Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

Article

An Anomaly Detection System for Vampire Attacks Crisis in Wireless Sensor Networks

G Kannan*, K Indragandhi, Midhat Jan

Department of Electronics & Communication Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India
E-mail: kannan@crescent.education

Received: 5 January 2024; **Revised:** 1 April 2024; **Accepted:** 9 April 2024

Abstract: One of the major crises to be addressed by Wireless Sensor Networks (WSN) is vampire attacks which disable the network connection by consuming node energy unnecessarily. Energy efficiency plays the prominent role in wireless sensor networks. In these networks many attacks are possible for energy draining at each sensor node. The proposed work investigates various resource consuming attacks called vampire attacks namely carousel and stretch attack which rapidly drain energy of a WSN node. It causes permanent disabling of WSN. These attacks are not protocol specific and it is hard to find out. The proposed work suggests Modified-PLGPa protocol to identify and remove the attacks to enhance network longevity. This protocol helps to reduce the effect of vampire attack by decreasing the energy loss caused by unwanted packet transmission in the network routing. The performance of the Modified-PLGPa protocol was demonstrated with the different types of vampire attack i.e., carousel attack and stretch attack. The experimental simulation result shows that overall residual energy and packet delivery ratio have been improved remarkably.

***Keywords*:** wireless sensor networks, crises, modified PLGP, energy efficiency, carousel and stretch attack

1. Introduction

A Wireless Sensor Network (WSN) is a distributed network system comprising a large number of spatially dispersed autonomous sensor nodes [1, 2, 3]. In the realm of computer networking, WSNs have garnered significant attention as a prominent research area. Thanks to advancements in the Internet of Things (IoT) and wireless communications, this field is experiencing a surge in interest, enabling the production of low-cost, miniature-sized sensors equipped with wireless networking capabilities [4, 5, 6]. The widespread deployment of WSNs across industries, military operations, and commercial sectors may pave the way for their ubiquitous presence [7, 8]. A wireless sensor network comprises a large number of tiny sensors dispersed across a geographical area. WSNs find extensive use in many applications where monitoring physical changes, as well as collecting and processing relevant data, are necessary [9, 10]. To ensure reliable operation in these applications, fault tolerance is critical in WSNs. Fault-tolerant mechanisms enable WSNs to maintain functionality despite failures of individual sensor nodes, communication disruptions, or other operational anomalies [11]. The architecture of a Wireless Sensor Network is depicted in Figure 1.

The attacks on Wireless Sensor Networks (WSNs) are typically categorized as routing depletion and resource depletion attacks [12, 13]. Routing depletion attacks impact critical networking features such as bandwidth and power delay. Resource

DOI: https://doi.org/10.37256/cnc.2120244226

depletion attacks, also known as vampire attacks, generate unnecessary network traffic through a vampire node, ultimately depleting the energy of nodes entirely [14, 15]. This can lead to the permanent disablement of nodes within the network. Vasserman and Hopper [16] conducted an analysis of vampire attacks and proposed various methods to mitigate them. Their study explored how these attacks manifest at the network layer, potentially leading to the permanent disablement of the entire network. It's worth noting that these attacks are not specific to any particular networking protocol but rather depend on various features of routing protocols. Also, it was found that almost every protocol is prone to these vampire attacks, and it is a very tedious process to discover them. Finally, it was concluded that a single vampire node could enhance energy utilization by a factor of O(N) throughout the network. Here, N represents the total number of sensor nodes in the network.

