Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: February, 2023 **2023, 20(5): 1817-1824** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2023.7161

Impacts of Denial-of-Service Attack on Energy Efficiency Pulse Coupled Oscillator

Faisal Osman Hassan [1] ***Nasrina M Samir*** [2] ***Zurina Mohd Hanapi*** [2*]

[1] Faculty of Information Communication Technology (ICT), University of Burao, Market Burao TG. Burao, Somaliland.
[2] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysia.
*Corresponding author: zurinamh@upm.edu.my
E-mail addresses: faisel.osman1@gmail.com , gs59090@student.upm.edu.my

Received 18/4/2022, Revised 2/11/2022, Accepted 3/11/2022, Published Online First 20/2/2023, Published 1/10/2023

Abstract:

The Pulse Coupled Oscillator (PCO) has attracted substantial attention and widely used in wireless sensor networks (WSNs), where it utilizes firefly synchronization to attract mating partners, similar to artificial occurrences that mimic natural phenomena. However, the PCO model might not be applicable for simultaneous transmission and data reception because of energy constraints. Thus, an energy-efficient pulse coupled oscillator (EEPCO) has been proposed, which employs the self-organizing method by combining biologically and non-biologically inspired network systems and has proven to reduce the transmission delay and energy consumption of sensor nodes. However, the EEPCO method has only been experimented in attack-free networks without considering the security elements which may cause malfunctioning and cyber-attacks. This study extended the experiments by testing the method in the presence of denial-of-service (DoS) attacks to investigate the efficiency of EEPCO in attack-based networks. The result shows EEPCO has poor performance in the presence of DoS attacks in terms of data gathering and energy efficiency, which then concludes that the EEPCO is vulnerable in attack-based networks.

Keywords: Biologically and non-biologically inspired network, Denial-of-service, Pulse coupled oscillator, Security, Transmission state, Wireless sensor network.

Introduction:

Wireless sensor networks (WSNs) consist of various autonomous devices, so-called sensor nodes (SN). The SNs have communication capabilities that can sense, process, and transmit data to the sink or base station[1]. Every SNs must act synchronized because the synchronization can save energy and impact the appropriate activity of sensors that assess time-sensitive actions[2]. Furthermore, the observation of natural phenomena regarded as the best source of information for spontaneous synchronization which closely match the WSN responses and tend to coordinate the power cycles to reduce the energy consumption. Thus, pulse coupled oscillators (PCOs) are the techniques inspired by biology suited to WSN for inner synchronization and model accurately complex network phenomena[3,4]. Nevertheless, the battery constraint caused the PCO model to be unsuitable for sensor networks, especially for simultaneous transmission and data reception[5]. Therefore, it is the primary concern to design an energy-efficient control mechanism in WSNs.

Due to the distributed and unattended environment, WSNs are incredibly vulnerable to attacks, making it vitally important to study synchronization in the presence of attacks. There are two types of attacks in a transmission medium environment: active attacks and passive attacks. Active attack is the attacks which aim to find and destroy the information. Denial-of-Service (DoS) attacks, jamming attacks, and tampering attacks, to mention a few, are examples of active attacks. In contrast, passive attack is the attacks which aim to steal valuable information such as passwords and confidential data. Passive attacks include traffic analysis, camouflage adversaries, monitoring and eavesdropping, etc[6]. Most of the energy-efficient

PCO models assumed that every oscillator operates correctly without any node compromised by malicious attacks, which may lead to ultimately corrupting an oscillator and taking over its behavior[7].

The rest of this paper is organized as follows: The related works on transmission scheduling mechanisms were presented in section two. Section three explains the EEPCO scheme without and with attacks. The implementation of security analysis has been detailed in section four. Finally, the last two sections are the result and discussion and the paper is concluded with some suggestions for future works.

Related Works:

The transmission scheduling mechanism has two categories: non-biologically inspired and biologically inspired network systems [8,9]. This study concentrates on the PCO model that utilizes firefly synchronization to attract mating partners for modeling the WSN. The energy-efficient of PCO on transmission scheduling is often applied in WSNs since it considers packet collision avoidance using a self-organizing method. The synchronization strategy by reducing idle listening during the oscillation period has been proposed which added the refractory period [10]. This makes a sensor able to avoid transmitting/receiving any signal, and it can deactivate its transceiver and switch to a sleep mode. The sensor turned off the radio and ignored the arrival signal, hence reducing the energy consumption. Moreover, the travelling wave pulse coupled oscillator (TWPCO) [11] based on the phase locking of the PCO model has been proposed which imitate the synchronization behavior of fireflies where the emission of radio signals represents firing. The method aims to avoid the deafness problem, thus improving data gathering and energy efficiency.

