor network. However, the most fundamental is intrusion attack against a victim node and the consequent depletion of its battery. This eventually have adverse effects on the performance of the network. Therefore, Adaptive Time-out of the protocol enables sensor nodes transit to standby mode from time to time. The inability of a node to enter a sleep mode is referred to as sleep deprivation or denial of sleep attack. This study proposes a technique for mitigating denial of sleep attack at the Network Organization stage of wireless sensor networks. The purpose of this research is to prevents the intruder from gaining access into the network. Simulation using OMNET ++ simulator was used to demonstrate the performance of the proposed approach. As a results the proposed method mitigates the denial of sleep attacks on wireless sensor networks.

KEYWORDS: *attack; denial of sleep; network organization algorithms; sink node; wireless sensor networks*

1.0 INTRODUCTION

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 [1] WSNs offer efficiently feasible solutions for numerous applications such as current implementations to monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings, and home environmental sensing systems for temperature, light, moisture, and motion.

The Development of wireless sensor networks resulted mainly from the military applications such as battlefield surveillance [2]. WSN is one of the most important technologies of the 21st century. There is a rapid increase in the deployment of WSNs increase because they support a variety of applications ranging from environmental monitoring to support and automate chores fields as a result of technological advancement. WSN is becoming a more commonplace 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.

WSNs face several security challenges when deployed to remote areas. One of the most challenging security threats is 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 [3]. 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. Attackers require minimum basic technical knowledge, tools and resources to carry out depletion attacks effectively [4]. The attacker can deplete the device's energy completely and rapidly, causing the compromised node to become completely disabled.

The wireless sensor network sensor nodes are normally powered with batteries, but they still suffer energy depletion [5]. this is caused due to collisions, overhearing, idle listening and control packet overhead. WSN technology are confronted with so many acquired constraints and this ranges from sensor node architecture, runtime, and others [6] All these, because the network faces many challenges such as energy

inefficiency, routing, self-organization and self-maintenance, data aggregation, security, and mobility. Wireless sensor network belongs to the family of ad hoc networks and it inherits the characteristics of ad hoc [7]. The nature of the wireless environment makes the sensor nodes susceptible to security breaches. Intruders may gain unauthorized access to the network and disrupt its normal operation. Nodes normally use energy-saving mechanisms which allow them to switch to standby (sleep) mode regularly.

However, malicious nodes join the network and prevent nodes wishing to enter standby mode from turning off their radio. This is called sleep deprivation torture or denial of sleep attacks. It is accomplished by making a victim node believe that there is data to be transmitted or it just has to stay awake for monitoring. This results in much overhead and eventually leads to poor performance [8]. A related study proposed an algorithm to mitigate sleep deprivation attack on sensor node [9]. The approach applies an authentication method on the TMAC using ID. A major limitation of this approach is that all the nodes are active during the organization stage of the network which leads to energy depletion. The need to trace any suspected attack to its root results in much overhead in terms of power consumption. Several studies have been carried out on denial of sleep attack (DoSL) but none address limitation found in [9]. [1] propose an algorithm to mitigate denial of sleep attack but uses a different approach; they use DoSA-immune schema by applying the Firefly, Hopfield Neural Networks (HNN), and RSA optimization. Also [5] proposed a technique for generating DoSL attack profiles from multiple sensor nodes such that the attacker nodes can be prevented from the communication process. The approach used is different from that of Manju et al [9]. A study of an attack implemented using SMAC protocol involved a clustered base station with each cluster having head [10]. It was replay attack based on Selective Local Authentication for detection of denial of sleep attack. Hashing and interlock protocol were used for key exchange and Zero Knowledge for authentication of base node.

This study proposes a technique for detecting, mitigating and isolating intruders in wireless sensor network in an efficient way. The proposed solution addresses energy depletion in WSN and eliminates the need to trace a node to the root whenever an attack is detected. The performance of the model is evaluated in order to determine its ability to detect intruders in the network. The rest of the paper is organized as follows. Section 2 focuses on related works highlighting potential attacks against WSNs and techniques for addressing them. Section 3 presents the methodology including the algorithm of the proposed

solution, tree structure of the proposed model and the simulation environment used for evaluating the proposed method. Section 4 highlights the results and discussion, while Section 5 presents the conclusion and future work.