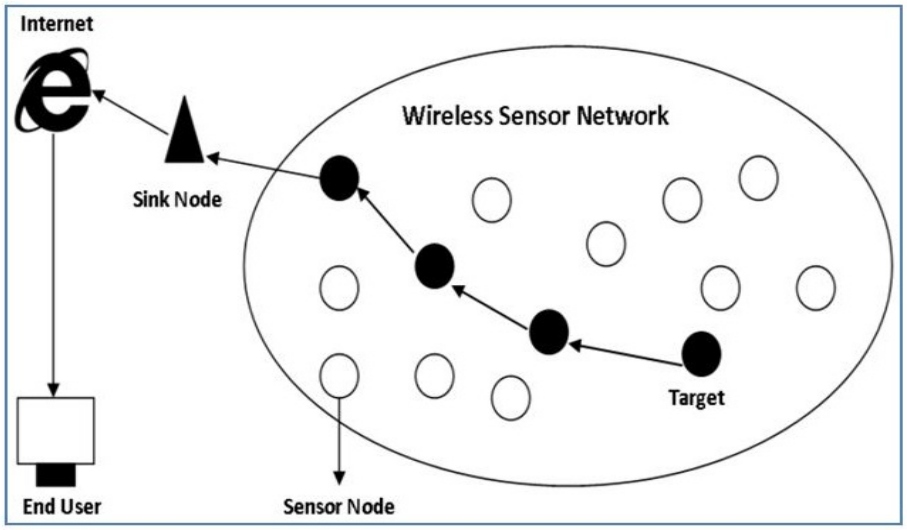


Figure 1. Scenario depicting WSN architecture

Jiang et al. [17] discussed the new emerging area of IoT, which is a global network of internet-connected objects based on standard communication protocols and having uniquely addressable virtual representations. The objects may include PCs, cell phones, RFID devices, and particularly WSNs. They are identified by a unique address, can join the network dynamically, and collaborate efficiently to attain tasks. Karlof et al. [18] considered security goals for routing protocols in WSNs. The major contributions of this paper are the analysis of attacks on wireless sensor network architecture. The authors described two novel attacks, namely Sinkhole and HELLO flood attacks, and proposed countermeasures for these crippling attacks. This paper concludes that secure routing plays an important role in utilizing sensor networks for many applications. Parno et al. [19] proposed the PLGPa protocol to mitigate the harm caused by vampire attacks during the forwarding phase. However, this paper does not provide a complete solution for vampire attacks during the topology discovery phase. To address this drawback, the authors proposed a modified PLGPa protocol to mitigate energy attacks in both phases.

2. Problem statement

Wireless Sensor Networks (WSNs) are increasingly deployed in remote areas, rendering them susceptible to a multitude of threats and attacks that compromise their functionality and deplete their battery resources [20]. Among these threats are energy or vampire attacks, which exploit vulnerabilities to drain the energy or battery life of individual nodes through various means. The primary objective of this proposed research is to conduct a comprehensive analysis of existing secure routing protocols within WSNs. This analysis aims to identify vulnerabilities and assess the potential impact of

energy attacks on these protocols. By thoroughly examining the implications of such attacks, the research endeavors to propose and develop a robust and energy-efficient solution to mitigate the risks posed by vampire attacks.

Through systematic investigation and evaluation, the study aims to contribute to the development of resilient WSNs capable of withstanding energy-based threats. By identifying weaknesses in current protocols and proposing effective countermeasures, the research seeks to enhance the overall security and longevity of wireless sensor networks in remote and vulnerable environments.

3. Energy attacks in WSN

Energy attacks are very tedious to identify and prevent because they use protocol-compliant messages. Numerous attacks were used by the attackers to drain the energy of WSN nodes. The proposed work focused on two types of attacks, namely Carousel Attack and Stretch Attack.

3.1 *Carousel attack*

In this attack, an unwanted packet is sent by the enemy with a route made of series of loops in order to traverse the same node many times Due to this approach; route length is increased more than the number of nodes existing in the network. Figure 2 illustrate this attack.

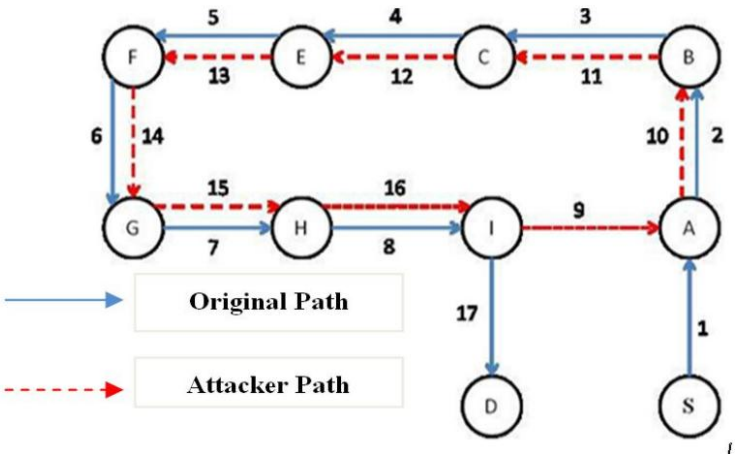


Figure 2. Carousel attack

In Figure 2, S represents source node, D indicates Destination node and the remaining nodes A, B, C, E, F, G, H and I represents intermediate nodes. Due to carousel attack, it forms continuous loop i.e., S, A, B, C, E, F, G, H, I and A instead of reaching from S, A, B, C, E, F, G, H, I to D.

