Enhance the Security and Prevent Vampire Attack on Wireless Sensor Networks using Energy and Broadcasts Threshold Values

Hesham Abusaimeh
Associate Professor of Computer Science Department
Middle East University
Amman, 11831 Jordan

***Abstract*—Measuring and monitoring the surrounded environment are the main tasks of the most battery-based Wireless Sensor Networks (WSNs). The main energy consumption in the WSN is the communication and transferring data between these nodes. There are many researches works on how to preserve the energy consumption of the nodes inside this network. Most of these methods could save the energy and made the WSN lives for longer. However, there might be another reason of consuming energy and loosing these nodes from the network by the threats that targeting this kind of Networks such as the vampire attack that load the WSN with fake traffic. In this paper, a proposed method is presented of preventing the vampire attack from wasting the energy of the sensor nodes based on the energy level of the intermediate nodes in the way to the destination.**

Keywords*—Network security; vampire attack; sensor nodes; energy; lifetime; power consumption; packets delivery ratio

I. Introduction

WSN is an ad-hoc nature, self-configured network in term of establishing its grid topology and distributed itself in the environment. This kind of network can be used in many applications such as environmental measurement, industrial, health and military applications. Therefore, protecting the network energy is very important such as the technique proposed in [1]. These sensor devices mainly gather the information from the physical environment, such as temperature degree and humidity, and send it by other nodes in the network until it reaches the destination node or the base station [2].

As WSNs, become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable. In WSN, the energy is the most important factor since its energy coming from the attached non-chargeable battery. This energy is mainly consumed in gathering and forwarding information in the network. All the nodes in the flat wireless sensor nodes are communicating using peer-to-peer fashion without the need of central access point, which may cause many security threats to this kind of network [3] [4].

There are many security breaches that can affect the WSN, one of them is the vampire Attack, which will be described in Section II; Section III will explain some of the related work to prevent such kind of attacks, Section IV will give more details about the proposed method to prevent Vampire attack by modifying the PLGP protocol to consider the router energy and the broadcast average of each node. The paper will be concluded in Section V.

II. Vampire Attack

During the transmission of the data in the WSN after triggering some event in the environment, many attacks can affect this transmitted data and reduce the energy level of these sensors. These attacks aim to destroy the network by reducing the lifetime of each sensor node and prevent the delivery of the data packets [5].

One of these attacks that affect the data while it is transferred is the Vampire attack. There are two types of vampire attack, the Carousal attack and the Stretch attack. In the Carousal attack, the malicious node composes a fake packet to be transmitted by intermediate nodes in the WSN in certain path frequently. Repeating this fake packet by the malicious node in loop among the intermediate nodes will delay the service in the WSN. It also will increase the energy consumption and reduce the lifetime of the sensor nodes among this loop which will also reduce the lifetime among the WSN as shown in Fig. 1, where the fake packet is transmitted in loop among the nodes (A, B, C, and D) [5].

In the Stretch Attack as in Fig. 2, the path between the source node and the destination node will be stretched to include all the nodes in the network. This will be done during the forward process by a malicious node. Using this long path will consume more energy than the optimal path which is a lot shorter, therefore more nodes will have energy reduction and lose their lifetime [4]. Energy usage increase of factor O(min(N,ג)), where N is the number of nodes in the network and ג is the maximum path length allowed.

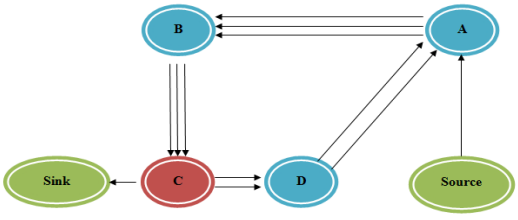

Fig 1. Carousel Attack [5].

