Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
2021, 18(4) Supplement: 1371-1377 **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2021.18.4(Suppl.).1371

Impact of Denial-of-Service Attack on Directional Compact Geographic Forwarding Routing Protocol in Wireless Sensor Networks

Nasrina M Samir ***Maisarah Musni*** ***Zurina Mohd Hanapi*** *
Mohamed Ridzal Radzuan

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-mails: gs59090@student.upm.edu.my , sarah.musni1821@gmail.com , ridzalradzuan77@yahoo.com

Received 12/10/2021, Accepted 14/11/2021, Published 20/12/2021

Abstract:

Directional Compact Geographic Forwarding (DCGF) routing protocol promises a minimal overhead generation by utilizing a smart antenna and Quality of Service (QoS) aware aggregation. However, DCGF was tested only in the attack-free scenario without involving the security elements. Therefore, an investigation was conducted to examine the routing protocol algorithm whether it is secure against attack-based networks in the presence of Denial-of-Service (DoS) attack. This analysis on DoS attack was carried out using a single optimal attacker, A1, to investigate the impact of DoS attack on DCGF in a communication link. The study showed that DCGF does not perform efficiently in terms of packet delivery ratio and energy consumption even on a single attacker.

Keywords: Denial-of-service, Routing protocol, Security, Wireless sensor network.

Introduction:

In recent years, Fourth Industrial Revolution (IR 4.0) has become the subject of much interest due to new waves of technological disruptions and the emergence of advanced technologies. Machine become more intelligent where it gives manufacturers insights they never had before. Therefore, IR 4.0 can be a more extensive perspective led by WSN applications in the near future. Wireless sensor networks (WSN) are rapidly growing in recent years, and it is undeniably one of the most implemented networks in modern communication technology. This is due to the development of inexpensive yet advanced devices comprising hundreds or thousands of independent sensor nodes that can sense various environmental and physical parameters, process them, and wirelessly transfer the processed data. The agility that WSNs possess in their structure allows them to adjust to different conditions. For example, it can accommodate the addition of new devices to the network with ease. WSNs are used in various applications, making them beneficial to society [1-4].

Despite having those benefits, sensor nodes in WSN suffer certain constraints, including limited memory, overhead computation, energy consumption, and security**.** These constraints also affect the routing mechanism of WSN. Routing is a vital function that needs to be prudently managed in WSN. A good routing technique is essential to ensure uninterrupted transmissions between the sensor nodes and the base stations. Characteristics of WSNs such as connectivity to various applications, deployment in extreme environments, and other attributes can cause energy drainage of nodes, depletion of node resources, and many more. These downsides made sensor node an easy target and forced them to be vulnerable to numerous attacks, consequently decreasing WSN communication efficiency. Routing attacks such as Sybil attack, blackhole attack, wormhole attack, Hello flood attack, denial-of-service (DoS) and sinkhole attack, to mention a few, are among the threats faced by WSN [5-6]. The attack of DoS, where an attacking node can place itself in the sensor field, wastes the limited energy of sensor nodes and causes loss of data packet within the network [7].

WSN is susceptible to DoS attacks since the scarce resources of the sensor device put it at risk of

high resource consumption under normal conditions [8]. A severe attack may cause a halted service, in which the target stops functioning even after the attack ends. The disruption could be caused by physical destruction, corrupted memory, or failures with no recovery. DoS attack and its aftereffect may last long enough to affect economic or permanent physical damage, which is why it is a disastrous attack. Researchers have proposed many improved routing protocols based on early secure routing protocols, such as DWSIGF [9], FuGeF [10] and SRBGR [11] etc. Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) is established to generate a potential time shift to create dynamic routine or ambiguity during selecting nodes. The usage of the lazy binding approach for forwarding makes the routing table not maintained, and this avoids routing to a failed node or node that is out of coverage. While DWSIGF is safe from sinkholes, wormholes, HELLO floods attack, apparently, this protocol is still exposed to blackhole, selective forwarding and DoS attack. DWSIGF is further improved in with the introduction of Fuzzy-based Geographic Forwarding (FuGeF) protocol which able to reduce the packet loss at the same time preserving Quality-of-Service (QoS) performance of DWSIGF. FuGeF is an enhancement of DWSIGF regarding the security aspect and ensures efficient consumption of limited resources. FuGeF utilizes three selection parameters: remaining energy, connectivity cost and progressive distance, and applying Fuzzy Logic System (FLS) to select a node. These methods are introduced to ensure non-malicious nodes are chosen appropriately. However, this protocol was tested only on blackhole with Clear To Send (CTS) rushing attack since it is deemed a Spatio-temporal attack. Secure Region-Based Geographic Routing Protocol (SRBGR) is proposed which able to boost the likelihood of choosing the appropriate forwarding node by expanding the assigned sextant and employing distinct message contention priorities in the routing process to allow more valid nodes. This protocol offers verification costs for both attacker's identification and isolation while providing a bound collection window for a sufficient time of collection. SRBGR proved that as the number of attackers increases, the number of legitimate nodes in the communication process participating in the communication also increases. The similarity of DWSIGF, FuGeF and SRBGR is that the protocols do not implement in the presence of DoS attacks and the energy consumed by the sensor nodes remains high.