3.2 *Stretch attack*

In this attack, a packet traverses more than optimal number of routes because of the malicious node which makes long source routes. Due to this attack, the routing path is increased as shown in Figure 3.

In Figure 3, S represents source node, D indicates Destination node and the remaining nodes A, B, C, E, F, G, H, I and J represents intermediate nodes. Due to Stretch attack, wrong and length path is introduced i.e., S, A, B, C, E, F, G, H, I, J and D instead of the optimum path S, J, D.

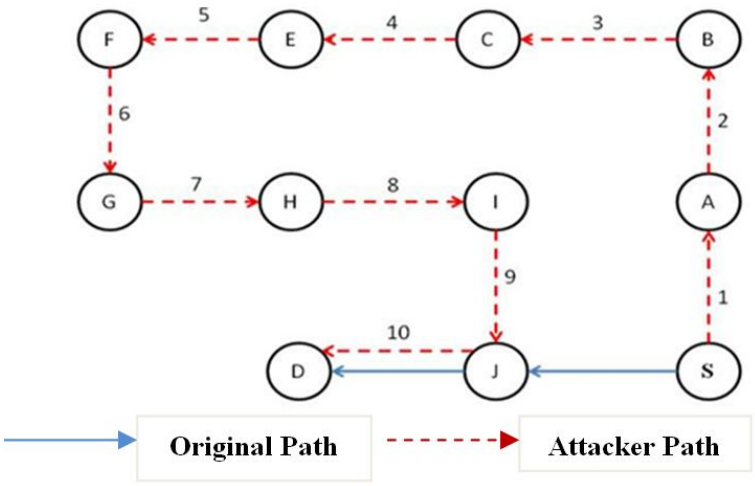


Figure 3. Stretch attack

4. Existing methods

The Provenance-based Data Possession and Secure Data Provenance (PLGP) protocol [19] is a clean-slate secure sensor network routing protocol designed to ensure secure data transmission by employing a path tracking technique. The protocol consists of two phases: topology discovery and packet forwarding. However, the original PLGP protocol does not satisfy the no-backtracking property, making it vulnerable to vampire attacks.

4.1 *PLGPa protocol*

To address the vulnerability of the PLGP protocol to vampire attacks, an extension called PLGPa [16] was proposed. In PLGPa, a verifiable path history is added to every PLGP packet, ensuring that the no-backtracking property is satisfied. While this solution is effective for the packet forwarding phase, it does not work in the topology discovery phase.

5. Proposed methodology

The proposed work mitigate the issues in existing methodologies and proposed Modified PLGPa scheme an improved energy efficient routing protocol to eliminate the impact of resource consumption attacks called vampire attacks. The pseudo code for the modified PLGPa protocol is shown in Figure 4, and the key features of the proposed modified PLGPa protocol are:

```
// Node initialization
initiateNode(isSource, isDestination)
// Route Discovery
routeDiscovery(src, dst):
    src.broadcastRouteRequest()
    if dst.receiveRouteRequest():
        dst.sendRouteReply(src)
    if src.receiveRouteReply():
        return buildRoute(src, dst)
// Data Transfer
sendData(src, dst, data):
    route = routeDiscovery(src, dst)
    data.SEED = src.id
    for node in route:
        if node.isVampire() or node.id != data.SEED:
            broadcastVampireAlert(node.id)
            return
        node.forwardPacket(data)
    dst.receiveData(data)
// Vampire Detection
isVampire(node):
    return vampireBehavior
broadcastVampireAlert(vampireId):
    for node in network:
        node.receiveVampireAlert(vampireId)
// Node actions
receiveVampireAlert(vampireId):
    updateRoutingTables(vampireId)
forwardPacket(data):
    nextNode = getNextNode(data.destination)
    nextNode.receivePacket(data)
```

Figure 4. Pseudo code for the proposed system

5.1 *Data transfer phase*

During the data transfer phase, a new field called “SEED” is added to the data packets. This field is used to verify the integrity of the routing path and detect potential vampire attacks.

5.2 *Vampire attack detection and mitigation*

If a malicious node attempts to introduce long routes or loops into the routing path, the next node in the path will detect the discrepancy by comparing the node ID with the SEED field in the data packet. Upon detecting a vampire attack, an alarm packet containing the ID of the malicious node is broadcasted to all other nodes in the network, allowing for the elimination of the malicious node and reducing energy consumption.