2.0 RELATED WORK

It is pertinent to note that in the context of DoSL a number of approaches exist to curb these attacks, however the majority of them are techniques that do not take energy-efficiency into consideration and even when they do, throughput becomes a trade-off which could become counter-productive in the long run [11]. Attack can be categorized into two which are external and internal attacks according to [12]. External attacks are usually initiated by nodes outside the logical network. The nodes do not have internal information such as cryptographic information about the network. Internal attacks include attacks launched by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes and who then use one or more laptop-class devices to attack the network.

Jamming attacks involve malicious nodes blocking legitimate communication by causing intentional interference in networks [13]. The attack interferes with the radio frequencies used by the sensor nodes. 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 checks 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.

Media Access Control (MAC)protocols play a huge role in the energy-efficiency of WSN especially as these networks have resource-constrained devices which are mostly battery powered. The radio is the major source of energy consumption in these devices and access to radio is controlled by the MAC layer. Hence, the MAC protocols use

duty cycling as one of the ways for saving energy by making nodes go to sleep when they are idle and having them only wake up when they need to transmit or receive data [11].

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 DSA attacks. These protocols however operate at the link layer. The link layer decides when the radio should transmit frames and listen to the channel. The MAC protocol is responsible for managing the radio of sensor, which is the main source of power consumption. More energy is consumed at the transceiver [14].

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 [15]. An ideal jam should have high energy efficiency, low probability of detection and disrupt communications to the desired or maximum possible extent.

For instance, in order to maintain a low probability of detection, the jammer can adopt techniques that are consistent with MAC layer behaviours. This attack however consumes less energy of the attacker but causes disruptions to the operation of the network [16]. An attacker may also send out many RTS packets so that the nodes will continuously send out CTS packets thereby exhausting the power [4]. It is assumed that the attacker has prior knowledge of the MAC protocol used so as to know the ideal time to send the packets, which is known as exhaustion attack.

Unfairness attack is a weaker form of DoS attack in which the attacker degrades the network performance rather than preventing legitimate nodes from having access to the channel. For example, the attack could cause users of a real-time MAC protocol to miss their deadlines. A proposed solution is to use small frames so that an individual node can capture the channel only for a short time. Framing overhead could however be increased provided long messages are transmitted. Furthermore, this solution is susceptible to further unfairness, if the adversary responds quickly rather than randomly delaying. The attacker uses traffic pattern analysis to identify and target these nodes since they provide critical services to the network. The network codes

are then destroyed by the attacker. One way to prevent this attack is to provide confidential information (encryption) for both message headers and their content, although it doesn't completely prevent traffic analysis. The use of "dummy packets" was recommended for preventing traffic analysis throughout the network.

However, this approach results in significant wastage of energy in sensor nodes [15]. Denial of sleep attack usually occurs at the link layer and it continually keeps the node's radio on thereby preventing the nodes from transiting to sleep mode. This kind of attack can drain the battery of the nodes only in few days. The MAC protocols however control the functionality of the transceiver and hence, become a natural focus for DSA attacks [12]. There are several ways by which the attack can be initiated against MAC protocol.

2.1 Unintelligent Attack

The attacker has no knowledge of the MAC protocol as well as no ability to Penetrate Network. Recorded traffic is replayed into the network, causing nodes to waste energy while trying to receive and process these extra packets. Nodes that do not implement anti-replay mechanisms are vulnerable to this type of attack causing replayed traffic to be propagated through the network. The replaying of events has adverse effect on the network lifetime and overall performance of WSN.

2.2 Unintelligent Broadcast Attack

The attacker here also has full knowledge of the MAC protocol used but has no ability to penetrate the network. The attacker simply broadcasts unauthenticated traffic into the network and publish larger duty-cycle schedule in order to reduce the network lifetime by obeying the rules of the MAC protocol. The messages are then received by the nodes in the network but are discarded. This attack causes the nodes to extend their listen period trying to receive the packets, which however leads to increase in energy consumption and reduction in network lifetime.

