Jamming Attack Against Structure-free of Wireless Sensor Networks

Hussain K. Chaiel

Department of Physics, University of Sumer
Thi-Qar - Iraq

***Abstract*—Structure free Wireless Sensor Network is a type in which the transfer of the data depends on the resources of the sensor nodes. Energy and memory utilization represent the main resources of this type of wireless sensor networks. The transfer of data in WSNs can be interrupted by launching special jamming nodes at the field. However, the life time of the jamming nodes depends on the jamming models used for such purpose. In this paper, we study the effect of different types of jamming models onthe performance of the structure free WSNs by using appropriate computer simulation tests. The results show that the random jammer with (25%) saving time is the most effective jamming model against the structure free wireless sensor networks as compared with the other jamming models.**

***Index Terms*—MLSA, SSS, Structure-free, UAV, WSNs.**

I. Introduction

Wireless sensor networks (WSNs) connect the sensors and actuators of a certain network without the use of wires. Conventional WSNs are more challenging due to the lack of sensor resources such as limited power and memory (Zheng & Jamalipour, 2009). Data aggregation may be considered as a very important method to reduce the energy required for transmitting data from the sensors to the base station, such network is called structure-free wireless sensor network (Dumka & Chaurasiua & Biswas & Mandoria, 2019). However, the structure free wireless sensor network should be capable of timely transmitting data without losing information in event-critical applications (Chao & Hsiao, 2014).

While transferring data, network may be interrupted by a number of attacks. One of these attacks is the jamming attack, which may be defined as a signal directed towards the network to eliminate its capacity (Mpitziopoulos & Gavalas & Konstantopoulos & Pantziou, 2009). Therefore, the jamming is considered as a denial of service attack (Wood & Stancovic, 2002 . This attack can achieve energy efficient jamming when the interruption occurs at the data link layer of the wireless network (Law & et al., 2005). The authors (Li & Koutsopoulos & Poovendran, 2010) study an idealized case of perfect knowledge by both the jammer and the network about the strategy of each other and the case where the jammer and the network lack this knowledge. Excluding the spread spectrum techniques, extensive works had been carried out to avoid the effect of jamming on conventional WSNs by changing the slot utilization pattern at every super frame of the TDMA-based WSNs (Tiloca & et al., 2017), by using mobility model based on game theory (Misra & Mondal & Bhavathankar & Alouini, 2020) or by using unmanned aerial vehicle UAV (Li & et al., 2019; Fotouhi, 2019). However, these solutions are not capable to eliminate the jamming attacks against structure-free wireless sensor networks (Chaiel, & Al-Husseini & Arif, 2020).

The main objective of this work is to study the effect of different types of jamming models on the performance of the structure free wireless sensor networks. The remainder of this paper can be organized as follows, Section 2 provides a description of the structure free WSNs, while Section 3 overviews the types of jamming models. Section 4 includes simulation tests to show the effect of these jamming models on the power consumption of the structure free WSNs and Section 5 concludes the works.

II. Structure-free Wireless Sensor Networks

The sensor nodes of wireless networks have sensing, processing, communication and storage capability. Therefore, it is important to design a suitable node structure to satisfy these operations (Singh & et al., 2018). Instead of constant node structure, the free-structure WSNs has, at each time, different route to transmit data through the network (Chen & Cai & Cheng & Gao, 2021; Boukerche & Quen & Peng, 2020). The selection of such route depends on the resources of the receiving node. The mechanism of routing operation in structure-free WSNs consists of two phases (Chaiel & Abass, 2020): -

A. Determination of Network Levels

The base station transmits a training signal to all the nodes of the networks and each node receives this signal correctly is assigned as a first level node. Then the first level nodes transmit new training signal and each node (excluding the first level nodes) receives the new training signal is called a node with second level. This operation will continue until all nodes are assigned with their level.