The TWPCO was then modified to reduce the delay and energy constraint, which introduced a random traveling wave pulse coupled oscillator (RTWPCO) [12] scheme. RTWPCO employs the same method as TWPCO in phase locking, and the improvement was made using the random method on anti-phase in the PCO model. Integrating both phases avoid unnecessary contact among sensors and simultaneously sustains the same hop count. Furthermore, an energy-efficient pulse coupled oscillator (EEPCO) [13] employed the self-organizing method, combining biologically inspired network systems and non-biologically inspired network systems. Phase-locking in TWPCO and anti-phase in a time division multiple access (TDMA) in the PCO model were utilized. As a result, it improves energy efficiency by avoiding packet collisions in the transmission state.

However, all the proposed schemes mentioned above are implemented in attack-free networks, assuming that all oscillators behave correctly and the all nodes are not compromised by malicious attackers. Thus, these schemes might be vulnerable when compromised nodes act maliciously to corrupt the phase synchronization of PCO. The present research on the attack-resilient synchronization algorithms in the PCOs model considers the synchronizability of PCOs in the presence of Byzantine attacks [14- 16]. Byzantine attack is the attack performed by a fully trusted node that's turned rogue and will passed all the authentication and verification phases. Therefore, those nodes can easily perform DoS attacks to avoid the other nodes from communicating in the media access control (MAC) layer and disrupt the communications [17]. DoS attacks can cause the malfunctioning of service which led to some disruption such as physical destruction, corrupted memory, or failures with no recovery and its aftereffect may last long [18]. Due to this matter, the EEPCO[13] scheme is used as a benchmark in this study to investigate the resiliency of EEPCO in attack-based networks with the presence of DoS attack in the transmission states. The security analysis for the simulation was conducted using java simulator to evaluate the impacts of DoS attack in EEPCO in terms of data gathering and energy efficiency.

Materials and Methods:

Even EEPCO has been proven to be energy efficient, but when there is an attacker in the network, SN could be died early, as the node might need to respond to the illegal operation. Consequently, it is also vital to investigate the EEPCO in the attack-based scenario in the presence of a DoS attack. The EEPCO scheme without and with DoS attack is evaluated for a fair comparison. The EEPCO scheme is explained as follows:

A. EEPCO Scheme without Attack

The EEPCO employs both biologically and non-biologically inspired network systems. This is due to the neglection of packet collisions in biologically inspired networks, which are then improved by introducing a non-biologically inspired network to counteract the packet collision, reducing energy consumption and increasing data gathering during transmission. Two patterns of synchronous firefly behavior in the PCO model are used in this method: phase and anti-phase locking.

Biologically inspired network system based on phase locking

Given a set of *N* oscillators $\emptyset_i$, where 1≤i≤N, each oscillator relates with a phase such that $\emptyset_i \in [\mathbf{0}, \boldsymbol{T}]$. *T* is the upper bound to shift the oscillator $\emptyset_i$ thus it fires before oscillator $\emptyset_i$ returns to zero. At the same time, the simulation is launched by coupling the oscillator $\emptyset_j$ with the firing oscillator $\emptyset_i$. This shifts the corresponding phase $\emptyset_j$ by an infinitesimal amount $\Delta(\emptyset_j)$,where $\emptyset_j = \Delta(\emptyset_j) + \emptyset_j$. Thus, the total $\Delta(\emptyset_j)$ is given by

$$\emptyset_j = \Delta(\emptyset_j) + \emptyset_j \quad \ldots 1$$

$\Delta(\emptyset_j)$ is equivalent to the PRC, used by experimentalists to measure the system behavior regardless the underlying mechanisms in charged for the behavior[8]. The travelling wave equation is used to present PCO firing. Then, to proof the Eq. 1, quadratic integrate and fire (QIF)[19] and the radial isochron clock model (RIC) [19] and PRC [20] function are utilized and developed the model as below:

Quadratic Integrate and Fire (QIF) model

$$\Delta_{QIF}(\emptyset) = \boldsymbol{PRC_a}(\mathbf{1} - \boldsymbol{cos}(\mathbf{2}\boldsymbol{\pi}\emptyset)) \quad \ldots 2$$

where $\boldsymbol{PRC_a} = \mathbf{0.5}, \mathbf{1.0}, -\mathbf{0.5}$. Once $\boldsymbol{PRC_a}$ approach a value equal to 1, then the PRC becomes singular.