2.3 Full Domination Attack

This classification is one in which the attacker has full protocol knowledge and has also penetrated the network. This attack is usually initiated using one or more compromised nodes in the network. For

example, knowing fully well the Sensor-MAC (SMAC) protocol, the attacker sends a SYNC message at a frequency just short of the duty cycle to keep delaying the transition to sleep mode. In T-MAC, the attacker sends continuous packets at an interval slightly shorter than the Adaptive Timeout (TA) to prevent the nodes from transiting to sleep mode. The Synchronization attack is not effective on T-MAC, because of TMAC's adaptive timeout mechanism. The nodes transit to sleep mode when there is no activity in the network for a period defined as TA. Despite the advantage of TMAC over SMAC protocol, TMAC is vulnerable to a simple denial of sleep attack by sending constant stream of small packets at an interval just short of the network's adaptive timeout. This can make the sensor nodes to be awake all through [9]. The solution in [9] was for existing MAC protocols such as S-MAC and T-MAC. The inability to authenticate the SYNC packet in SMAC and T-MAC makes MAC protocols susceptible to sleep deprivation attack. Also, the network is easily susceptible to replay attack. The proposed solution is based on providing strong authentication to the SYNC packets; so as to defend denial of sleep attack in the network.

A related study is the DoSA-immune schema based on Firefly, Hopfield Neural Networks (HNN), and RSA [1]. The proposed WSN-FAHN consists of nodes distributed randomly. The network has a multi-channel mobile sink and n sensor nodes which have primary energy. The communication of cluster members with CH is done in one hop. Moreover, each CH communicates with the sink in one hop. Nodes are able to adjust their transmission radius. The network activity cycle is divided into several rounds. Similarly, [5] proposed a method which generates DoSL attack profiles from multiple sensor nodes such that the attacker nodes can be prevented from the communication process. The authors simulated the WSN with 100 static sensor nodes and then used the BS to performs 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. An estimation of the fitness value is for every chromosome provided the means of validating the trustworthiness of the relay nodes in the route. A chromosome that is suspected to be unusual is validated against the

existing attack profiles. If there no a match, the pair of chromosomes is subjected to 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. The study in [4] focused on a special software for Arduino platform based legitimate nodes. The firmware (also known as sketches) ensures correct reading of GPS data and sends the data in a timely manner as in a normal network operation. A sketch for the attacking node was also written to model the normal operation of the network and the messaging process. The software of one of the legitimate nodes was modified. The model uses a coordinator node to achieve stable network operation. It also has a victim node consisting of an Arduino microcontroller and XBee module. The node is connected via USB to the computer to intercept and analyze incoming traffic. Another element of the model is a typical network node, which has hardware interface settings (display and buttons), implementation of the software function of sending messages to the victim node and a connection to an attacking parasite module to initiate a vampire attack. The variability of the modeled normal traffic is provided by using parameters, taking into account some maximum possible deviation defined on the basis of a random number sensor. The MAC protocol in the data link layer of the WSN allows intruders to send fake packet in an interval below the Adaptive Timeout (TA) of the Timeout Medium Access Control (TMAC) protocol and this increases energy consumption because the nodes need to stay awake for transmission which in the long run result in energy depletion [9]. Hence the authors suggested that the application of network organization algorithm at the deployment stage will help to conserve the energy of the sensor node. However, all the nodes are active during network organization and the need to trace a malicious node down to the root results in much overhead and energy consumption. Thus, it is pertinent to propose a solution which minimizes energy consumption by allowing nodes to transit into sleeping mode once they are not sending or receiving messages. Table 1 presents the summary of study used in the research. The table shows the proposed approaches as well as their strengths and weaknesses.