5.3 *Performance evaluation*

The performance of the proposed modified PLGPa protocol is evaluated by comparing it with the original PLGP protocol and the network under vampire attacks. The key performance metrics considered are Energy Levels and Packet Delivery Ratio

5.4 *System design in the presence of a vampire node*

The proposed system design addresses the scenario when a malevolent node, capable of launching vampire or energy attacks, is present within the network. If left unchecked, the presence of such a node can cause rapid depletion of network resources, leading to network failure.

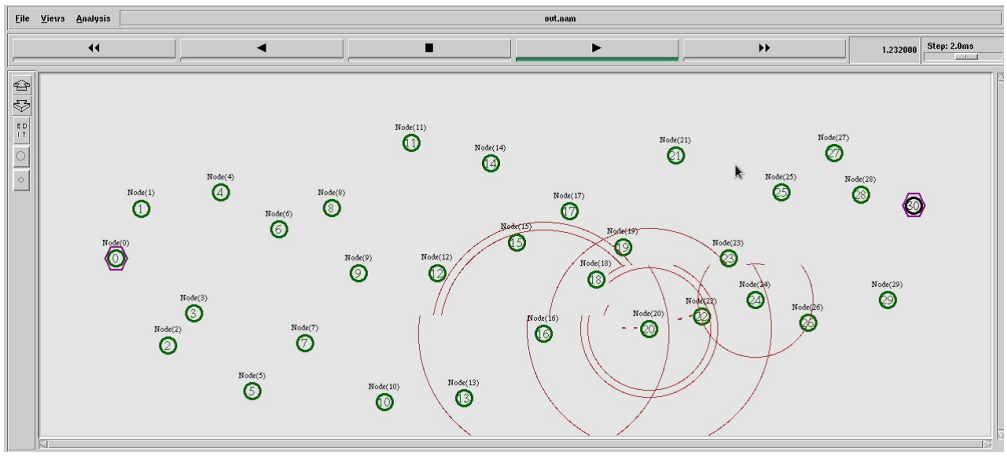
6. Experimental setup

This section elaborates the experimental setup to evaluate the performance of the proposed modified PLGPa mechanism using Network Simulator (NS-2) with Carousel and Stretch attacks. The initial energy of nodes is kept as 3J and these nodes are having non-renewable batteries. The experiment is done with 20 and 30 nodes. The energy of each node is utilized during the simulation. And once a nodes' energy is drained out it is considered as dead and after that it can't take part in communication. The results are obtained by extracting data from trace file generated after simulating tcl script using awk files. The different parameters configured in the simulator are shown in Table 1.

Table 1. Configuring simulation parameters in NS2

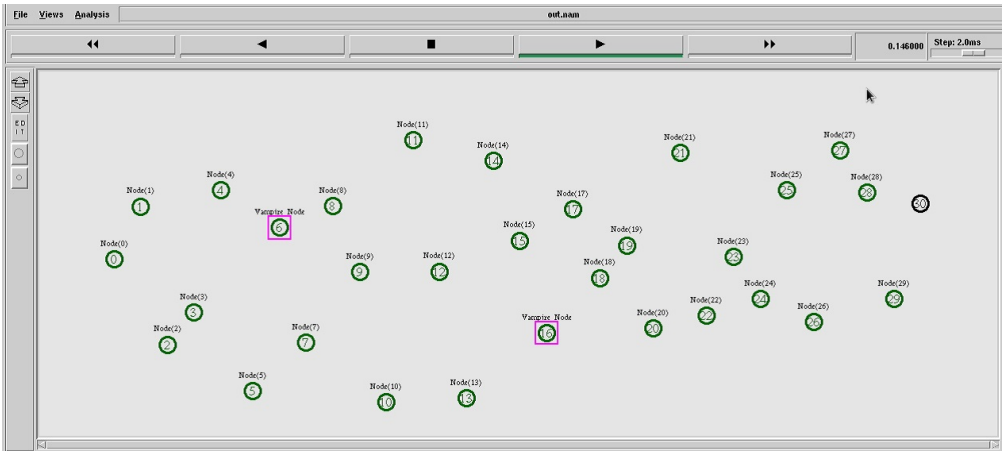
Parameters	Type/Value
Simulator Name	NS 2.34 version
Network Traffic	Constant Bit Rate
Channel	Wireless
MAC	802.11
Packet size (bytes)	512
Routing protocol	PLGP
Number of nodes	20 and 30
Initial node Energy (Joule)	3

Figure 5 illustrate the simulation setup and configuration made in NS2 simulator. Figure 5a deals with packet transmitted from source node to destination node with proposed modified PLGPa protocol. Figure 5b, shows random distribution of the vampire node across the network. Network Animator (NAM) output derived through animation tool to view the vampire attack is shown in Figure 5c. The screenshot of trace file output is visualized from Figure 5d.