Radial Isochron Clock (RIC) model

$$\Delta_{RIC}(\emptyset) = -PRC_a * sin(2\pi\emptyset) \quad \ldots 3$$

where $PRC_a = 0.5, 1.0, -0.5$. It should be emphasised that the oscillator in the QIF and RIC models ignores all stimuli at the moment of firing and treats multiple stimuli received concurrently as a single stimulus.

The PRC function satisfies

The developed equation is based on the TWPCO model as follow:

$$\begin{cases} 0 < \Delta(\emptyset) \leq 1 - \tau - \emptyset & (0 \leq \emptyset < 1 - \tau) \\ \Delta(\emptyset) = 0 & (\emptyset = 1 - \tau) \\ 1 - \tau - \emptyset \leq \Delta(\emptyset) < 0 & (1 - \tau < \emptyset < 1) \end{cases} \quad \ldots 4$$

Hence, from Eq. 3 and Eq. 4, the new equation is generated as

$$\Delta_s(\emptyset) = -PRC_a * sin\frac{\pi}{1-\tau} * \emptyset + PRC_b(1 - \tau - \emptyset) \quad \ldots 5$$

Also, from Eq. 2 and Eq. 4, another new equation is formed as

$$\Delta_s(\emptyset) = PRC_a * cos\frac{\pi}{2(1-\tau)} * \emptyset + PRC_b(1 - \tau - \emptyset) \quad \ldots 6$$

where $PRC_a(-\frac{PRC_b(1-\tau)}{\pi} < PRC_a \leq \frac{(1-PRC_b)*(1-\tau)}{\pi})$ and $0 < PRC_b \leq 1$ are the main requirement to determine the characteristic of PRC. Therefore, Eq. 6 represents the TWPCO equation scheme. The TWPCO phase is then modified by applying Eq. 6 in Eq. 1 and catalyze the SN as:

$$\emptyset_j = \emptyset_j + PRC_a * cos\frac{\pi}{2*T} * \emptyset_j + PRC_b * (T - \emptyset_j) \quad \ldots 7$$

During the phase of its timer, each sensor broadcasts the data it has collected. The network adjusts the phase of its timer whenever a sensor picks up any transmissions from another node. Finally, SN cooperate with their neighbor's node to reach the phase-locking state, in which the sensor data are released. The timing of an emitted message is now seen to be a travelling wave phenomenon that either aims to gather or disseminate information from or to all SN. Overall, this biologically inspired network system is where the node uses the travelling wave phenomenon to catalyse and modify its phase.

Non-biologically inspired network system based on anti-phase locking

Non-biologically inspired network system utilized the TDMA protocol which includes the desynchronization method (DESYNC) and the anti-phase of the PCO model. The desynchronization will be accomplished when the SN is communicating with other SN, ensuring that all the SN are linked altogether. Given a set of N oscillators $\emptyset_i$, in DESYNC, where $1 \leq i \leq N$, each oscillator associated with a phase such that $\emptyset_i \in [0, T]$. *T* is the upper bound to shift the oscillator $\emptyset_i$ thus it fires before oscillator $\emptyset_i$ returns to zero. Then, the simulation is launched by coupling the oscillator $\emptyset_j$ with the firing oscillator $\emptyset_i$. If the reception of control packet is not the first time after the broadcast of node n_j, it simply records the previous phase difference $\Delta_j^{prev} = 1 - \emptyset_j$. Otherwise, it records the next phase difference $\Delta_j^{next} = \emptyset_j$, and changes its phase $\emptyset_j$ as:

$$\Delta_j = (1 - \alpha) * \emptyset_j + \alpha * \emptyset_j^{mid} \quad \ldots 8$$

where α represents the speed of assemblage, $\emptyset_j^{mid}$ is the destination phase of sensor node n_j which determine as:

$$\emptyset_j^{mid} = \frac{\Delta_j^{prev} + \Delta_j^{next}}{2} \quad \ldots 9$$

EEPCO Mechanism

The EEPCO mechanism is divided into two main parts. Firstly, the mechanism utilized the phase-locking of the TWPCO scheme in order to organize the SN from the source node to the destination during the transmission, as observed in the flashing synchronization behaviour of fireflies. Secondly, the mechanism used the DESYNC scheme to counteract packet collision by allowing the SN through self-organization and allocating equally spaced time slots.

After generating the SN packets, the radio range is determined to check for the range of SN by considering the distance's equation as below:

$$d = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2} \quad \ldots 10$$

If all the SN packets are verified under the same radio range, equals to 50, then the neighbour of SN packets is registered. All the required parameters are initialized, such as the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) model. This paper concerned on three main mechanisms: energy consumption operation, transmitting operation, and receiving operation.