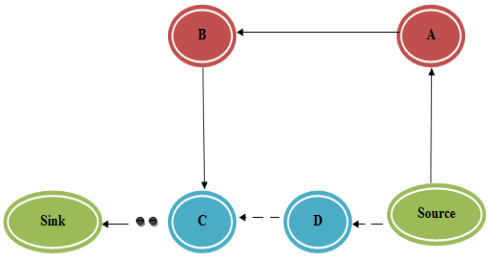

Fig 2. Stretch Attack [5].

Therefore, both famous types of vampire attack reducing the lifetime of the WSN either by having the packet to go in loop or to increase the number of intermediate nodes in the path to the destination.

III. Related Work

Nandhini, M. et al. proposed a method called Stop Transmit and Listen to detect the malicious node in the WSN. All nodes in the network will stop their transmission at a certain built-in time and listen for malicious transmission in the neighbor nodes, which can be malicious when it is sending in the non-transmitting time [6].

Pinky. B. et al. suggested content-based multicasting approach to defend the vampire attack and increase the battery life by enforcing a certain path of the data from the source to the destination [5].

Patil, A. and Giakwad, R. proposed a trust model system to prevent the vampire attack by defining a trust parameter for each sensor in the network [7].

Eugene Y. Vasserman and Nicholas Hopper introduced a definition for vampire attacks. Authours evaluates the vulnerabilities of existing protocols to routing layer energy depletion attacks. It is found that existing secure routing protocols such as Ariadne, SAODV, and SEAD does not provide security against Vampire attacks. The authors proposed defenses against some of the forwarding-phase attacks and introduced PLGP. The fully satisfactory solution for Vampire attacks during the topology discovery phase is not offered and further modifications to PLGPa is suggested [8].

Sivakumar and Murugapriya described the detection and elimination of vampire attacks in sensor networks. Authors proposed Optimal Energy Boostup protocol for providing the security. The PLGP protocol is performed as a tree structure. It is predicted that vampire attacks based on the behaviors of nodes and used to find the optimal path. It is found that the network energy is increased based on the location in forwarding phase [9].

In 2014, Menasinakai et al., explained the prevention and detection of vampire attacks. PLGP protocol is used to prevent the vampire attacks. To securely transmit the data, the path tracking technique is used in PLGP. The buffer technique also used in the proposed system in which the details of previous activity of every node is stored in a small buffer. It is found that, the proposed scheme is performed well to prevent attacks and achieved high energy consumption [10].

All of the above methods deal with the vampire attack as it is a serious problem in the WSN. Therefore, there is a need to detect this attack at early stages. In addition, most of these techniques considered their proposed method to be run over the clean-slate sensor network routing protocol (PLGP), which is originally considered as vulnerable to the vampire attack. PLGP has a discovery phase and then forwarding phase. There is also an enhancement on PLGP with attestations (PLGPa) by adding a verifiable path history to every PLGP packet. The addition of extra packet for verification also increases processor utilization, enquiring time and power consumption [11].

IV. Proposed Method and Simulation Results

Having vampire attack in any WSNs is critical. There is a need to detect these attacks as early as possible and prevent them from badly consuming the WSN energy level. The high availability of these networks is the critical property, and should stay alive even under malicious conditions. The PLGP protocol bounds damage from vampire attack, but it has some drawbacks. The PLGP includes path attestations, increasing the size of every packet results in increased bandwidth use, and thus radio power used to transmit these packets. In addition, of extra packet for verification, it also increases processor utilization, requiring time, and additional power for cryptographic computations and operations. PLGP is not considered to be vulnerable to Vampire attacks during the forwarding phase, but it might be vulnerable to that during the route discovery phase. Therefore, there is a need of new protocol that consumes less energy and discover the route and keep sending the data packets without any penetration by the vampire attacks. The modified PLGP protocol proposed in this paper to be enhanced version of PLGP and detect then prevent the vampire attacks in WSNs. The modified PLGP is based on reducing the processor utilization; requiring less detection time and maximizing the network lifetime. In this technique, we are arranging the sensor nodes in a particular manner so that there will be very less chances for occurrences of Vampire attack in the WSNs. This proposed modification of PLGP concentrate on measuring the route energy during the route discovery process, and it is also based on calculating the energy of the intermediate node on the route during the transmission of the data packet to the destination node. This route energy parameter will be calculated based on [1] route energy model and it will be added to the PLGP factors of choosing the best route to start routing the data packet.