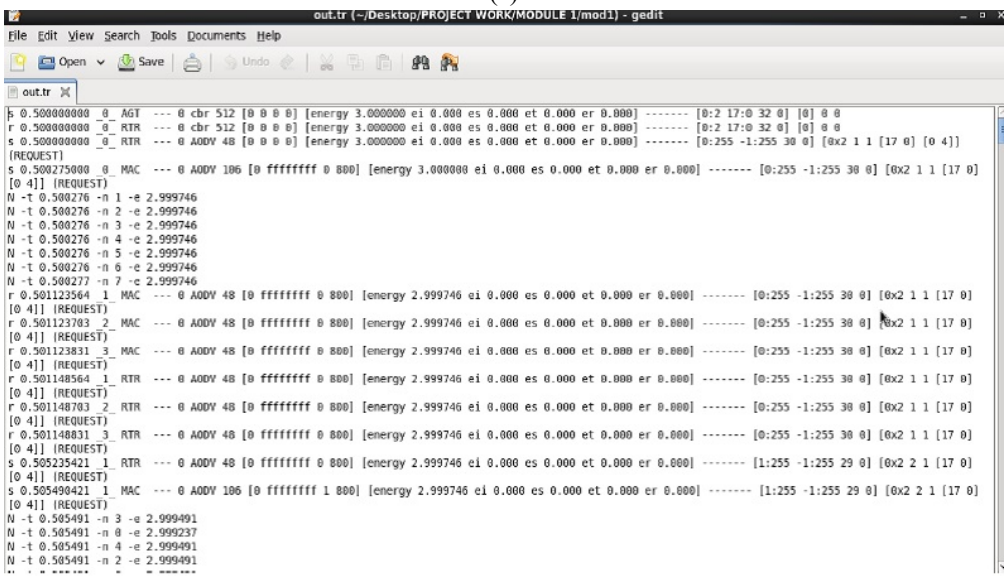
(a)

Figure 5. *Cont.*



(b)

(c)



(d)

Figure 5. Simulation setup (**a**) Packet Transmission from S to D; (**b**) Deployment of the vampire nodes in a sensor network; (**c**) NAM output showing implementation of Vampire Attacks; (**d**) Trace file output.

7. Performance estimation

The performance of the proposed modified PLGPa scheme is done with the following QoS parameters like energy consumption of the nodes, residual energy, average network energy and packet delivery ratio (PDR).

(1) Residual energy (E_{re}):

It can be defined as the energy level in a sensor network after each network perform data transmission phase.

$$E_{re} = E_{in} - \sum E_r \tag{1}$$

where, E_{re} is residual energy, E_{in} represents sensor node energy during the initial deployment and E_r is the energy consumption by the individual sensor node after a particular data transmission round.

(2) Average network energy (E_{av}):

$$E_{av} = \sum \frac{E_{re}}{n} \tag{2}$$

where, n indicates the total number of sensor nodes participated in the network.

(3) Total energy consumption (TEC):

This terminology represents the total amount of energy consumed by all the nodes in the network.

$$\text{TEC} = n\,(E_i - A_{re}) \tag{3}$$

whereas, n denotes number of nodes, E_i denotes initial energy of a node and A_{re} denotes the average residual energy.

(4) Packet delivery ratio (PDR):

It is the ratio of number of packets received (NPR) successfully to the total number of packets transmitted (NPT). The greater value of PDR is directly proportional to the performance of the protocol

$$\text{PDR} = \frac{\text{NPR}}{\text{NPT}} \tag{4}$$

8. Simulation results and analysis

The main goal of this proposed system is to develop a resilient energy protocol which will defend the vampire or energy attacks, so that network life would be increased in terms of energy. The analysis is performed for the various scenarios by considering without any attack and after launching vampire attacks in WSN. In Figure 6a, Energy consumption increases by 28.2116J and 25.4305J for Carousel Attack for 20 & 30 nodes respectively and overall energy consumption decreases by 12.9752J and 25.0063J for 20 and 30 nodes respectively in the proposed method. Hence, average energy consumption get increased by a factor of 1.41058J & 0.84769J per node for 20 & 30 nodes respectively. Similarly, In Figure 6b Energy consumption increases by 2.0194J & 24.3331J due to Stretch attack for 20 and 30 nodes respectively and Energy consumption is reduced by 1.9781J and 6.268J for 20 and 30 nodes respectively in proposed method. From the results, average energy consumption has been increased by 0.10097J & 0.21282J per node for 20 & 30 nodes respectively. From Figure 7a, it clearly visualize that due to the proposed system, the overall residual energy have been increased from