Directional Compact Geographic Forwarding (DCGF) [12] is used as a benchmark protocol of this study that integrates two active energy conservation mechanisms. The combination of smart antenna and QoS aggregation introduced in DCGF was implemented to mitigate excessive overhead production, subsequently reducing the energy consumed and delay. Since power limitation is considered a crucial issue in WSN, it is vital to analyze the energy consumption in the network, especially in the cross-layer approach, which was proven to conserve energy during the communication process in previous studies. DCGF's approach has successfully addressed the issue of an excessive overhead generation. However, the implementation of DCGF was conducted in an attack-free network where it was only concentrated on routing performance while the protocol's security was not tested. Hence, this study investigates the resiliency of DCGF protocol towards attack, especially DoS, as it may be vulnerable to such attack, which can drain the resources, decrease routing efficiency, and eventually disrupt the entire communication.

Materials and Methods:

Directional Compact Geographic Forwarding (DCGF)

The DCGF utilizes 802.11 Distributed Coordinated Function (DCF) MAC, exhibiting a 4-way handshake routing approach. A smart antenna and QoS aware aggregation in DCGF can alleviate the excessive overhead due to repeated subjection of a multi-hop network. This method mitigates the spreading in a broadcast received and multiple unicast transmissions by restricting the broadcast spread that affects the non-forwarding candidate nodes and replaces it with the unicast data propagation.

A. Smart Antenna & Channel Reservation Phase

Using a smart antenna in the channel reservation phase minimized the spread in the Open Request to Send (ORTS) broadcast propagated within the range of the sender S. This method is used only for target nodes in the forwarding area. Two beams were utilized by DCGF, where one beam is located at the destination node that used for transmission; on the other hand, one beam is used for reception on the opposite side. The forwarding area is defined using the beam width, which is identical in both areas by following the equation (1) below:

$$\text{DCGF (direction)} = 1/6\pi R^2\rho \quad (1)$$

In accordance with the density of ρ, only 1/6 of the nodes applied in this phase of DWSIGF are affected

when the DCGF is employed. This is due to the smart antenna only switches one beam/node at a time. Therefore, only the receiving beams of nodes located along the projected beamwidth are accessible.

B. QoS-Aware Aggregation Approach in Transmission Phase

The generated overhead occurs due to the increase of energy and bandwidth, which can be overcome through an added aggregation layer (between data link and network layer). Each data packet is padded with a MAC header, making the method focused on packet transmission, adding a fixed overhead during the transmission. In addition, the individual data packets had joined into a larger data packet. The DCGF decrease the volume of unicast data packet transmission, especially the overhead cost due to MAC header using the equation (2) below:

$$\text{DCGF (overhead)} = \frac{N}{DOA} + DOA \quad (2)$$

where N is the number of data packet transmitted and the degree of aggregation (DOA) is the fixed data aggregation used.

DCGF Routing Process Without Attack

The beginning of routing process of DCGF starts with the sender node (S) transmitting a Directional Request-to-Send (DRTS) broadcast which contains location for both source and destination for nodes spreading in the particular beam-width directed to the sink. The candidate nodes continue to establish the Clear-to-Send (CTS) response time Rt once the signal is received and must wait for the CTS to expire before unicast their particular CTS for sampling. Then, S begins to collect its CTS responses after the CTS timer of the nodes expired. A fixed Collection-Window-Time (CWT) was utilized in furnishing particular and adequate time to accumulate CTS responses. At the end of channel reservation phase, a forwarding node is selected after the collected responses are sampled by following the priority or random forwarding technique.

