Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No.04
Pages: 223-227
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.4.006

A Novel Hybrid HNN and Firefly Algorithm to Overcome Denial of Sleep Attack on Wireless Sensor Nodes

B Vivekanandam
Senior Lecturer,
Faculty of Computer Science and Multimedia,
Lincoln University College, Malaysia.
Email: vivekanandam@lincoln.edu.my

Abstract- A typical Wireless Sensor Network (WSN) comprises of multiple nodes that are used to control as well as monitor the environment and perform pre-described actions. Based on the network, the sensor nodes are distributed and their energy consumption proves to be challenging. When the nodes are located near the sink, they serve as the interface for data transfer between the sink and the node. Because of this, there is a decrease in the networks lifetime and further the energy consumption of the nodes increases significantly. Denial-of-sleep attack is a threat that sensor nodes face in WSNs. DoSA is the condition when there is much loss of energy at the nodes by preventing them from entering into sleep mode and power save mode. We propose a hybrid methodology of Hopfield neural network and firefly algorithm using leach to tackle this issue such that there is a significant increase in network lifetime and energy consumption patterns.

Keywords: Wireless Sensor networks; Hopfield neural network; Firefly algorithm; denial-of-sleep attack; Hybrid algorithm

1. Introduction

Environmental circumstances like temperature, vibration, pressure and sound is monitored with the help of self-guiding sensors of the WSN. These nodes are powered by batteries and their energy loss is one of the primary concerns of WSN. Energy loss may be due to a number of issues such as control packet overhead, idleness, listening, collision and overhearing. WSNs are built to be susceptible to non-invasive as well as invasive attacks, by default. Invasive attacks occur during routing process, service availability and information transmission while non-invasive attacks affect frequency, timing of the channel and power. The DoSA attack is one of the attacks on the sensor nodes such that it is unable to enter sleep mode or save mode resulting in power exhaustion. This is carried out by the attacker by transferring dummy data packets continuously resulting in high consumption of energy. Moreover, analysis of the data packet is also performed and if the source of the data packet is unidentified, it will lead to further increasing the energy consumption.

In recent times, there has been much survey and research on how mobile sinks are used in WSN such that there is a significant decrease in the distance between the sink and node. This is in view of reducing energy consumption and increasing network lifetime. In this paper, we first use hierarchical networks to study the sinks reaction. Each sink is made up of clusters that are used to receive the required data and transmit them to the cluster head (CH). There are four phases in the proposed methodology. Phase one involves the use of fire-leach algorithm to free the cluster. At cluster level, authentication of the data is performed using CH in phase two. In phase 3, optimal points are taken into account by Hopfield neural network (HNN). In the final phase, data is authenticated using CH to the mobile sink. The introduction of mobile sink helps decrease energy consumption in the node as it can be moved anywhere between the sensor nodes. Fig.1 represents an overview of DoSA in a WSN.

ISSN: 2582-337X
Submitted: 16.12.2020
Accepted: 05.01.2021
Published: 12.01.2021

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No.04
Pages: 223-227
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.4.006

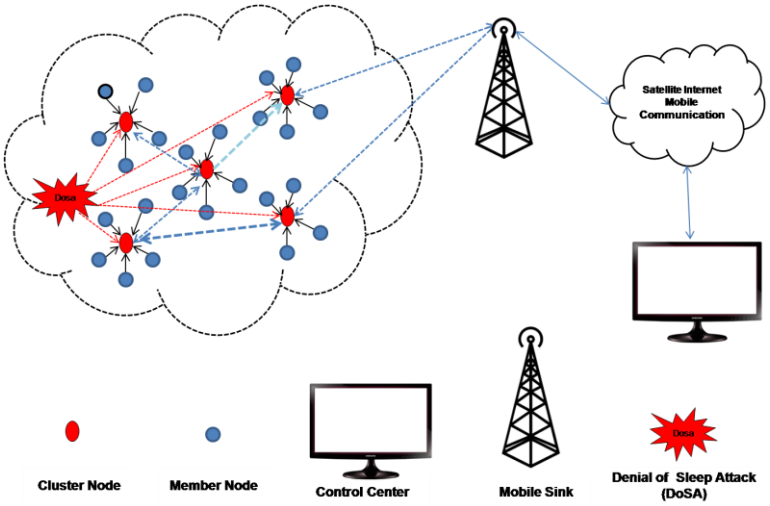

Fig.1. Denial of Sleep Attack (DoSA) in WSN

Section 2 gives a brief outline of the progress in research during the course of time. Section 3 gives a detailed explanation of the proposed work and the results are recorded in section 4. Section 6 concludes the work carried out.