Table 1: Summary of Related Studies

No.	Author(s)	Method	Strength	Weakness
1.	Chen et al. [18]	A fake schedule switch method was proposed with RSSI measurement aid. This method was implemented on S-MAC algorithm, which adopts active/sleep switch and lower duty cycle for conserving power.	Active/sleep switch and lower duty cycle for conserving power was realize.	Due to the mechanism used in S-MAC, introducing energy silent mechanism also creates the possibility for attackers to disrupt the normal communication of the system.
2.	Fotohi and Bari [1]	Proposed a DoSA-immune schema by applying the Firefly, Hopfield Neural Networks (HNN), and RSA optimization. The proposed WSN-FAHN consists of nodes distributed randomly. The network has a multi-channel mobile sink and n sensor nodes which have primary energy.	Each CH communicates with the sink in one hop. Nodes are able to adjust their transmission radius. Also, the network activity cycle is divided into several rounds.	Much overhead is incurred because the process is complicated.
3.	Manju et al. [9]	Proposed a solution on the existing MAC protocols such as S-MAC and T-MAC using Network Organization Algorithm, the method was based on providing strong authentication to the SYNC packets; so as to defend denial of sleep attack in the network.	There was strong authentication the SYNC packets.	The affected node is traced down to the root with authentication token. Energy consumption increases as all nodes are active during the network organization.

2.4 Recent Advances in DoSL Attack Detection and Mitigation

Folohi et al [19] proposed an algorithm for detecting DoSL attacks in vehicular ad-hoc networks. Such attacks usually occur at the confirmation phase due to overhead delay at the network's base station. The method used P-secure to detect attacks before the confirmation phase. This reduces the processing delay and increases security in the networks**.** A related work presents a comprehensive, validated and practical solution to DoSL attacks in wake-up-radio-based systems [20]. The approach integrates Elliptic Curve Cryptography-based key exchange protocol and implicit certificates. Shakhov and Koo [21] proposed a theoretical model for evaluating energy consumption of an IoT network during attack. Simulation results show that the approach is effective against depletion of battery attack. On the other hand, Krentz et al [22] focused on the use of dozing optimization to reduce energy consumption during ding-dong ditching attack and minimize energy requirement during normal operation. The approach is resistant to collision attack and efficient in terms of energy consumption.

Sun et.al [23] proposed a hybrid method based on blockchain permission, attribute-based access control and identity-based signature to build a lightweight, secure, and cross-domain access control system for IoT. An implementation of the proposed solution shows that it is suitable for detecting DoSL attacks in real-life IoT networks. Another multialgorithmic solution used recurrent neural network and long short-term memory (LSTM) to address the inability of narrowband Internet-of-Things (NB-IoT) to support advanced and complex security mechanisms suitable for preventing DoSl attack [24]. Experimental results show that the accuracy and detection time of LSTM classifier are 98.99% and 2.54 x 10^{-5} second/record. This is higher than the performance of a gated recurrent unit. However, RNNs can detect NB-IoT networks-based DoSl attacks better than other machine learning approaches. An improved solution measures the Euclidean distance of each node from the base station in order to detect sinkhole attack [25]. The proposed technique does not require additional overhead in terms of hardware and communication cost. A similar strategy suggested the use of intelligent agents to distribute relevant knowledge useful for preventing denial of-sleep attacks [26]. The approach used different network sizes to simulate three media access control (MAC) protocols. The evaluation, comparison and analysis of signal strength at the

destination and the parameters for measuring link quality for each protocol demonstrates the necessity of and procedure for DoSL attack detection based on such parameters. A very recent study [27] surveyed IoT security issues, challenges, opportunities, and solutions for addressing security problems in IoT networks. This includes basic architectural description of the four IoT layers and security concerns associated with each layer. It also presented various IoT security attacks and their solutions.

3.0 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 transit to sleep mode upon receipt of Hello Response from all child nodes. At the end of network organization, all nodes wake up to begin synchronization. An algorithm was developed and the simulation frameworks is implemented using OMNeT++ language to find experiment analysis of the behaviour of the nodes. The nodes transit to sleep mode once Hello packet has been sent and Hello Response packet received. This approach reduces energy consumption. 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. There are five steps presented in the network organization approach.

5 Steps (Network Organization):

a) The Base-station (Sink node) broadcasts Hello Packets with ID and RSSI value.
b) 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.
c) The Node which receives Hello Packet includes the sender as its parent only if it has no parent.
d) The node updates its child list on the arrival of hello Response packet.
e) The node(s) then transits to sleep after receiving hello response packet.

The network organization algorithm used in the study is presented as follows.

```
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
```

The synchronization phase for the MAC protocol is initiated after network organization. Only valid nodes are able to synchronize with neighbours. Then, network is built in a tree-like structure as shown in Figure 1.