3.6707J to 16.6459J and 18.5032J to 43.5095 for 20 and 30 nodes respectively when the Carousel Attacks. Similarly from Figure 7b, overall residual energy has been increased from 29.8629J to 31.841J and 37.5492J to 43.8172J by considering 20 and 30 nodes respectively due to stretch attacks.

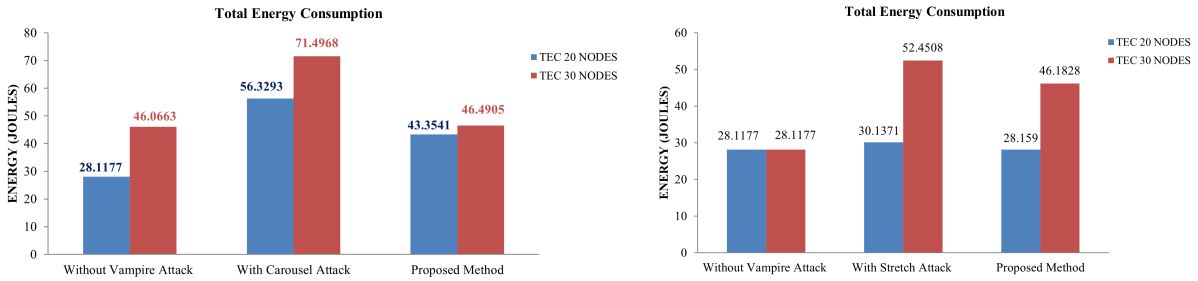


Figure 6. Total energy consumption without attack and with attack through proposed method for (**a**) carousel attacks (**b**) stretch attacks

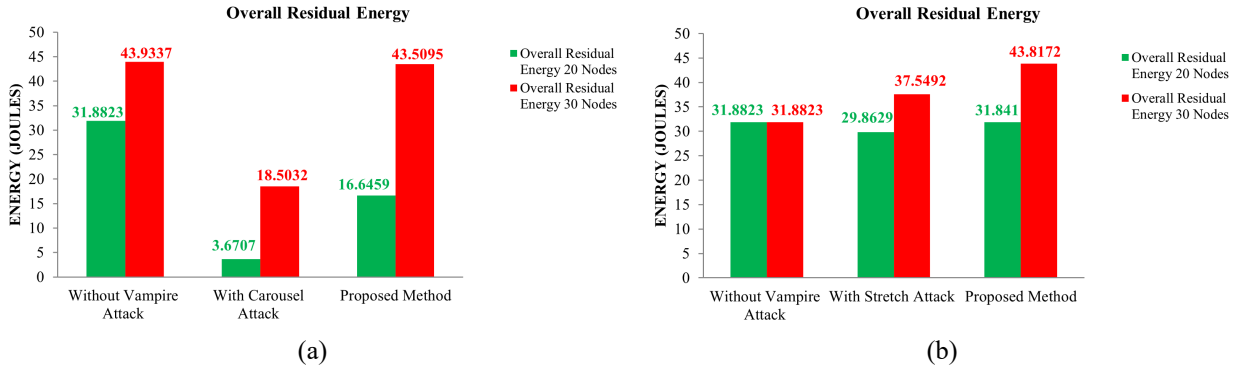


Figure 7. Overall residual energy without attack and with attack through proposed method for (**a**) carousel attacks (**b**) stretch attacks

Figure 8a, represents average residual energy is increased from 0.183537J to 0.832293J and 0.616775J to 1.45032J for 20 and 30 nodes respectively when the Carousel Attacks in the system. Correspondingly from Figure 8b, average residual energy is improved from 29.8629J to 31.841J by considering 20 and 30 nodes respectively due to stretch attacks.