- ***Energy consumption operation***

  To obtain the energy consumption of SN, the sleep, idle, transmit, and receive mode of the SN is evaluated using the equations below:

Sleep mode:

$$ConsumEnergy = E_{sleep} * advphase \quad \ldots 11$$

Idle mode:

$$ConsumEnergy = E_{idle} * advphase \quad \ldots 12$$

Transmit mode:

$$ConsumEnergy = E_{TX} * \frac{Packet_{size}}{Data_{rate}} \quad \ldots 13$$

Receive mode:

The receive mode is obtained from listening and receiving period.

Listening

$$ConsumEnergy = E_{RX} - E_{idle} * CCA_{Duration} \quad \ldots 14$$

Receiving

$$ConsumEnergy = E_{RX} - E_{idle} * \frac{Packet_{size}}{Data_{rate}} \quad \ldots 15$$

- ***Transmitting operation***

  The SN behavior is the performance of the sent message per cycle in the condition where the nodes is stable. The SN depends on the current phase $\emptyset_i$ and receives the messages from the neighboring nodes. Table 1 describes the SN state in transmitting operations.

Table 1. SN states in transmitting operation

SN state	Phases
Wake up	Wake up state for SN is when $\emptyset_i = T - \tau^{max}$.Node empties the transmission's message of timing table and waits the message from the neighbor node.
Message reception from the same hop nodes	Node adds new entry into its data transmission timing table after receiving message from other nodes.
Message transmission	If the phase $\emptyset_i = T$, node transmit a broadcast packet during wake up state in the transmission range. The phase $\emptyset_i$ is reset to zero when T is reached.
Message reception from upstream nodes	Node remains in wake up state upon resetting to zero and adjusts and shifted its phases.
Message reception from downstream nodes	A new entry is made in the node's data transmission timing table and newly received data is added to its overall data.

- **Receiving Operation**

If the node does not get any entries in its message transmission timing table, it will create a new entry in the table; otherwise, the node will overwrite the entry if the condition is satisfied. Moreover, when phase $\emptyset_i$ reaches T^{max}, node is stimulated and updates its offset. In contrast, the node needs to wait for another simulation. Node is associated with τ_i^{prev} and τ_i^{next} as follows:

$$\tau_i^{prev} = \tau \epsilon T_{i,t}^{max} < \tau_i^{trans^t} \quad \ldots 16$$

$$\tau_i^{next} = \tau \epsilon T_{i,t}^{min} < \tau_i^{trans^t} \quad \ldots 17$$

where T_i is the set of time for estimating transmission message. Both τ_i^{prev} and τ_i^{next} will be assumed to be zero if they are not attained and the offset τ_i is adjusted based on the following relation:

$$T_i = (1 - \alpha) * T_i + \alpha * T_i^{mid} \quad \ldots 18$$

$$\begin{cases} \frac{T_i^{prev} + T_i^{next}}{2} & if\ \tau_i^{next} > \tau_i^{prev} > 0 \\ \frac{T_i^{prev}}{2} & if\ \tau_i^{next} = 0, \tau_i^{prev} > 0 \\ T^{max} & otherwise, \end{cases} \quad \ldots 19$$

$$T_i^{prev} = \tau_i^{stim} - \tau_i^{prev}$$
$$T_i^{next} = \tau_i^{stim} - \tau_i^{next}$$

B. EEPCO Scheme with DoS Attack

This study mainly focuses on the performance of EEPCO in attack-based networks regarding data gathering and energy efficiency by using two scenarios: sets 10, 20, 30 up to 100 number of SN and number of SN equal to 30. The security analysis was implemented by designing the EEPCO scheme with a DoS attack, as shown in Fig. 1.

The malicious node attempts to enter the node connection and desynchronizes the sensor node connectivity. When the number of SN increases, the malicious node can desynchronize the SN connection and seize network control. Since a DoS attack was performed, the back-off procedure was violated and caused the CSMA/CA interruption. The attacker takes the priority to send Request-to-send (RTS) to interrupt the back-off procedure. When this happens, the attacker is able to initiate the RTS broadcast. Then, the attacker tries to act normally by following all the protocol's procedure as the attacker still need to follow the same control messages (RTS, CTS, and ACK). The other nodes in the network does not realize the presence of the attack since the EEPCO scheme does not provide any security detection method. The result of the simulation compared the EEPCO scheme with no attack and EEPCO scheme with DoS attack.