DOI: http://doi.org/10.24086/cocos2022/paper.756

B. Transmission of Event Data

When all nodes are assigned with their levels and an event is accrued, the nearest node with (j^{th}) level, for example, transmits the event data to one of the $(j-1)^{th}$ level nodes. The selection of the receiving node, from (N) nodes has the same level, is totally depends on so called cost function. That means the event data is transmitted to the node with maximum cost function. This function can be written as (Mohanty & Kabat, 2016):-

$$\mathrm{CF} = \max_{\mathrm{i}\in\mathrm{N}} \frac{1}{\alpha}(\mathrm{E_{res}(i)} + \mathrm{Buff(i)} + \mathrm{SNR(i)}) \qquad (1)$$

where $\mathrm{E_{res}(i)}$ is the residual energy, $\mathrm{Buff(i)}$ is the available buffer, $\mathrm{SNR(i)}$ is the signal to noise ratio of the transmission link of the (i^{th}) node and (α) is the distance between the rectangular coordinates of the transmitting, (x_t, y_t), and the receiving, (x_r, y_r) nodes and it can be represented by:-

$$\alpha = \sqrt{(x_t - x_r)^2 + (y_t - y_r)^2} \qquad (2)$$

III. Jamming model in Wireless Sensor Networks

The jamming operation can be done using illegitimate nodes immersed in the field of the wireless sensor network. These nodes are energy inefficient, which means that their energy is exhausted sooner than the victim nodes (Xu & Trappe & Zhang & Wood, 2005). The aim of the jamming nodes is to reduce the packet delivery ratio of the wireless network to zero. This can be satisfied,if the jamming nodes are placed at a suitable distance from the legitimate nodes. The types of jamming attacks in wireless sensor networks can be summarized as follows (Mingyan & Koutsopoulos & Poovendran, 2007 May):-

A. Constant Jammer

The constant jammer transmits random signal through the wireless channel to keep the band of the channel busy all the time. This signal eliminates the ability of wireless nodes to transfer the data.

B. Deceptive Jammer

This type emits regular radio sequence of bits without separations into the channel. The legitimate receiving node beliefs that a normal transmission is happened. This type of jamming is more effective than the constant jammer and also it is difficult to detect by the wireless network, but it consumes more energy than the first type.

C. Random Jammer

This type works only for a certain time t_j and then the jammer stays without transmission for a time t_s to save the power. As a result, the required energy consumption is less than the constant and the second types.

D. Reactive Jammer

The reactive jammer listens the activity of the wireless channel and sends a random signal to corrupt the legitimate signal.

IV. Simulation Results

Computer simulation tests have been carried out to show the performance of the structure free wireless sensor network under different types of jamming. In all the simulation tests, the average energy consumption is determined by summing the energy consumption of each operation with the aid of information listed in Table.1. Then the relations between the energy consumption and each of data rate and the event period, of the network, are plotted. Normally, the energy consumption is inversely proportional with the event period because larger event period means less number of events and so less energy consumption. While the relation between the energy consumption and the data rate is directly proportional due to higher operations needed for transmission of data with high rate.

Table.1 Parameters of simulation tests

Parameter	Number	Unit
Area of the network field	500*500	meter
Initial energy for each node	0.65	joule
Energy consumption for transmitting and receiving data	50	nano joule
Energy consumption for sensing operation	0.083	nano joule
Energy consumption for radio amplification	10	nano joule
Number of transmitted packet	1-60	
Saving time for random jammer	25%	
Path loss exponent under noiseless conditions	2500	
Time needed to generate an event	3	second
Maximum sensing distance	50	meter
Total number of transmitted channels	51	
Guard band	5	MHz
Total jamming power	100	watt/MHz

In all tests, we assume two cases of jamming. In the first case, the jamming covers only one transmission channel, while it covers thirty channels in the second case. According to that, and for the four types of jamming, the relations between the average energy consumption and the data rate of the network are shown as in fig.1 and fig.2.