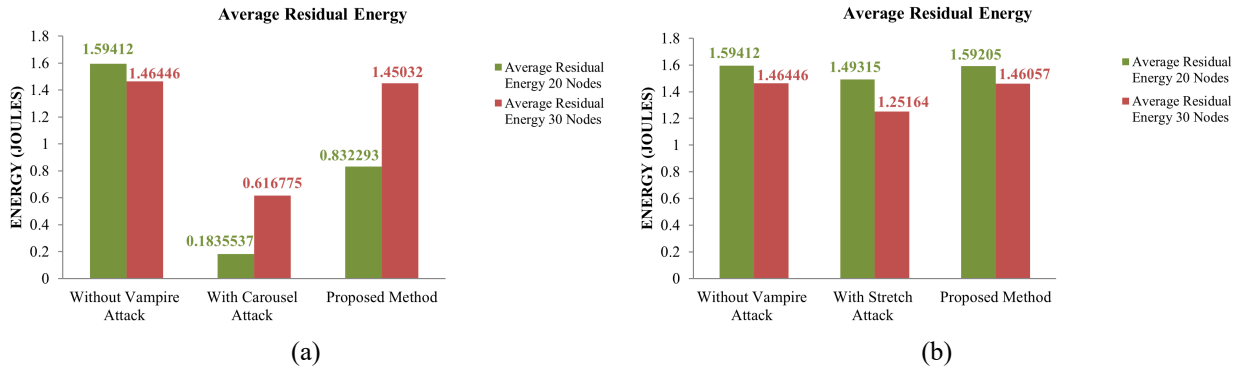


Figure 8. Average residual energy without attack and with attack through proposed method for (**a**) carousel attacks (**b**) stretch attacks

Figure 9 indicates the successful delivery of packet for the proposed method due to vampire attacks. From the experimental results it clearly depict that less number of packets are dropped due to stretch attack as compared to carousel attack as shown in Figure 9a,b.

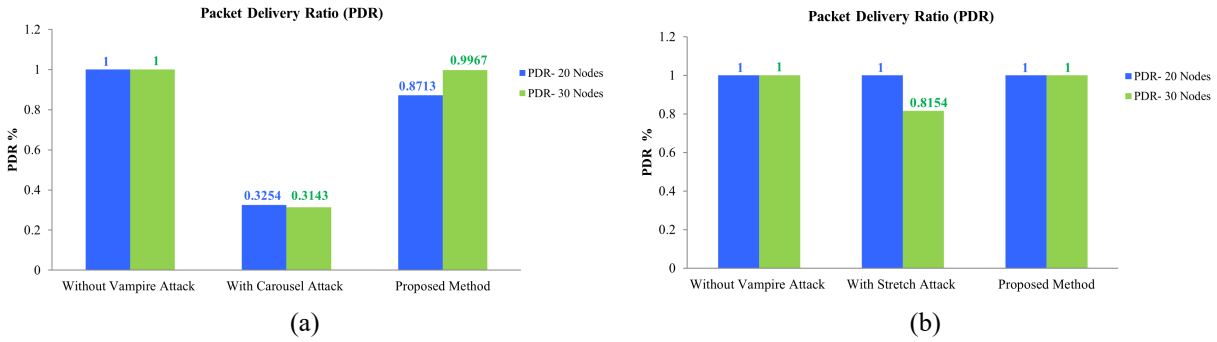


Figure 9. Packet Delivery Ratio (PDR) without attack and with attack through proposed method for (**a**) carousel attacks (**b**) stretch attacks

9. Conclusions

This paper mainly focuses on one of the critical issue of routing protocols which will disable WSN permanently by draining nodes' battery power called vampire energy attacks. Two types of vampire attacks i.e., Carousel & Stretch attacks were implemented and their impact on wireless sensor network was analyzed. From the experimental investigation it is shown, how the impact of these kind of attacks can be reduced with the help of proposed Modified-PLGPa protocol and in turn increases the network lifetime. This proposed resilient approach greatly reduces the energy consumed by WSN nodes due to vampire attacks. Hence the problem of vampire attacks in WSN can be mitigated significantly and network longevity has been enhanced. This work can be extended further in future to produce the best energy resilient protocol and will be emulated in real-time scenario, using actual hardware simulation. A quick self-healing or self-repair mechanism is much desirable, wherever possible to make sensor network nodes resilient from the undesirable crisis.

Conflict of interest

There is no conflict of interest for this study.

References

[1] C. Park, K. Lahiri, and A. Raghunathan, "Battery discharge characteristics of wireless sensor nodes: an experimental analysis," in *Proc. 2005 2nd Annu. IEEE Commun. Soc. Conf. Sens. Ad. Hoc. Commun. Netw.*, Santa Clara, CA, USA, Sep. 26–29, 2005, pp. 1–6, https://doi.org/10.1109/SAHCN.2005.1557096.