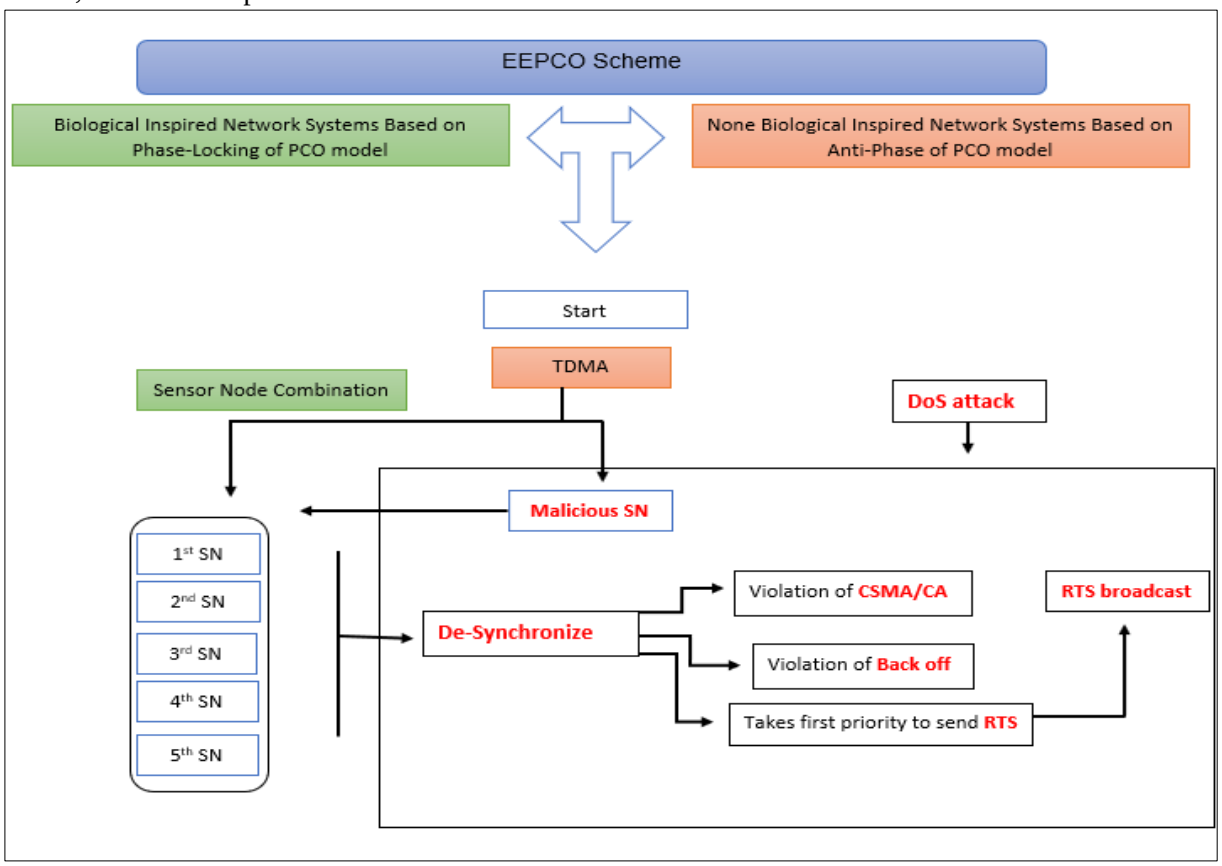

Figure 1. EEPCO scheme with DoS attack

Implementation:

The experimental simulation was carried out using a java simulator, Java simulation version 4.2.2, and a laptop of Intel® Core, i7-8550U CPU @ 1.80GHz, 8 GB of RAM (Windows 10). Table 2 shows the simulation parameters applied in this study. The SN is randomly deployed in a fixed 100*100 m^2 field with the centered base station in the field. The Omni-directional transmission radius is set up within 50 m. Two performance metrics were measured: data gathering ratio and energy efficiency ratio.

Data gathering ratio: total of SN data obtained at the base station per cycle. The equation is:

$$DataGathering = \frac{\sum_{i=1}^{n} Topck_{sink}}{SNC} \quad \ldots 20$$

where n is the number of SN in the network, $Topck_{sink}$ is the number of packets collected for each SN and SNC is the number of SN per cycle.

Energy efficiency ratio: energy consumed by the number of packets collected by the sink node. The equation is:

$$EnergyEfficiency = \frac{\sum_{i=1}^{n} ToEnc(i)}{Topck_{sink}} \quad \ldots 21$$

where $ToEnc(i)$ refer to the total energy consumed by each SN.