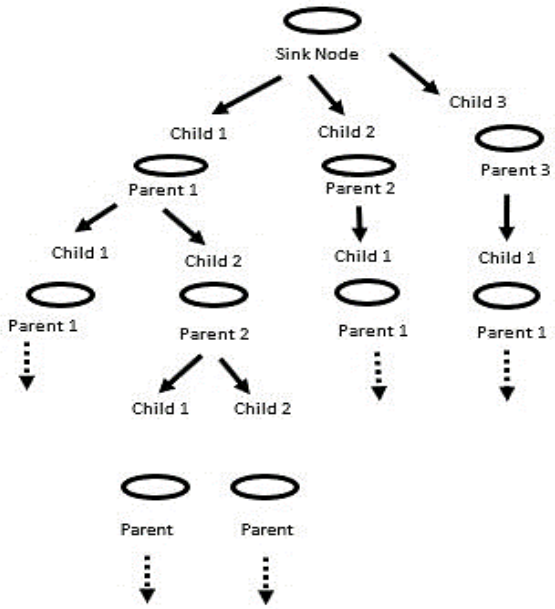

Figure 1: Tree structure of the mode.

Figure 1 shows that the Sink Node (Base station) broadcasts 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. The dotted arrow signifies that those parents do not have a child.

During the simulation the network size is increased and the performance of the nodes is recorded. The simulation is done for 1,450 milliseconds. Readings were taken for different network sizes (15, 30 and 50 nodes). From the experiment result, it shows that the attackers continuously send fake packets at different rates at an interval lower than the adaptive timeout value. A security mechanism is implemented on TMAC protocol and the analysis of the performance of the intrusion detection mechanism was carried out using OMNet ++ simulation environment. The model is constructed on various number of nodes with diverse field sizes and deployment types.

i. Assumption

a). Attackers are external.

b). No attack at deployment stage.

ii. Simulations and Parameters

The TMAC protocol is used with transmission power of 60.15MW (MegaWatt), and the receiving power of 73 MW (MegaWatt), the RTS is the request to send packet 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 20milliseconds and packet spacing is 12milliseconds. All these parameters in Table 2 are necessary because the amount of energy consumed under attacked network and secured network scenarios are need to be understood.

Table 2: General Simulation Parameters

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

4.0 RESULTS AND DISCUSSION

Based on the simulation result, the intruder constantly sent fake packet at interval less than the TA. The algorithm is tested with different number of nodes with varying the simulation time. The first scenario involves 15 nodes with 5 attackers.

The energy consumption of all nodes in the network versus the algorithm is compared with the situation when the nodes are under attack, secured and in improved performance. The graph in Figure 2 contains the following results:

a) Attacked, which refers to when intruders gain access to nodes on the network. Only 5 intruders were able to gain access to the network consisting of 15 nodes and field sixe of 25x25 meters. The ability of intruders to access the network due to lack of security measures resulted in energy consumption of 530 J/s.

b) Secured refers to performance results of the algorithm developed by [9]. It shows that the energy consumption reduced from 600 J/s to 75 J/s over a simulation time of 1450 ms.
c) Improved refers to the performance of our algorithm on TMAC protocol. The graph shows an improvement in energy efficiency because of the further reduction in energy consumption from 75 J/s to 30 J/s over the same simulation time of 1450 ms.