Basically, the modified PLGP protocol detects the vampire attack based on two elements, the first one is the number of hops among the intermediate nodes, and the second one is the energy consumption of the routes to the destination. If any of these have been increased more than a threshold values expected of each route the discovery process will be initiated again by the modified PLGP. This regular checking and route discovery initiation will eliminate any suspicious nodes to be in the intermediate nodes in the route and choosing the shortest route without any loop in the middle.

In addition, the threshold value of the number of hops have been calculated based on the proposed model in [12]. This model discovers the malicious nodes during the discovery

phase based on the average number of broadcast packets in the network as in the following equation:

$$Threshold = \sum_{i=1}^{n} \frac{Number\ of\ Broadcast}{N}$$

Moreover, the malicious node and the attacked route by the vampire attack will be detected based on the threshold value and the route energy of the route. Therefore, if the energy of the route is on high consumption speed and the node broadcast packet average is larger than the threshold value, then the network might be under vampire attack. Afterword, the source node will initiate the route discovery process of the PLGP again in order to choose new route and eliminate any malicious node participating in the route to the destination. This will make the current route to be the shortest route and eliminate any loop to the destination sensor node.

The modified PLGP also calculated the packet delivery ratio after transmitting the whole data in order to guarantee the enhancement on delivery percentage of each source node packets to the destination node.

The proposed modified PLGP routing protocol in the WSN has been tested by implementing the updated model of the route energy and the broadcast value in the network layer of the sensor devices Using NS-3 simulation environment. The simulation was conducted of grid of 100 sensor nodes and Personal Area Network (PAN) coordinator to establish the network and establish the traffic in the network. These nodes are distributed systemically as shown in Fig. 3. The simulation has been run of 60 minutes period with initial full battery of sensor energy of 40 Joules.

Fig. 4 shows the simulation scenario that is created to generate the data packet from the coordinator node to different destinations, and many vampire attacks were established from different malicious node in the WSN grid. Afterward the results have been captured of the modified PLGP routing protocol and compared that with the original PLGP in term of energy consumption and node lifetime. Finally, the delivery ratio of the sent packet has been calculated to in both protocols. The following figure also shows the data packet path from the coordinator node to various destination nodes in dashed lines.

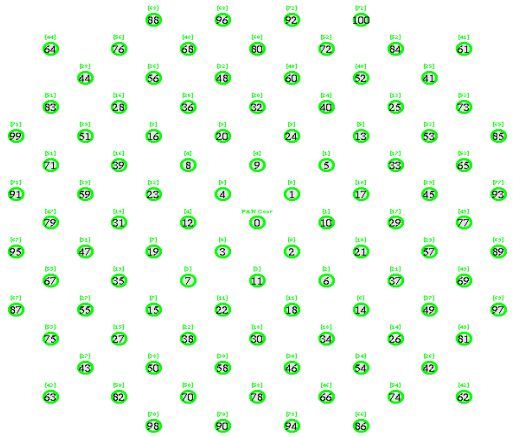

Fig 3. Sensors distribution in the Wireless Sensor Networks.

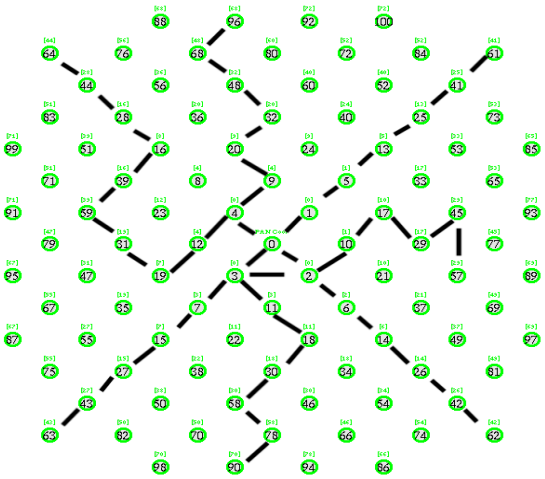

Fig 4. Traffic paths in the WSN grid.