A channel is secluded after a node is chosen for the transmission phase. The unicasting process is captured by the aggregation layer. In this phase, several data packets with multiple headers are concatenated into a single frame with a single header, which is then forwarded to the receiving nodes. The de-aggregation process ensures the aggregated packet is unimpaired before being forwarded to the higher layer. Once the packets are successfully delivered, an acknowledgement (ACK) packet is dispatched back to the sender S. The routing process of DCGF without attack is shown in Figure 1.

DCGF Routing Process with DoS Attack

For attack-based simulation, the routing process of DCGF is modified against malicious nodes inside the network. Similar to the original routing process, it begins with DRTS broadcast sent to the nodes lying within the beam-width until the sampling of gathered response. However, during the selection of nodes, a modification is included by which upon selecting an attacker node, the malicious node will drop the data. Such adjustment ensures that by dropping the data packet, the whole network will suffer from the loss of packets and consequently instigating denial of service. Thus, the attack tolerance level of DCGF can be determined by analysing the attacker selection possibility and packet delivery ratio. The flowchart of the DCGF routing process in an attack-based environment is illustrated in Figure 2.

The DoS attack simulation is conducted using Sybil nodes in which the malicious node displays several identities to other nodes in the network, with the purpose of dropping packets in route. Numerous virtual Sybil nodes are created with distinct identities for each and are located at a single attacker, A1, in the routing path, as shown in Figure 3. The virtual Sybil nodes transmit their responses using the identities attached when they overhear a DRTS signal to manipulate the collaborative nature of WSN. Data exchange occurs if the node is chosen as the forwarding candidate, after which the virtual node forwards an ACK to the DRTS sender. However, in this study, the virtual attacker(s) is forced to drop all the received data.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