2.Related Work

A number of works have been developed over the years, using safety measures to protect the WSNs from DoSA. To cope with these attacks, a number of methodologies have been proposed. In [1] wireless sensor networks that make use of vector machine learning. Results showed that the throughput shows good results to help detect DoSA. Similarly in [2] denial of sleep attack is observed in WSN with the help of Markov chain model. This methodology will help to determine the attack by predetermining death anticipated time. In [3], the authors have made use of a distributed cooperation-oriented hierarchical framework to determine DoSA. Using two phases, anomalies can be identified to determine the intrusions. On detecting intrusions, the nodes are isolated in order to prevent the transmission of fake packets. Authors in [4] have listed a review of the different DoSA attacks that are prevailant in WSN and proper measures to help prevent these attacks are also given. The storm control mechanism prescribed by authors in [5] come in handy to prevent DoSA and also to decrease the data flooding. Gunasekaran et al. in [6] analyzed the nodes using Genetic Algorithm (GA) which was built using modified RSA algorithm.

3. Proposed Methodology

3.1 Assumptions Made:

In the proposed methodology, the nodes are distributed randomly such that the below mentioned characteristics are used:

- Adjustment to the transmission radius is done by the nodes
- Within a hop, the cluster nodes can communicate information with their CH. Similarly, each CH takes one hop to communicate with the sink.
- The network is built with ‘n’ sensor nodes and a multi-channel mobile sink

There are four phases involved in this proposed methodology which includes: data authentication by mobile sink, movement of sink points, data transmission to CH and formation of cluster.

3.2 Formation of Cluster

The amount of information and clusters required is aggregated for the complete system and based on the information, the nodes are asked to generate a random number. This number is compared with a pre-defined calculated value such that if the generated value is found to be less than the calculated value, it is declared to be the CH. A target function I(x) is calculated using the formula below and this is further sent in the form of message to the other nodes.

ISSN: 2582-337X
Submitted: 16.12.2020
Accepted: 05.01.2021
Published: 12.01.2021

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No.04
Pages: 223-227
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.4.006

$$I(x) = \left(\frac{I_0}{(1+\gamma S_i^2}\right)$$

As intensity quantity increase, the distance between two nodes decreases. I_0 represents the intensity at zeroth time in a node and S_i can be calculated such that

$$S_i = (S_i + \beta(S_j - S_i) + \alpha(round - 0.5))$$

where S_j and S_i are the location of common sensors and CH sensor respectively. The intensity of the CH nodes are examined and the node with highest intensity is connected to the common nodes.

3.3 Data Transmission to Cluster Heads

Here the common sensors gather information and forward it to the CH node. S-MAC protocol is used to monitor the sleep cycle of the sensors. However, a DoSA will occur when the control messages are periodically sent by the attacker such that the node is unable to enter into sleep mode. Hence two levels of authentication are proposed in this methodology.

- **Level 1:** The first level of authentication is performed at the cluster heads. This involves defining a threshold for synchronizing packets. When the synchronization value is high, the possibility of DoSA is high. When a packet reaches the CH node, the origin and sender of the packet is examined to determine if it is within the cluster. Only if it exists will the CH node accept the packet. This authentication is further checked in level 2 authentication of the packet.
- **Level 2:** This level of authentication is carried out at the sink. The node data authenticated at the cluster level is sent to the TDMA scheduler created by the CH. Data is stored in the buffer of each CH till the sink stops in a nearby area.

3.4 Movement of Sink Points

Hopfield is used to identify optimal sink points for the WSN network. It makes use of neurons that are used to point the best triggers for a mobile sink. Fig.2 represents a combination of WSN and HNN such that columns represent K*S and rows represents CH nodes. Here S is the stop points for sink and K is the number of stop point. Here P_{11} to P_{ks} represents the stop points for the sink.