Table 2. Simulation parameters

Parameter	Value

Channel Frequency	2.4 GHz
Initial Energy	100 joules
Idle Power	60 µ W
Transmit Power	52.2 µ W
Receive Power	59.1 µ W
Sleep Power	3 µ W
Data Rate	250 kbps
Energy Model	MICAz
MIN_TIME_STEP	0.00001

Results and Discussion:

First scenario: 10, 20, 30 up to 100 SN

The first scenario selected 10, 20, and 30 up to 100 as the number of SN at each time. Fig. 2 shows the result of the impact of the EEPCO scheme in attack free and with the presence of DoS on data gathering ratio, respectively. Both mechanisms affect the data gathering performance with the increasing number of SN. The data gathering ratio drops dramatically when the number of SN exceeds 20 in EEPCO with DoS attack compared to EECPO with no attack. Moreover, the energy consumption increases simultaneously after the attacker successfully executes the attack. It can be seen starting from 40 SN until it reaches 100 SN, where the impact of DoS attack started to appear, as shown in Fig. 3. This is because the attacker has adequate time to desynchronize the SN connection as the number of SN increases while seizing control of the network connection, thus reducing the number of received packets and consuming more energy.

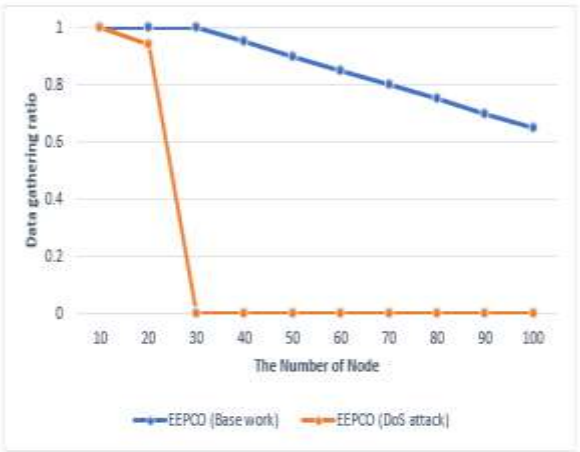

Figure 2. Impact on data gathering ratio

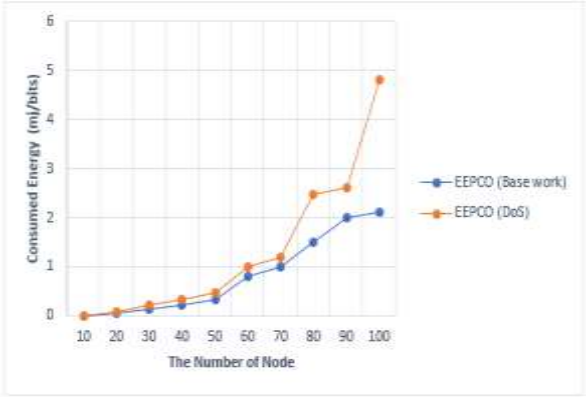

Figure 3. Impact on energy efficiency

Second scenario: 30 SN only

The second scenario compared the performance of both schemes when the number of SN was fixed to 30, which is based on data packet size. The data gathering ratio decreases when both mechanisms have bigger data packet sizes. As presented in Fig. 4, the data gathering ratio of EEPCO with DoS attack begins to decline when data packet size exceeds 20B and finally reaches zero percentage. The energy consumption also gradually increases for EEPCO with DoS attack compared to EEPCO without attack, as shown in Fig. 5. The presence of DoS attack in the EEPCO scheme needs more forwarding nodes to meet the desired network lifetime during the communication process. Since the number of SN is fixed to 30, the retransmission might frequently occur before the packet is discarded, which wastes many resources such as SN memory and the node's energy.