DOI: http://doi.org/10.24086/cocos2022/paper.756

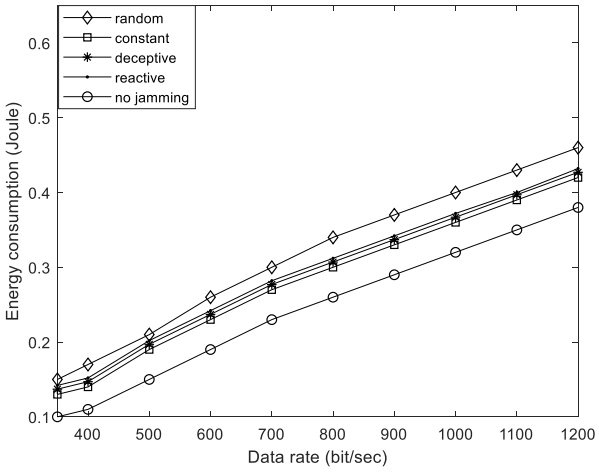

Fig. 1. Relation between the average energy consumption and the data rate for structure- free *WSNs* under different types of jamming models when one transmission channel is jammed.

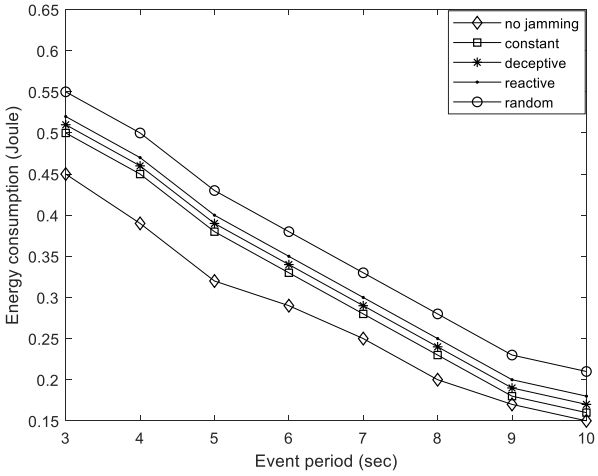

Fig. 3. Relation between the average energy consumption and the event period for structure- free *WSNs* under different types of jamming models when one transmission channel is jammed.

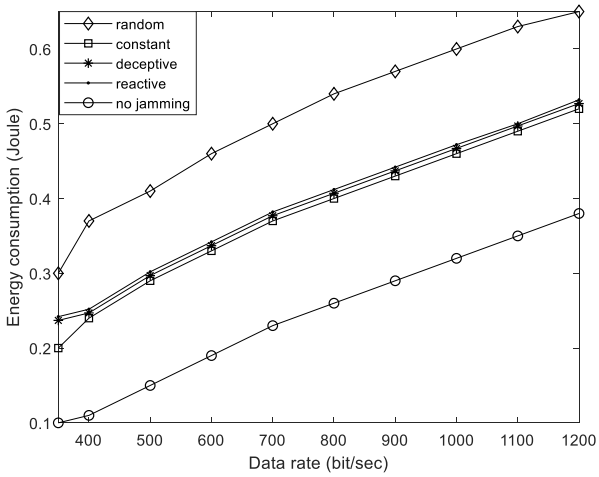

Fig. 2. Relation between the average energy consumption and the data rate for structure- free *WSNs* under different types of jamming models when thirty transmission channels are jammed.

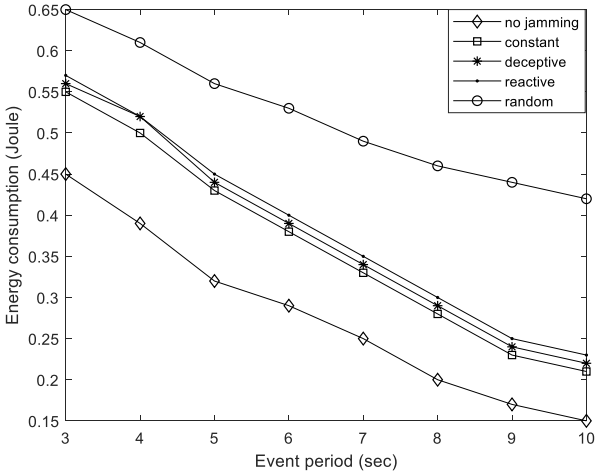

Fig. 4. Relation between the average energy consumption and the event period for structure- free *WSNs* under different types of jamming models when thirty transmission channels are jammed.