Firstly, the consumption rate of the sensor node energy was compared between the modified PLGP with the route energy and number of broadcast approach to the tradition PLGP, where the vampire attack is most like to be happened and consume all the WSN energy. The results showed that the modified PLGP has reduced the energy consumption of each node in the WSN. Consequently, the energy consumption speed in the tradition PLGP was 0.03 Joules/Seconds, the modified PLGP has slowed the energy consumption average to 0.016 Joules/ Seconds, as in Fig. 5 shows the energy consumption rate of each wireless sensor nodes in both protocols.

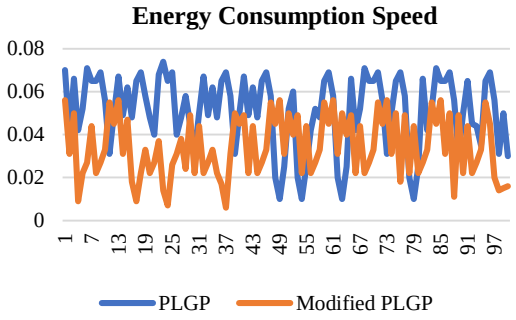

Fig 5. Energy Consumption Rate of the Sensor Nodes.

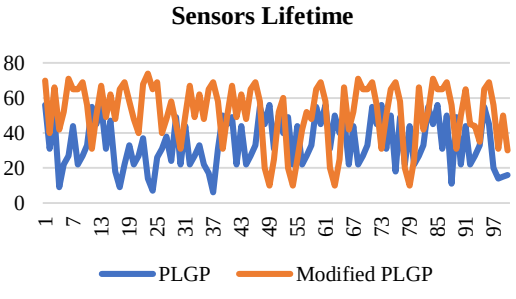

Fig 6. Wireless Sensor Nodes Lifetimes.

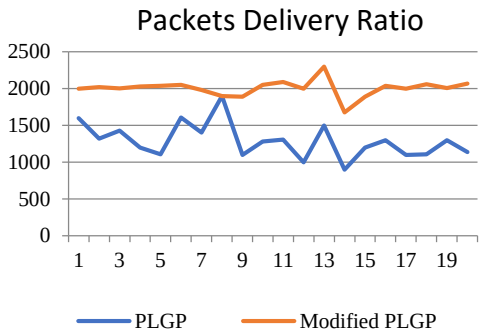

Fig 7. Packet Delivery Ratio of the Generated Packets.

The previous Fig. 6 clearly presents the results of the lifetime of each sensor nodes in the WSN among the Modified PLGP and the traditional PLGP. The results showed that the sensor node in the WSN that used the modified PLGP preserve more energy in the sensor nodes during transmission by detecting and preventing attack in the WSN. The average lifetime of the sensor node in the WSN that used the Modified was 54 minutes, where the lifetime of the sensor node in the WSN that used the traditional PLGP was 30 minutes.

The presence of the vampire attacks in the WSN decreases the delivery ratio to the destination node. The simulation results showed that the packet delivery ratio average of the generated packet was 2000 Bits Per Seconds (BPS), when the WSN used the modified PLGP. While, the packet delivery ratio when the WSN used the traditional PLGP was 1300 BPS as shown in Fig. 7.