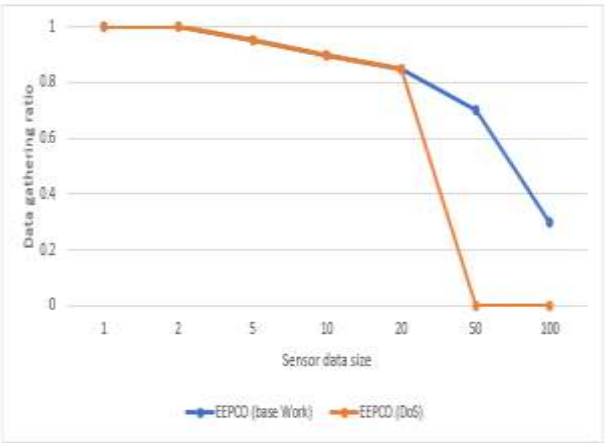

Figure 4. Impact on data gathering ratio

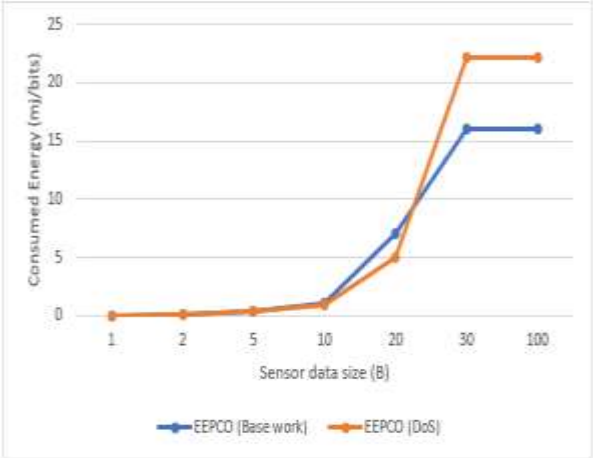

Figure 5. Impact on energy efficiency

Conclusion:

The EEPCO scheme has proven to improve the data gathering and energy efficiency in the attack-free network. However, after the security analysis implemented in this study, the result showed that the EEPCO scheme has poor performance where it is vulnerable to DoS attacks in terms of data gathering and energy efficiency. Two scenarios were involved where the number of SN was tested in the range of 10, 20, 30 up to 100 SN and the number of SN equal to 30, respectively. The presence of DoS attack makes the attacker seize control of the network connection. Moreover, maximum retransmission might occur, which wastes many resources. For future work, a lightweight authentication method can be employed for the EEPCO scheme to authorize the nodes to improve their performance.

Acknowledgment:

This work was supported by Geran Putra Berimpak Universiti Putra Malaysia, Vote Number 9659400.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in Universiti Putra Malaysia, Malaysia.

Authors' contributions statement:

F.S.H participated in designing the study, acquisition and analysis of data. N.M.S participated in the interpretation and conception of the study. Z.M.H participated in revision and proofreading of the manuscript. All the authors contribute in drafting the manuscript, reading and approving the manuscript.

References:

1. Saeedi IDI, Al-Qurabat AKM. Perceptually Important Points-Based Data Aggregation Method for Wireless Sensor Networks. Baghdad Sci.J. 2022Aug.1; 19(4): 0875. https://doi.org/10.21123/bsj.2022.19.4.0875
2. Al-Mekhlafi ZG, Hanapi ZM, Shamsan Saleh AM. Firefly-Inspired Time Synchronization Mechanism for Self-Organizing Energy-Efficient Wireless Sensor Networks: A Survey. IEEE Access. 2019; 7: 115229–115248.
3. Cui L, Cao J, An Z, Yang Y, Guo Q. Research on time synchronization of linear pulse-coupled oscillators model with delay in nearest neighbor wireless multi-hop networks. Int J Distrib Sens Netw. 2021 Jul; 17(7).
4. Zong Y, Dai X, Gao Z, Binns R, Busawon K. Simulation and evaluation of pulse-coupled oscillators in wireless sensor networks. Syst Sci Control Eng. 2018 Jan 1; 6(1): 337–49.
5. Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA, Hashim F, Saleh AMS. Impact of the Deafness Problem on Clock Synchronization in a Wireless Sensor Network. Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems. 14. 2014 Sept; 127–132. https://dl.acm.org/doi/10.1145/2668260.2668261
6. Keerthika M, Shanmugapriya D. Wireless Sensor Networks: Active and Passive attacks Vulnerabilities and Countermeasures. Glob.Transit. Proc. 2021 Aug; 2(2): 362-367.
7. Wang Z, Wang Y. Attack-Resilient Pulse-Coupled Synchronization. IEEE Trans Control Netw Syst.. 2019 Mar; 6(1): 338–51.
8. Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA. A Firefly-Inspired Scheme for Energy-Efficient Transmission Scheduling Using a Self-Organizing Method in a Wireless Sensor Networks. J Comput Sci. 2016 Oct 1; 12(10): 482–494.
9. Alshudukhi JS, Al-Mekhlafi ZG, Alshammari MT, Mohammed BA. Desynchronization Traveling Wave Pulse-Coupled-Oscillator Algorithm Using a Self-Organizing Scheme for Energy-Efficient Wireless Sensor Networks. IEEE Access. 2020; 8: 196223–34.
10. Wang Y, Nunez F, Doyle FJ. Energy-Efficient Pulse-Coupled Synchronization Strategy Design for Wireless Sensor Networks Through Reduced Idle Listening. IEEE Trans Signal Process. 2012 Oct; 60(10): 5293–5306.
11. Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA. Travelling Wave Pulse Coupled Oscillator (TWPCO) Using a Self-Organizing Scheme for Energy-Efficient Wireless Sensor Networks. PLOS ONE. 2017 Jan 5; 12(1).
12. Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA, Shamsan Saleh AM. Random traveling wave pulse-coupled oscillator algorithm of energy-efficient wireless sensor networks. Int J Distrib Sens Netw. 2018 Apr; 14(4).

13. Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA. Self-organizing Method for Energy-efficient Pulse Coupled Oscillator (EEPCO) in Wireless Networks. Wulfenia. 2016 Dec; 23(12): 240-265.
14. Wang Z, Wang Y. Pulse-Coupled Oscillators Resilient to Stealthy Attacks. IEEE Trans Signal Process. 2018 Jun 1; 66(12): 3086–3099.
15. Wang Z, Wang Y. An Attack-Resilient Pulse-Based Synchronization Strategy for General Connected Topologies. IEEE Trans Automat Contr. 2020 Sep; 65(9): 3784–3799.
16. Iori Y, Ishii H. Resilient Synchronization of Pulse-Coupled Oscillators under Stealthy Attacks. IFAC-Papers OnLine. 2021; 54(14): 424–429.
17. Soryal J, Saadawi T. Byzantine Attack Isolation in IEEE 802.11 Wireless Ad-Hoc Networks. 2012 IEEE 9th Int Conf on Mobile Ad-Hoc and Sensor Systems (MASS 2012). 2012 Oct. https://ieeexplore.ieee.org/abstract/document/6708510.
18. Samir NM, Musni M, Hanapi ZM, Radzuan MR. Impact of Denial-of-Service Attack on Directional Compact Geographic Forwarding Routing Protocol in Wireless Sensor Networks. Baghdad Sci J. 2021 Dec.20; 18(4(Suppl.): 1371. https://doi.org/10.21123/bsj.2021.18.4(Suppl.).1371
19. Goel P, Ermentrout B. Synchrony, stability, and firing patterns in pulse-coupled oscillators. Physica D. 2002 Mar 15; 163(3-4): 191–216.
20. Taniguchi Y, Hasegawa G, Nakano H. Self-organizing Transmission Scheduling Considering Collision Avoidance for Data Gathering in Wireless Sensor Networks. J Commun. 2013; 8(6): 389–397.

آثار هجوم رفض الخدمة على مذبذب النبض المقترن بكفاءة الطاقة

فيصل عثمان حسن [1] نسرين م سامير [2] ذورينا محمد هانفي[2]

[1]كلية تكنولوجيا المعلومات والاتصالات، جامعة بوراو، صوماليلاند.
[2]قسم تكنولوجيا وشبكات الاتصال، كلية علوم الحاسب وتكنولوجيا المعلومات، جامعة بوترا ماليزيا، سيردانج 43400 ، سيلانجور، ماليزيا.

الخلاصة:

وقد اجتذب مذبذب النبض المقترن (بك) اهتماما كبيرا ويستخدم على نطاق واسع في شبكات الاستشعار اللاسلكية (وسنز)، حيث يستخدم تزامن اليراع لجذب شركاء التزاوج، على غرار الحوادث الاصطناعية التي تحاكي الظواهر الطبيعية. ومع ذلك، قد لا يكون نموذج تكو قابلا للتطبيق على الإرسال المتزامن واستقبال البيانات بسبب قيود الطاقة. وهكذا، تم اقتراح مذبذب نبض مقترن موفر للطاقة (إيبكو) ، والذي يستخدم طريقة التنظيم الذاتي من خلال الجمع بين أنظمة الشبكات المستوحاة بيولوجيا وغير البيولوجية ، وقد أثبت أنه يقلل من تأخير الإرسال واستهلاك الطاقة لعقد المستشعر. ومع ذلك، لم يتم تجربة طريقة إيبكو إلا في شبكات خالية من الهجمات دون مراعاة العناصر الأمنية التي قد تسبب أعطالا وهجمات إلكترونية. وسعت هذه الدراسة التجارب من خلال اختبار الطريقة في وجود هجمات الحرمان من الخدمة (دوس) للتحقيق في كفاءة إيبكو في الشبكات القائمة على الهجوم. وتظهر النتيجة أن إيبكو لديها أداء ضعيف في وجود هجمات دوس من حيث جمع البيانات وكفاءة الطاقة، والتي تستنتج بعد ذلك أن إيبكو معرضة للخطر في الشبكات القائمة على الهجوم

الكلمات المفتاحية: الشبكة المستوحاة بيولوجيا وغير بيولوجية رفض الخدمة، مذبذب النبض المقترن، الأمن ، شبكة الاستشعار اللاسلكية، ، شبكة الاستشعار اللاسلكية