It is clearly appears from Fig.2 the average energy consumption for a network under random jamming, at 1200 bit/sec data rate, is equal to the initial energy of the nodes (0.65 joule), which means that the network lose their communication capability.

Further tests are used to examine the effect of jamming on the relation between the energy consumption of the network and the event period. The results of the tests for the two cases of jamming are shown in Fig.3 and fig.4.

The results of the simulation tests shown in (Fig.1-Fig.4) show that the random jammer is the most effective type of jamming models and nearly no difference among the other three types. Extensive tests are used to examine the packet delivery through structure-free WSNs under random jamming with the aid of so called Packet success delivery rate (PSDR). Fig.5 and Fig.6 show the packet success delivery rate of the wireless network *under* random jamming. These two figures shows that the PSDR is nearly 98% for the case of one channel jamming, while it reduced to nearly 48% for the second case.

DOI: http://doi.org/10.24086/cocos2022/paper.756

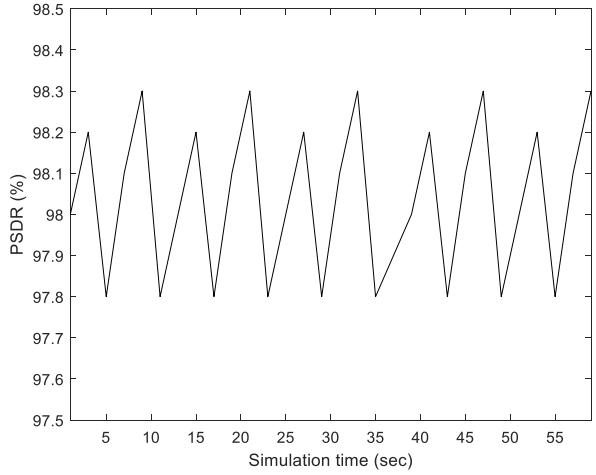

Fig. 5. Packet success delivery rate for a structure- free *WSNs* under random jamming when one transmission channel is jammed.

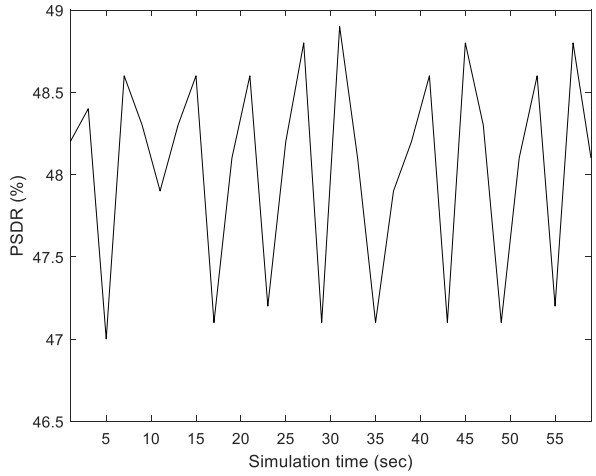

Fig. 6. Packet success delivery rate for a structure- free *WSNs* under random jamming when thirty transmission channels are jammed.

CONCLUSION

In this paper, we studied the issue of jamming attacks against the structure-free WSNs, and examined the ability of different types of jamming models to eliminate the transmission of data through the nodes of the networks. We showed that the random jammer is totally interrupts the transmission at (1200 bit/sec data rate) and the PSDR is reduced to (48%) when the thirty channels, out of 51 channels, are jammed. The value of saving time of the random jammer and its effect on the performance of the wireless network need further efforts to reach its optimal value.

DOI: http://doi.org/10.24086/cocos2022/paper.756

REFERENCES

Zheng, J. & Jamalipour, A. (2009). *Wireless sensor networks,* A John Wiely &sons.

Dumka, A. , Chaurasiua, S., Biswas, A & Mandoria, H. (2019) *A complete guide to wireless sensor networks from inception to current trends*. CRC.