V. Conclusion

WSN is used in many critical applications that are targeted from various malicious attacks. One of these is the vampire attack which has two kinds the carousal attack and stretch attacks. These vampire attacks consume all the power of the sensor nodes in the WSN and reduce the packet delivery ratio. The proposed technique has modified the PLGP protocol to consider the route energy of the intermediate nodes and the number of the broadcast packets of each node. In addition, the modified PLGP has initiated the discovery process of the PLGP and prevent and malicious node in the network from sending packets and prevent the loops in any route to the destination nodes by comparing the route energy and the number of the broadcast which should be less than the threshold value. The new proposed technique has been implemented using NS-3 simulation to compare the result of the modified PLGP with the original PLGP. All the simulation results showed that the modified PLGP has better performance in term of the nodes consumption speed and increasing the nodes lifetime. In addition, the packets delivery ratio is also calculated and compared between the two protocols, and the modified PLGP has also presented increasing the delivery ratio by 50% at the destination nodes.

Acknowledgment

The author is grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

References

[1] H. Abusaimeh, M. Shkoukani and F. Alshrouf, "Balancing the Network Clusters for the Lifetime Enhancement in Dense Wireless Sensor Networks," Arabian Journal for Science and Engineering, 2013.

[2] A. Mahafzah and H. Abusaimeh, "Optimizing Power-Based Indoor Tracking System for Wireless Sensor Networks using ZigBee," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9, no. 12, pp. 255-230, 2018.

[3] H. Abusaimeh, "Low Energy Consumption Rateinhome Sensors Using Prime Nodes," ARPN Journal of Engineering and Applied Sciences, vol. 13, no. 22, pp. 8738-8744, NOVEMBER 2018.

[4] V. Lokhande, S. DESHMUKH and S. SUTAR, "Vampire Attacks Prevention In Wireless Sensor Network," International Journal Of Current Engineering And Scientific Research (IJCESR), vol. 3, no. 1, 2016.

[5] P. Beaula, C. Anand and R. Gnanamurthy, "Defending Against Energy Draining Attacks in Wireless Sensor Networks with Secure Synchronization," International Journal of Science and Engineering Research (IJ0SER), vol. 3, no. 3, 2015.

[6] T. Sathyamorthi, D. Vijayachakaravarthy, R. Divya and M. Nandhini, "A Simple and Effective Scheme to find Malicious node in Wireless Sensor Network," International Journal of Research in Engg. And Tech., vol. 3, no. 2, 2014.

[7] A. Patil and R. Gaikwad, "Preventing Attack in Wireless Sensor Network by Using Trust Model," International Journal of Engineering Research & Technology (IJERT), vol. 4, no. 6, pp. 254-258, 2015.

[8] E. Y. Vasserma and N. Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," IEEE Transactions on Mobile Computing, vol. 12, no. 2, Feb 2013.

[9] K. Sivakumar and P. Murugapriya, "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 1, 2014.

[10] S. D. SoumyashreeMenasinakai, "Prevention and Detection of Vampire Attacks Problem in Wireless Ad-Hoc Sensor Network," in International Conference on Information and Communications Security Protocols, Hong Kong, 2014.

[11] B. Parno, M. Luk, E. Gaustad and A. Perrig, "Secure sensor network routing: A clean-slate approach," in he 2006 ACM Conference on Emerging Network Experiment and Technology, Lisboa, 2006.

[12] D. Verma, G. Singh and K. Patidar, "Detection of Vampire Attack in Wireless Sensor Networks," International Journal of Computer Science and Information Technologies, vol. 4, no. 6, 2015.

Author's Profile

Hesham Abusaimeh is an associate professor of computer science in the Middle East University, Jordan. He is also senior IEEE member in the Jordan Section. Dr. Abusaimeh received his B.Sc. and M.Sc. Degrees both in computer science from Applied Science University and New York Institute of Technology respectively. Dr. Abusaimeh has received his Ph.D. from Loughborough University in the UK in 2009 in computer networks. His research interest includes wireless sensor networks, routing protocols, cyber security, and energy-aware routing protocols in sensor networks. Nowadays, Dr. Abusaimeh is the Dean of Graduate Studies and Scientific Research and the Dean of International Programmes at the Middle East University.