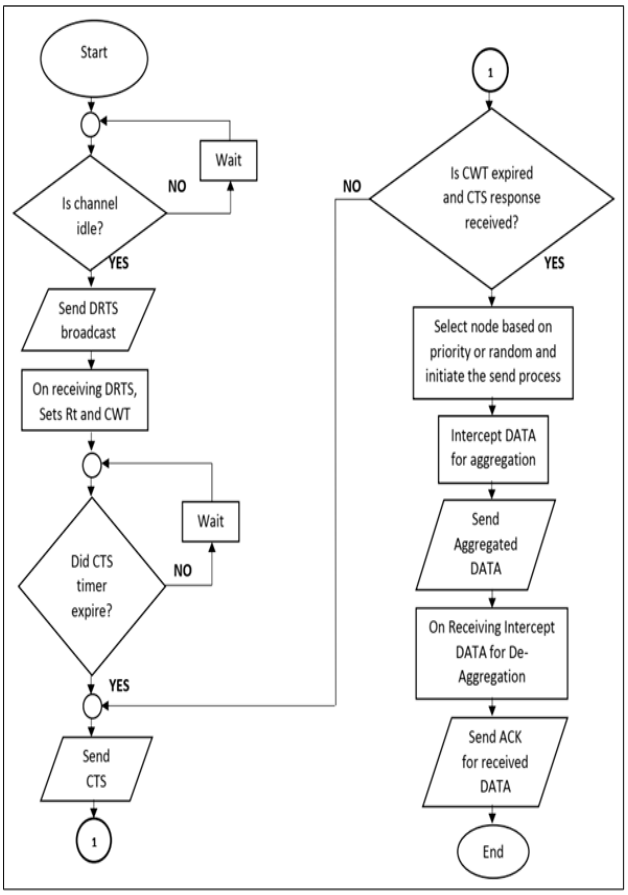

Figure 1. Routing process of DCGF without attack

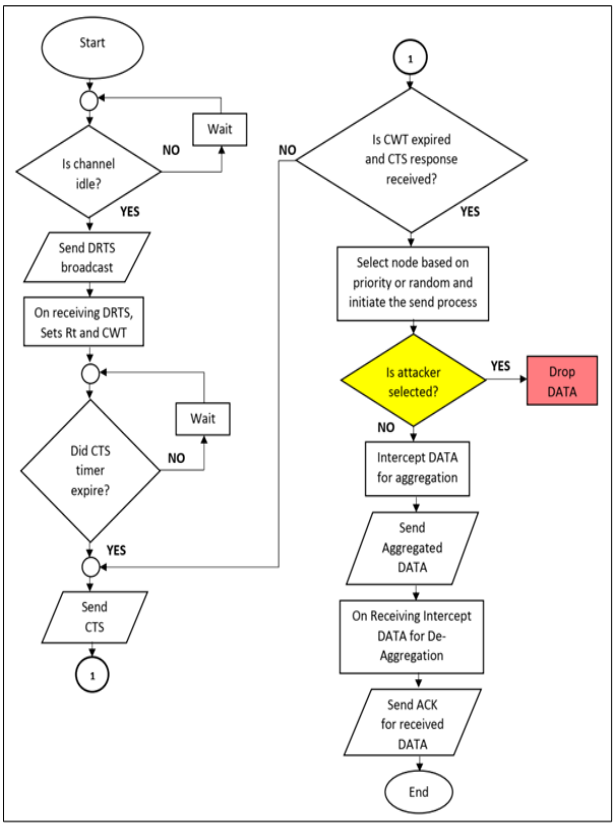

Figure 2. Routing process of DCGF with DoS attack

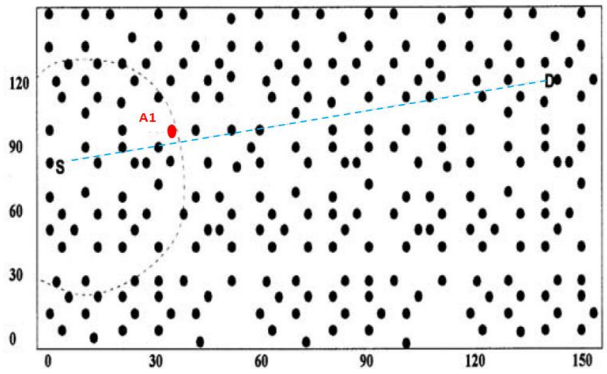

Figure 3. Deployment of 196 nodes with attacker A1

Implementation:

The simulation is conducted using MATLAB and the parameters for DCGF under attack-based scenario is applied as shown in Table 1 to have a fair comparison for both scenarios. Since the analysis was conducted to analyse the security of DCGF, the parameters used for number of nodes, packet size and DOA are fixed at 196, 32 and 5, respectively. Such parameter is configured in view that the DCGF needs to be analysed in the environment which requires medium bandwidth with the insertion of DoS attack for the first time. Network performance during the DoS attack also needs to be determined under a progressively stressful scenario. This setup serves as the baseline for further analysis in lower and higher bandwidth setup.

In an attack-based scenario, the protocol was tested on a DoS attack with a single attacker, A1, which has the highest likelihood to be selected as the first hop. Sybil nodes are present in the vicinity of A1 to act as interceptors so that more than one candidate node participating in the process of node selection.

Table 1. Simulation parameters

System parameter	Value
Number of nodes	196
DOA	5
Radio range	40 m
Packet size	32 bytes
Terrain	150 × 150 m^2
Radio bandwidth	200 Kpbs
Initial node energy	5 J
Node placement	Uniform, Grid + N (0,16) noise
Radio	Lossy channel
Application streams	CBR

Results and discussion:

Analysis on packet delivery ratio (PDR)

PDR is measured to ensure the efficacy of node-to-node mapping and corroborate effective connectivity between the nodes. Figure 4 demonstrates the outcomes of the impact of DoS attack which positioned at a single attacker, A1, where six virtual nodes of Sybil were randomly placed within a 25m distance from each of them. As mentioned previously, the attacker increases the number of its candidates during the selection process by having multiple identities. Therefore, a large number of pooled resources are allotted to these nodes. Additionally, network traffic will be compelled by the virtual nodes to go through a single node. As expected, non-malicious nodes selected for forwarding were capable of delivering during low traffic flows. Furthermore, the smart antenna mechanism of DCGF played its role in selecting nodes within the propagated range.