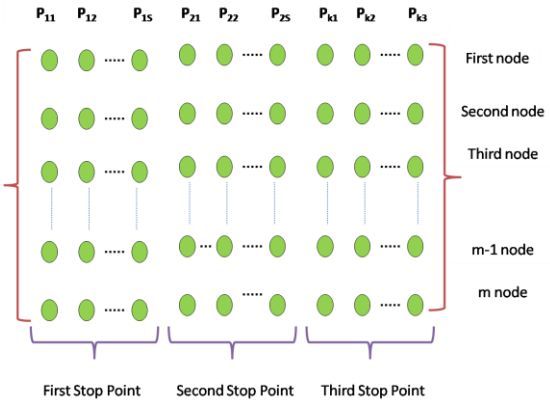

Fig.2. HNN and WSN Combination

3.5 Data Authentication

Data present in the buffer is sent to the mobile sink for second level of authentication by the Ch. The data is sent when the sink stops in the neighbourhood and at this point, it receives all the data from the CH. This is then stored for further access. Protecting the keys is one of the crucial role of the sink and this is done using AES algorithm which is encrypted. The encrypted key is also divided into two parts for better protection.

4. Results and Discussion

The packets delivery ratio of sensors using the proposed method is compared with other similar methods. Simulation results indicate that the reception rate of the hybrid algorithm proposed is considerably high because of cluster head data reach and mobility of the sink. This results in low data transmission time and lesser data loss, when compared with CrossLayer methods. On adjustment of the power in the right manner, our methodology will require lesser amount of power to transmit the data packets as shown in Fig.3

ISSN: 2582-337X
Submitted: 16.12.2020
Accepted: 05.01.2021
Published: 12.01.2021

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No.04
Pages: 223-227
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.4.006