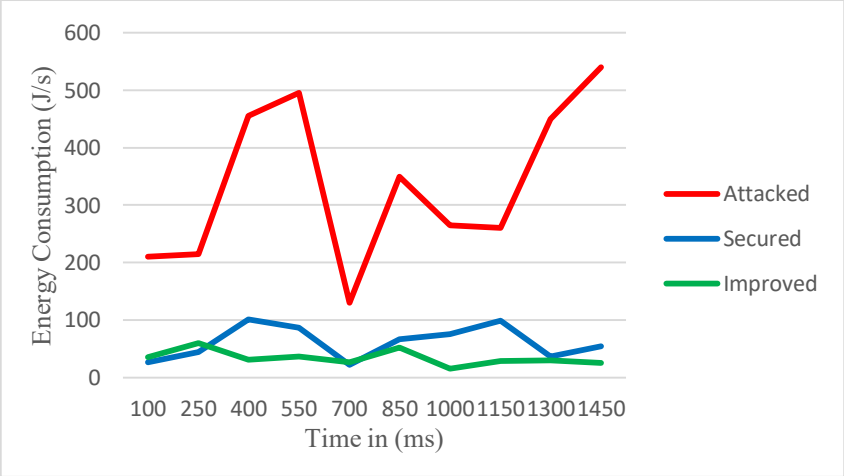

Figure 2: Energy consumed with 15 nodes

From the graph in Figure 2, when the nodes are attacked, the energy consumed increased, but with our improved mechanism, the energy is reduced to the nearest minimum.

The second scenario involves 30 nodes with 6 attackers. The field size is 35 x 35 meters and the deployment type is 10 x 3.

The energy consumption of all nodes in the network versus the algorithm is compared with the situation when the nodes are under attack, secured and in improved performance. The graph in Figure 3 contains the following results:

a) Attacked refers to the situation whereby a network is compromised. 6 intruders were able to access a network of 30 nodes and field size of 35x35 meters with 10 nodes per deployment. The large number of intruders resulted in high energy consumption due to lack of security measures in the network.

b) Secured refers to performance results of the algorithm developed by [9]. It shows that the energy consumption reduced from 900 J/s to 110 J/s over a simulation time of 1450 ms.
c) Improved shows the performance of the proposed algorithm on TMAC protocol. The proposed solution provides better energy efficiency because the amount of energy consumed over the same simulation time of 1450 ms further reduced to 20 J/s.

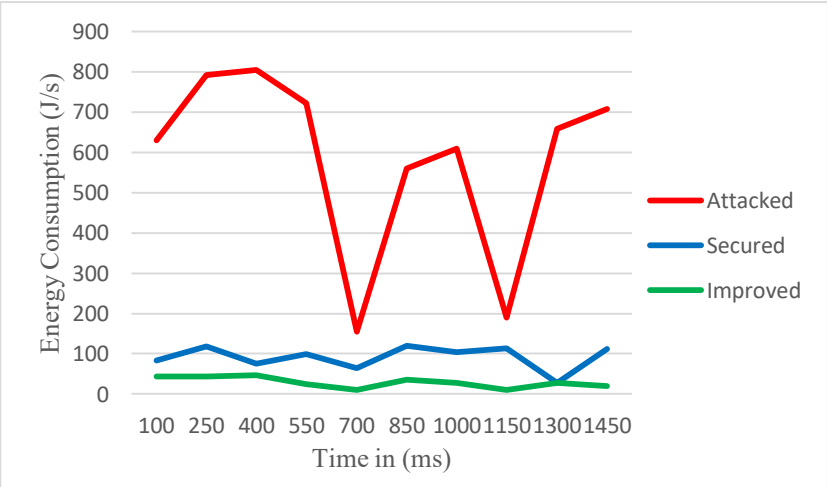

Figure 3: Energy consumed with 30 nodes

Figure 3 shows that an increase in the number of nodes and attackers results in a corresponding increase in energy consumption. However, the results show that the proposed method conserves energy and minimizes the rate of energy consumption.

3rd Case with 50 nodes on the network

The third scenario has 50 network nodes with 7 attackers. The field size is 40 x 40 meters and the deployment type is 10 x 5.

The energy consumption of all nodes in the network versus the algorithm is compared with the situation when the nodes are under attack, secured and in improved performance. The graph in Figure 4 contains the following results:

a) Attacked refers an attempted compromise of the network by intruders. 7 intruders were able to access a network of 50 nodes and field size of 40x40 meters with 10 nodes per deployment. The energy consumption of the nodes (685 J/s) is very high because there is no security measure in place. This resulted in energy consumption of about 685J/s.
b) Secured refers to performance results of the algorithm developed by [9]. The graph shows that over a simulation time of 1450 ms, the energy consumption reduced to 80 J/s despite an increase in the number of compromised nodes.
c) Improved illustrates the performance of our algorithm on TMAC protocol. It shows the proposed approach provides a significant reduction in energy consumption rate from 80 J/s to 25 J/s over a simulation time of 1450 ms. This is in spite of the increase in the number of deployed nodes.