[2] A. Sinha and A. Chandrakasan, "Dynamic power management in wireless sensor networks," *IEEE Des. Test Comput.*, vol. 18, no. 2, pp. 62–74, 2001, https://doi.org/10.1109/54.914626.

[3] G. Kannan and T. SreeRenga Raja, "An Efficient Cluster-based Reliable Power Aware Scheme (RPAS) for Network Longevity in WSN," *WSEAS Trans. Comput.*, vol. 12, pp. 366–373, 2013.

[4] P. K. Jawahar, K. Indragandhi, G. Kannan, and Y.-W. Leung, "Development of a Secured IoMT Device with Prioritized Medical Information for Tracking and Monitoring COVID Patients in Rural Areas," in *Healthcare Monitoring and Data Analysis Using IoT: Technologies and Applications*, online: IET Digital Library, pp. 99–131, 2022, https://doi.org/10.1049/PBHE038E_ch6.

[5] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, https://doi.org/10.1109/access.2021.3094024.

[6] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, "Improved Deep Convolutional Neural Network based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, pp. 3272–3281, 2021, https://doi.org/10.1109/TNSE.2021.3098011.

[7] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data Collection for Security Measurement in Wireless Sensor Networks: A Survey," *IEEE Internet Things J.*, vol. 6, pp. 2205–2224, 2018, https://doi.org/10.1109/jiot.2018.2883403.

[8] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," *IEEE/ACM Trans. Netw.*, vol. 12, pp. 609–619, 2004, https://doi.org/10.1109/tnet.2004.833122.

[9] G. Kannan and T. S. R. Raja, "Energy efficient distributed cluster head scheduling scheme for two tiered wireless sensor network," *Egypt. Inform. J.*, vol. 16, pp. 167–174, 2015, https://doi.org/10.1016/j.eij.2015.03.001.

[10] R. Shah and J. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Proc. 2002 IEEE Wireless Commun. Netw. Conf. Record*, Orlando, FL, USA, Mar. 17–21, 2002, pp. 1–6, https://doi.org/10.1109/WCNC.2002.993520.

[11] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Fault tolerance techniques for wireless ad hoc sensor networks," in *Proc. 2002 IEEE SENSORS*, Orlando, FL, USA, Jun. 12–14, 2002, pp. 1–6, https://doi.org/10.1109/ICSENS.2002.1037343.

[12] W. Gu, X. Wang, S. Chellappan, D. Xuan, and T. H. Lai, "Defending against search-based physical attacks in sensor networks," in *Proc. IEEE Int. Conf. Mobile Adhoc. Sens. Syst. Conf.*, Washington, DC, USA, Nov. 7, 2005, pp. 1–6, https://doi.org/10.1109/MAHSS.2005.1542839.

[13] Z. Alansari, N. B. Anuar, A. Kamsin, and M. R. Belgaum, "A systematic review of routing attacks detection in wireless sensor networks," *Peer J. Comput. Sci.*, vol. 8, e1135, 2022, https://doi.org/10.7717/peerj-cs.1135.

[14] W. K. Seah, A. C. Valera, P. W. Lee, and Y.-F. Wong, "Topology Skewing for Improved Route Selection in Wireless Multi-hop Networks," in *Proc. 2012 45th Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, Jan. 4–7, 2012, pp. 1–6, https://doi.org/10.1109/HICSS.2012.595.

[15] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 4, pp. 54–62, 2002, https://doi.org/10.1109/mc.2002.1039518.

[16] E. Y. Vasserman and N. Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 12, pp. 318–332, 2011, https://doi.org/10.1109/tmc.2011.274.

[17] Y. Jiang, L. Zhang, and L. Wang, "Wireless Sensor Networks and the Internet of Things," *Int. J. Distrib. Sens. Networks*, vol. 9, 2013, https://doi.org/10.1155/2013/589750.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Netw.*, vol. 1, pp. 293–315, 2003, https://doi.org/10.1016/s1570-8705(03)00008-8.

[19] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure sensor network routing," in *Proc. 2006 ACM CoNEXT Conf.*, Lisboa, Portugal, Dec. 4–7, 2006, pp. 1–6, https://doi.org/10.1145/1368436.1368452.

[20] J. Li and G. Gao, "Analysis of Energy Consumption for Ad Hoc Wireless Sensor Networks Using a Bit-Meter-per-Joule Metric," *IPN Progress Report*, vol. 42, pp. 1–19, 2002.