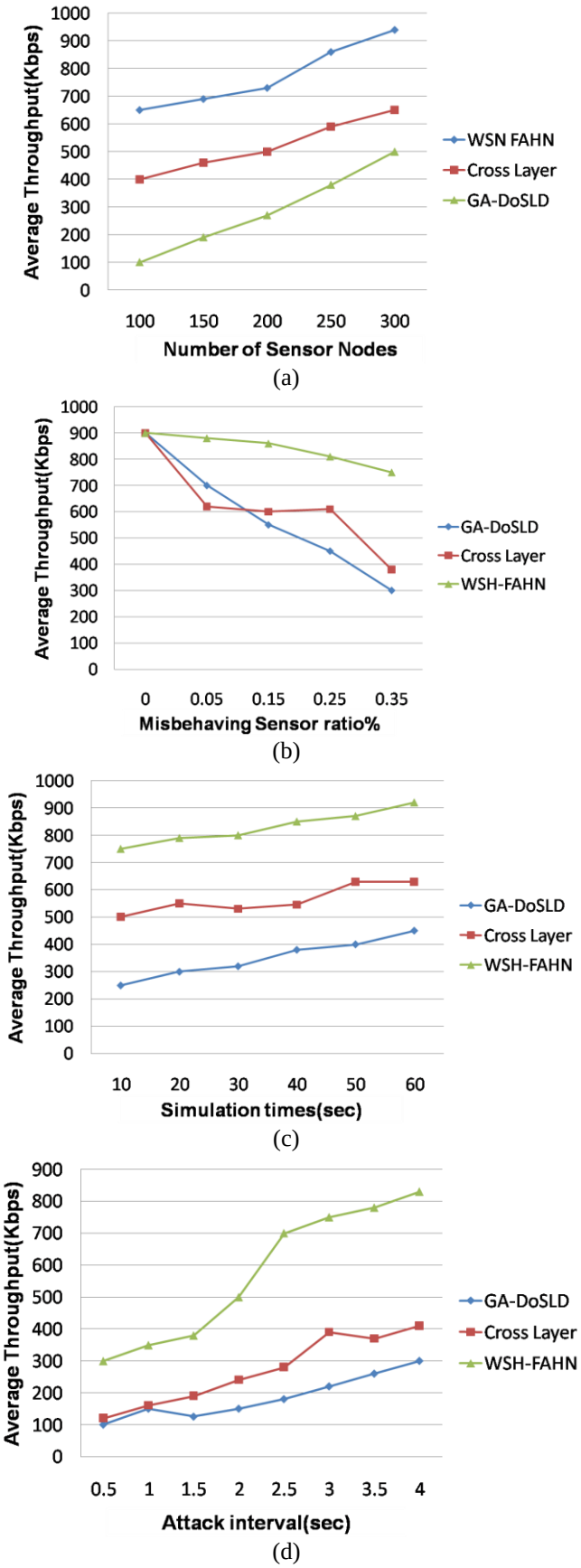

Fig.3. Comparison of GA-DoSLD, Cross Layer and Proposed methodology (WSN-FAHN)

ISSN: 2582-337X
Submitted: 16.12.2020
Accepted: 05.01.2021
Published: 12.01.2021

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No.04
Pages: 223-227
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.4.006

Moreover, the node which holds higher energy is selected to be the CH. This is done based on identification of the node with highest energy level by measuring the residual energy of the node along with the distance to the receiver.

5. Conclusion

A hybrid approach for detecting and preventing Denial of Sleep Attack is presented in this paper based HNN and mobile sink. Experimental analysis shows that the use of mobile sink increases network lifetime and also improves the energy consumption of each node in the WSN. Authentication of the node is done in two phases to prevent DoSA. Since the synchronization message needs to be identified and verified, other messages from third party and attackers are not accepted by the node. This ensures that messages from attackers are denied authentication, thereby preventing unnecessary attacks. Future work includes further expanding the use of mobile sink to decrease energy consumption issues in WSN.

References

[1] Mohd N, Singh A, Bhadauria HS (2019) A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. Wirel Pers Commun. https://doi.org/10.1007/s11277-019-06969-9
[2] Bhattasali T, Chaki R (2012) AMC model for denial of sleep attack detection. arXiv preprint arXiv:1203.1777
[3] Bhattasali T, Chaki R, Sanyal S (2012) Sleep deprivation attack detection in wireless sensor network. arXiv preprint arXiv:1203.0231
[4] Bhattasali T, Chaki R (2011) Lightweight hierarchical model for HWSNET. arXiv preprint arXiv:1111.1933
[5] Rughiniş R, Gheorghe L (2010) Storm control mechanism in wireless sensor networks. In: 9th RoEduNet IEEE International Conference. IEEE, pp 430–435
[6] Gunasekaran M, Periakaruppan S (2017) GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN. Secur Commun Netw 2017:1–10
[7] Desnitsky, V., (2020) September. Approach to Machine Learning based Attack Detection in Wireless Sensor Networks. In 2020 International Russian Automation Conference (RusAutoCon) (pp. 767-771). IEEE.
[8] KanagaSuba Raja, S. and Pushpa, S.X., (2020). A Review on detection mechanisms used in Wireless Sensor Network for DoS attacks.
[9] Mehta, N. and Kumar, A., (2020). Detecting WSN Attacks Through HMAC and SCH Formation. In Computational Methods and Data Engineering (pp. 21-37). Springer, Singapore.
[10] Shirley, D. Ruth Anita. (2014) "Systematic diagnosis of power switches." In 2014 International Conference on Embedded Systems (ICES), pp. 32-34. IEEE,
[11] Meleshko, A.V., Desnitsky, V.A. and Kotenko, I.V., (2020), November. Modelling attacks in self-organizing wireless sensor networks of smart cities. In IOP Conference Series: Materials Science and Engineering (Vol. 971, No. 3, p. 032077). IOP Publishing.
[12] Raj, J.S., (2019). Energy Efficient Sensed Data Conveyance For Sensor Network Utilizing Hybrid Algorithms. Journal: IRO Journal on Sustainable Wireless Systems December, 2012(04), pp.235-246.
[13] Raj, J.S., 2020. Machine Learning Implementation in Cognitive Radio Networks with Game-Theory Technique. Journal: IRO Journal on Sustainable Wireless Systems June, 2020(2), pp.68-75.

ISSN: 2582-337X
Submitted: 16.12.2020
Accepted: 05.01.2021
Published: 12.01.2021