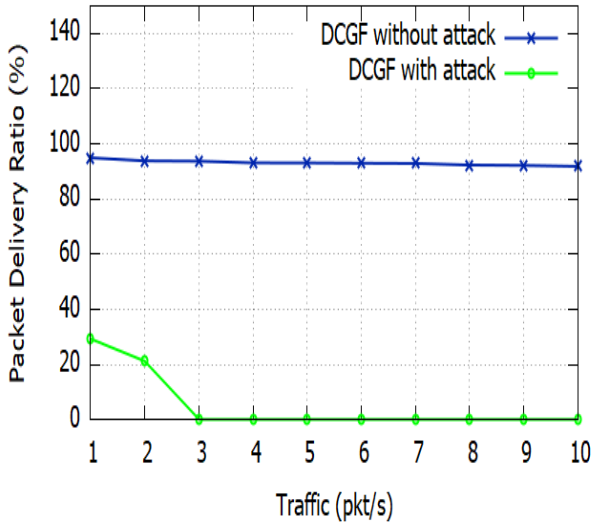

Figure 4. Impact on PDR

In this case, a few malicious nodes were outside the projected beam-width and bypassed during the node selection. However, as the traffic gradually increased, the communication was overcrowded and the nodes were forced to drop the packets. At attacker A1, the selection of attacker becomes 100% starting at traffic 3 pkt/s, which resulted in 0% PDR throughout traffic 10 pkt/s. This resulted in a total average of 5.1% of the PDR and achieved an average of 94.8% chance of being selected in the overall simulation. PDR of DCGF in the attack-based network is significantly lower than the rate for DCGF in the attack-free network. This is because DCGF does not have any security mechanism integrated to avoid selecting malicious attackers as forwarding nodes during transmission.

Analysis on energy consumption

The term energy consumption is defined as depleted energy by the participating nodes from the initial communication process to the end of the communication process. To obtain the simulation result, an average of 100 runs per traffic flow is set up for the experiment. Figures 5a and 5b illustrate the impact of DoS on energy consumption against the traffic flow and network size.

The result obtained shows that the energy consumed by attacker A1 steadily increased across the increased traffic flow and network size. This might occur because the attacker A1 has a high possibility of being selected as the first hop, which gives significant impact because it does not easily bypass the attackers during node selection. The existence of six randomly positioned virtual nodes on A1 would intercept the responses to allow more than one candidate node to engage in the node selection process. This behaviour causes the malicious nodes to be selected as the forwarding node. Under such occurrence, retransmission of the packet is required. The consumption of energy during retransmission is high, as the data needs to be transmitted several times before the packet is successfully received. This will drain the energy of the node and die afterwards.

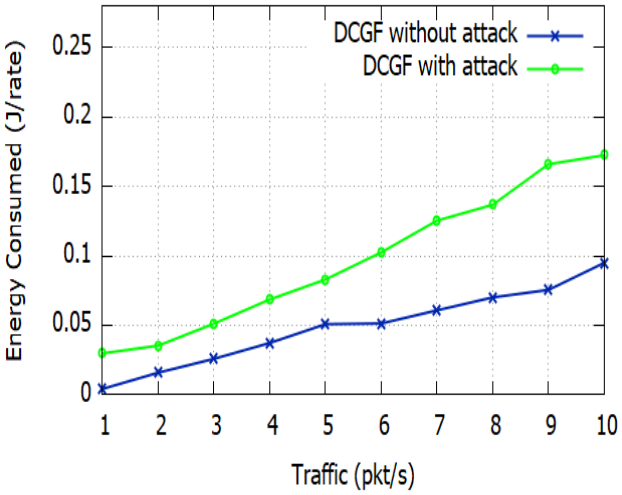

Figure 5a. Impact on energy consumption vs traffic loads

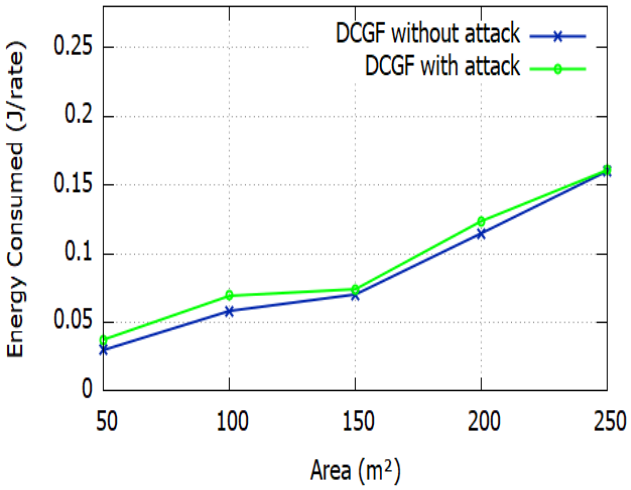

Figure 5b. Impact on energy consumption vs network size

Conclusion:

DCGF protocol had addressed the issues of excessive overhead during the communication process in an attack-free network. However, the protocols' algorithm does not guarantee its performance when there is a DoS attack even with a single attacker, which produced a low packet delivery ratio and high energy consumption. Therefore, improving the limitation of DCGF in attack-based networks will be the next direction of this research.

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.
- The author has signed an animal welfare statement.
- Ethical Clearance: The project was approved by the local ethical committee in University of Putra Malaysia.

Authors' contributions:

Nasrina M Samir, Maisarah Musni, Zurina Mohd Hanapi and Mohamed Ridzal Radzuan contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript.