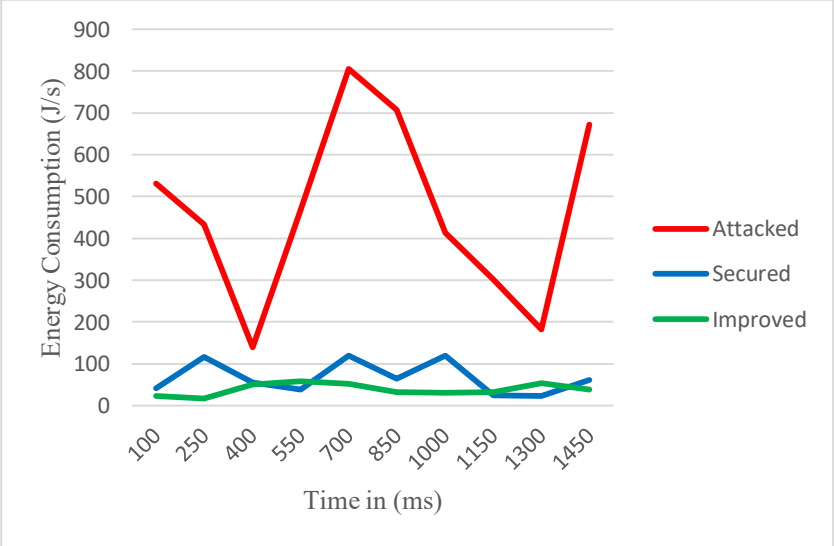

Fig. 4. Energy consumed with 50 nodes

Figure 4 shows that our improved mechanism helps to preserve more energy despite an increase in the number of attackers.

5.0 CONCLUSION

This paper proposed a novel algorithm for preventing DoSL attacks. We simulated broadcast attacks on TMAC protocol. The results of simulation showed that the proposed technique performs better and conserves a significant amount of energy. This is because the nodes go to sleep after the network organization and an intrusion is detected immediately a node receives a packet from a node that is not its parent or child. Such packet is discarded and there is no need to trace an intruder to the root. The proposed approach is efficient because it provides a significant reduction in energy consumption rate from 80 J/s to 25 J/s over a simulation time of 1450 ms. This is in spite of the increase in the number of deployed nodes. Network organization improves efficiency by providing better energy consumption distribution and minimizing overall energy requirement during attacks against wireless sensor networks [28]. It also offers robustness against changes in the network and provides self-optimization based on the needs of different applications which the network supports. A future work will perform the simulation on more deployment platforms and use a uniform distribution. This will involve testing the algorithm with other classes of denial-of-service attacks and on larger field sizes.

REFERENCES

[1] R. Fotohi, and S. F. Bari, "A Novel Countermeasure Technique to Protect WSN against Denial-of-Sleep attacks using Firefly and Hopfield Neural Network (HNN) algorithms", *The Journal of Supercomputing*, vol. 76, no. 6, 2020.

[2] W. Dargie,, and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*", New Jersey, United States: John Wiley & Sons, 2011.

[3] A. Wood and J. A. Stankovic, "Denial of service in sensor networks, *Computer*", vol. 35, no. 10, pp. 54–62, 2002.

[4] V. Desnitsky, I. Kotenko and N. Rudavin, "Protection mechanism against energy depletion attacks in cyber-physical system", in IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ELconRus), Saint Petersburg and Moscow, Russia. doi: 10:1109/ElconRus. 8656795, 2019.

[5] M. Gunasekaran and S. Periakaruppan, "GA – DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN", *Security and Communication Networks*, vol. 2017, pp. 1-10, 2017.

[6] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network", *ArXiv Prepr*, 2012.

[7] T. Bhattasali and R. Chaki, "Lightweight hierarchical model for HWSNET", *ArXiv Prepr*, 2011.

[8] E. Gelenbe, and Y. M. Kadioglu, "Bettery attacks on sensors", International Symposium on Computer and Information Sciences, Security Workshop Springer International Publishing, 2018.

[9] V. C. Manju, L. S. Senthil and M. Sasi-Kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks", in IEEE Conference Information & Communication Technologies (ICT), Tamil Nadu, India, pp.74–77, 2013.