Chao, C.M. & Hsiao, T.Y. (2014). Design of structure-free and energy balanced data aggregation in wireless sensor networks. *Journal of network and computer applications*, 37, 229–239. doi. 10.1109/HPCC.2009.63.

Mpitziopoulos, A. Gavalas, D. , Konstantopoulos, C. & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys Tutorials*, 11(4), 42–56. doi.org/10.1109/SURV.2009.090404.

Wood, A. & Stancovic, J. (2002). Denial of service in sensor networks. *Computer*, 35(10), 54-62. doi.org/ 10. 1109/ MC.2002.1039518

Law, Y., Van Hoesel, V., Doumen, J. Hartel, P. & Havinga, P. (2005) .Energy efficient link-layer jamming attacks against wireless sensor networks. in *Third ACM workshop on security of the ad-Hoc and sensor networks (SASN 2005)*. doi.10.1145/1102219.1102234.

Li, M, Koutsopoulos, I & Poovendran, R. (2010). Optimal jamming attack strategies and network defense policies in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 9(8), 1119–1133.

Tiloca, M., De Guglielmo, D., Dini, G., Anastasi, G. & Das, S.K. (2017) .Jammy: A distributed and dynamic solution to selective jamming attack in TDMA WSNs. *IEEE Transactions on Dependable and Secure Computing*, 14(4), 392–405. doi. 10.1109/TDSC.2015.2467391.

Misra, S., Mondal, M., Bhavathankar, P & Alouini, M.(2020). M-jaw: Mobility-based jamming avoidance in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 69(5), 5381–5390. doi. 10.1109/ TVT. 2020. 2982966

Li, K., Voicu, R.C., Kanhere, S.S., Ni, W and Tovar, E, (2019). Energy Efficient Legitimate Wireless Surveillance of UAV Communications. *IEEE Transactions on Vehicular Technology*, 68(3), 2283-2293, doi: 10.1109/ TVT.2019. 2890999.

Fotouhi A. (2019). Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges," in *IEEE Communications Surveys & Tutorials*, 21(4), 3417-3442, doi: 10.1109/COMST.2019.2906228.

Chaiel, H., Al-Husseini, Z. & Arif, K. (2020). Energy enhancement techniques for structure free wireless sensor network with encrypted data. *International Journal of Sensors, Wireless Communications and Control*, 10(3), 402–412. doi. DOI: 10.2174/2210327909666190627155223.

M. K. Singh, M.K., Amin, S. I. Imam, S.A., Sachan, V.K., Choudhary. A. (2018). A survey of wireless sensor network and its types. *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 326–330. doi. 10.1109/ICACCCN .2018. 8748710

Boukerche, A. QUEN. Wu & Peng, S. (2020). Efficient green protocols for sustainable wireless sensor networks. *IEEE Transactions on Sustainable Computing*, 5(1), 61–80. doi. 10.1109/TSUSC.2019.2913374.

Chen, Q., Cai, Z.M Cheng, L. & Gao, H. (2021). Structure-free general data aggregation scheduling for multi-hop battery-free wireless networks. *IEEE Transactions on Mobile Computing*. doi.org/10.1109/TMC.2021.3053557.

Chaiel, H., Abass, A. (2020, October). Game theoretical for information transmission in structure-free wireless sensor networks. *IET Communication*, 14(17), doi. 10.1049/iet-com 2019.1216.

Mohanty, P, & Kabat, M.R. (2016). Energy efficient structure-free data aggregation and delivery in WSN. *Egyptian Informatics Journal*, 17(3),273–284. doi.org/ 10. 1016/ j.eij.2016.01.002.

Xu, W., Trappe, W. Zhang, Y. & Wood, T. (2005) . The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. The 6th ACM international symposium on Mobile ad hoc networking and computing. 46-57. doi.org/10.1145/1062689.1062697.

Mingyan Li, Koutsopoulos, I., Poovendran, R., (2007 May). Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks. INFOCOM 26th IEEE International Conference on Computer Communications, 1307-1315. Doi. 10.1109/ INFCOM. 2007. 155.

DOI: http://doi.org/10.24086/cocos2022/paper.756