References:

1. C. A. Ramírez, R. C. Barragán, G. García-Torales and V. M. Larios, "Low-power device for wireless sensor network for Smart Cities," 2016 IEEE MTT-S Latin America Microwave Conference (LAMC), 2016, pp. 1-3, doi: 10.1109/LAMC.2016.7851298.
2. N. B. Gayathri, G. Thumbur, P. Rajesh Kumar, M. Z. U. Rahman, P. V. Reddy and A. Lay-Ekuakille, "Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9064-9075, Oct. 2019, doi: 10.1109/JIOT.2019.2927089
3. E. Aguirre et al., "Design and Implementation of Context Aware Applications With Wireless Sensor Network Support in Urban Train Transportation Environments," in IEEE Sensors Journal, vol. 17, no. 1, pp. 169-178, 1 Jan.1, 2017, doi: 10.1109/JSEN.2016.2624739.
4. F. Viani, G. Oliveri, M. Donelli, L. Lizzi, P. Rocca and A. Massa, "WSN-based solutions for security and surveillance," The 40th European Microwave Conference, 2010, pp. 1762-1765, doi: 10.23919/EUMC.2010.5616285.
5. Singh, R., Kathuria, K., & Sagar, A. K. (2018). Secure Routing Protocols for Wireless Sensor Networks. In 2018 4th International Conference on Computing Communication and Automation (ICCCA).
6. Rehman, A., Rehman, S. U., & Raheem, H. (2019). Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Personal Communications, 106(4), 2291–2313..
7. Stankovic, J. A., & Wood, A. D. (2004). A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks. Handbook of Sensor Networks.
8. O. A. Osanaiye, A. S. Alfa and G. P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 6975-7004, 2018, doi: 10.1109/ACCESS.2018.2793841.
9. Hanapi, Z.M., Ismail, M., Jumari, K., Mahdavi, M.: 'Dynamic window secured implicit geographic forwarding routing for wireless sensor network', *Int. J. Electron. Commun. Comput. Eng.*, 2009, **1**, (4), pp. 213– 219
10. Umar, I. A., Hanapi, Z. M., Sali, A., & Zulkarnain, Z. A. (2016). FuGeF: A Resource Bound Secure Forwarding Protocol for Wireless Sensor Networks. Sensors, 16(6), 943.
11. Adnan, A. I., Hanapi, Z. M., Othman, M., & Zukarnain, Z. A. (2017). A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks. PLOS ONE, 12(1).
12. Umar, Idris Abubakar, et al. "Towards Overhead Mitigation in State-Free Geographic Forwarding Protocols for Wireless Sensor Networks." Wireless Networks, vol. 25, no. 3, 2019, pp. 1017–1030.

Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
2021, 18(4) Supplement: 1371-1377 **E-ISSN: 2411-7986**

تأثير هجوم رفض الخدمة على بروتوكول التوجيه التوجيهي الجغرافي المضغوط في شبكات الاستشعار اللاسلكية

نسرين م. سامير **ماءيساراه موسني** **ذورينا محمد هانفي***
محمد ريضال رضوان

قسم تكنولوجيا وشبكات الاتصال، كلية علوم الحاسب وتكنولوجيا المعلومات، جامعة بوترا ماليزيا، سيردانج ، سيلانجور، ماليزيا.

الخلاصة:
يَعِدُ بروتوكول التوجيه، الموجه الجغرافي المضغوط (DCGF) بتوليد الحد الأدنى من النفقات العامة من خلال استخدام هوائي ذكي وتجميع واعٍ لجودة الخدمة (QoS) .ومع ذلك، تم اختبار DCGF فقط في سيناريو خالٍ من الهجمات دون إشراك عناصر الأمان. لذلك، تم إجراء استقصاء لفحص خوارزمية بروتوكول التوجيه فيما إذا كانت آمنة ضد الشبكات القائمة على الهجوم بوجود هجوم رفض الخدمة (DoS). تم إجراء هذا التحليل على هجوم DoS باستخدام مهاجم واحد مثالي،A1 ، للتحقيق في تأثير هجوم DoS على DCGF في خط اتصال. أظهرت الدراسة أن DCGF لا يعمل بكفاءة من حيث نسبة تسليم الحزم واستهلاك الطاقة حتى على مهاجم واحد.

الكلمات المفتاحية: رفض الخدمة، بروتوكول التوجيه، الأمن، شبكة الاستشعار اللاسلكية.