[10] S. Naika, and N. Shekokarb, "Conservation of energy in wireless sensor network by preventing denial of sleep attack", *Procedia Computer Science*, vol. 45, pp. 370-379.

[11] C. Hsueh, C. Wen, and Y. Ouyang, "A sesure scheme against power exhausting attacks in hierarchical wireless sensor networks", *IEEE Sensor Journal*, vol. 15, no.6, pp. 3590-3602, 2015.

[12] G. Kalnoor, and J. Agarkhed, "Detection of intruder using KMP pattern matching technique in wireless sensor networks", *Procedia Computer Science*, vol. 125, pp. 187 -193, 2018.

[13] M. Cakiroglu, A. Özcerit, T. Ekiz, H. and Çetin, "MAC layer DoS attacks in wireless sensor networks: a survey", International Conference of Wireless Networks, pp. 45–48, 2006.

[14] D. R. Raymond, and S. F Midkiff, "Denial-of service in wireless sensor networks: Attacks and defences", *IEEE Pervasive Computing,* vol. 7, no. 1, pp. 74-81, 2008.

[15] R. Bhullar, L. Pawar, and Kumar, "A novel prime numbers based hashing technique for minimizing collisions", in 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), pp. 522-527, 2016.

[16] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy", *Magnetism*, vol. 3, pp. 271–350, 1963.

[17] K. Pelechrinis, Iliofotou and Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers", *IEEE Commun. Surv. Tutor.*, vol. 13, no. 2, pp. 245–257, 2011.

[18] C. Chen, L. Hui, Q. Ning, and P. Qingquan, “An effective scheme for defending denial-of-sleep attack in wireless sensor networks”, IAS’09 Fifth International Conference on Information Assurance and Security, vol. 2, pp. 446–449, 2009.

[19] R. Fotohi, Y. Ebazadeh and M. Seyyar, "A new approach for improvement security against dos attacks in vehicular ad-hoc network", *International Journal of Advanced Computer Science and Application*, vol. 7, no. (7), 2020. doi: http://dx.doi.org/10.14569/IJACSA.2016.070702.

[20] T. Capossele, V. Cervo, C. Petrioli and D. Spenza, "Counteracting denial-of-sleep attacks in wake-up-radio-based sensing systems," in 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1-9, 2016.

[21] V. Shakhov and I. Koo, "Depletion-of-battery attack: specificity, modeling and analysis", *Sensors 2018*, vol. 18, no. 1849, pp. 1-20, 2018.

[22] K-F. Krentz, C. Meinel and H. Graupner, “Countering three Denial of Sleep Attacks on ContikiMac”, In EWSN ’17: Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks, pp. 108 – 119, 2017.

[23] S. Sun, R. Du, S. Chen and W. Li, "Blockchain-based IoT access control system: toward security, lightweight and cross-domain, *IEEE Access*, vol. 9, pp. 36868 – 36878, 2021.

[24] T. Bani-Yaseen, A. Tahat, K. Kastell and T.A. Edwan, "Denial-of-sleep attack detection in NB-IoT using deep learning", *Journal of Telecommunications and Digital Economy*, vol. 10, no. 3, pp. 14-38, 2022.

[25] K. Mondal, S.S. Yadav, V. Pal, A.P. Singh, Y. Yogita and M. Singh, "Detecting sinkhole attacks in IoT based wireless sensor networks using distance from base station", *International Journal of Information System Modeling and Design*, vol. 13, no. 6, pp. 1-18, 2021.

[26] E. Udoh and V. Getov, "Performance analysis of denial-of-sleep attack-prone MAC protocols in wireless sensor networks", in 2018 UKSim-AMSS 20th International Conference on Modelling & Simulation, pp. 151-156, 2018. doi: 10.1109/UKSim.2018.00038.

[27] Y. Alotaibi and M. Ilyas, "Security risks in internet of things (IoT): a brief survey", in Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2022), pp. 1-5, 2022.

[28] M. Asim, "Self-organization and management of wireless sensor networks," Doctoral thesis, Liverpool John Moores University, Liverpool, United Kingdom, 2010.