Internet of Things 17 (2022) 100464

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

A jamming attack detection technique for opportunistic networks

Jagdeep Singh [a], Isaac Woungang [b,*], Sanjay Kumar Dhurandher [c], Khuram Khalid [b]

[a] Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, Longowal, Punjab, India
[b] Department of Computer Science, Ryerson University, Toronto, Ontario, Canada
[c] Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

ARTICLE INFO

Keywords:
Jamming detection
Opportunistic networks
Routing
Statistical information
Energy

ABSTRACT

Opportunistic networks (OppNets) are dispersed in nature, with nodes acting as resource restrictions, with intermittent connectivity. These nodes are subject to various types of attacks, posing a security risk in data transmission. One of the most common attacks that cause jamming among the message forwarding nodes in infrastructure-less networks is Denial of Service (DoS) attack. Most of the methods addressing this type of attack rely on cryptographic algorithms, which are too difficult to implement. In this paper, a novel jamming attack detection technique (JADT) for OppNets, is proposed, which relies on the use of some statistical measures collected from the relay nodes and a prescribed threshold on the packet delivery ratio (PDR) to discover a jamming attack while decrypting the acknowledgement, stopping the message transmission and rebroadcasting the message through a different channel. The proposed JADT is evaluated using the ONE simulator, showing its superiority against the Fuzzy Geocasting mechanism in Opportunistic Networks (F-GSAF) scheme in terms of packet delivery ratio and overhead ratio, under varying TTL and buffer size.

1. Introduction

OppNet [1] is a type of intelligent wireless network that consists of tens of thousands of sensor nodes capable of detecting and communicating in a self-organized way. The nodes collect information through their neighbours nodes and perform the information collection task autonomously through wireless, low energy, single or multi-hop transmission and data exchange between the nodes. These nodes have a high data acquisition capability and they can operate in any situation, at any time, and location, making it helpful in several practical domains such as military, medical health, traffic management, and environmental monitoring.

OppNets nodes are dispersed in nature, have resource constraints, and are deployed remotely. They are susceptible to various types of attacks, which cause security issues in data transmission. One of the most dominant types of attacks in OppNets is the jamming attack, which targets the perception layer and disrupts the communication between the nodes, causing them to consume the resources of the canal and severely damage them. Because the OppNet nodes communicate in a store-carry-forward fashion, they are subject to a variety of attacks, among which are the denial of service (DoS), spoofing attacks, selective forwarding attacks, sinkhole attacks, sybil attacks, wormhole attacks, and jamming attacks, to name a few.

This paper focuses on jamming attacks, i.e. an attack that uses a rogue node to overwhelm the transmitted signal by introducing a large amount of noise, thereby restricting the attainable rate of a sent signal by drastically lowering the packet delivery ratio (PDR). In an OppNet, jamming detection and prevention [2] is more difficult because detecting the malicious nodes among a dispersed group of nodes is extremely tough due to the network inherent characteristics such as unstable topology, frequent changes in

* Corresponding author.
E-mail address: iwoungan@ryerson.ca (I. Woungang).

https://doi.org/10.1016/j.iot.2021.100464
Received 17 September 2021; Accepted 20 October 2021
Available online 23 November 2021

connections, high delay, to name a few. Some of the approaches used so far in the literature to address this type of attacks are game theory methods, trust-based methods, auto regression technique, Markov chain models [3], to name a few. Besides, there are four different types of jamming attacks, namely: (1) Proactive jammer, which is implantation friendly. This type of jamming attack attempts to emit jamming signals regardless of the traffic pattern in the channel, but is ineffective in terms of attacking damage, detection probability, and energy efficiency due to a lack of channel awareness; (2) Deceptive jammer, which sends the regular packets constantly, rending it more difficult to detect than in a continuous jammer case since it broadcasts the genuine packets rather than the random bits; (3) Constant jammer, which emits a constant jamming signal at all time, as well as unpredictable jamming signals; and (4) Random jammer, which generates a continuous jamming signal and random jamming signals, alternating between two states on a regular basis, namely the sleep and jamming states.

In this paper, a statistical process control (SPC) approach [3] is used to implement a novel jamming detection scheme in cluster-based OppNets, which minimizes the routing overhead. This approach mainly relies on the use of the packet drop ratio (PDR) as a significant parameter in detecting the jamming attacks, noting that the PDR is defined as the number of dropped packets divided by the total number of packets transmitted. An encryption key is used to encrypt the sender's acknowledgement, ensuring that the data transfer remains absolute within the prescribed threshold. This method is dynamic and it organizes the sensor nodes according to their node coverage range. Through simulations using the ONE simulator [4], the efficiency of the proposed JADT scheme in comparison to the F-GSAF scheme, is demonstrated.

The remainder of the paper is organized as follows. Section 2, some related works are discussed. In Section 3, the proposed jamming attack detection technique (JADT) is described. Simulation results are presented in Section 4. Finally, Section 5 concludes the paper.

2. Related work

In the literature, there are few works on jamming attacks detection and/or prevention in ad hoc and delay tolerant networks. Representative ones are as follows [5–16].

In [5], Altaweed et al. studied the hybrid and Prophet routing protocols for OppNets and demonstrated their vulnerabilities against collusive hijack attack. Some defense mechanisms are proposed against such attacks, referred to as path detection technique (PDT) and hop detection technique (HDT) Those methods rely on the use of a Kolmogorov–Smirnov test to find whether the statistical distribution of the delays encountered by the packets follows the distribution of the Inter Contact Times of the nodes. The obtained simulation results demonstrate the effectiveness of the proposed techniques in effectively detecting the collusive hijack attacks.

In [6], AbdelRaheem et al. proposed an anti-jamming method for OppNets,in which some cooperative collations over the available channels are constructed by the secondary nodes to counteract the signal-to-noise-ratio(SINR) drop caused by the presence of the jammer nodes. In their scheme, the secondary nodes and the jammer nodes interact by means of a modified Colonel Blotto game in which the jammer node is the attacker and the secondary nodes have elected coordinators. Using a fictitious play-based algorithm, a Nash strategy equilibrium solution of the game is found. Simulation results showed the rationale of using such a cooperative communication strategy to improve the performance generated by the nodes with low data rates.

In [7], Parris et al. proposed a simple flooding attack that can be used to restrict or deny the services in OppNets. In the proposed scheme, before each message is sent, it is signed by the original sender, and its retransmission is operated only the trusted social contacts of this sender node. In this sense, the defense strategy relies only on the local knowledge at each node. Through trace-driven simulations, the efficiency of the proposed attack-resistant protocol is proven using real-world datasets.

In [8], Kasturi et al. proposed a machine learning-based technique that uses some indicators to detect and classify different types of jamming attacks. These indicators (i.e. parameters) are derived from a simulation study of three kinds of interferences approaches (constant, reactive and random interferences), and the collected metrics from different layers are utilized as inputs to a set of ML algorithms. Due to changes made in the ML algorithm parameters during the dataset collection process, the retained ML technique is shown to achieve a high accuracy while generating a minimal overhead cost and being suitable for use on equipments.

In [9], Lalropuia et al. proposed a Bayesian game and network availability models for small base stations under denial of service (DoS) attacks on the 5G wireless communication networks. In this work, the interaction between the attacker (i.e. mobile user) and the network defender (i.e. the intrusion detection system) is modelled as a Bayesian game model, then solved to find the best strategy for the attacker and the defender. Also, since DoS attacks [10] make the network unavailable, the network availability problem is also addressed and resolved by means of a network availability model of about 1 MB in the 5G wireless communication networks under the bandwidth spoofing attack using a Signal to Noise Ratio model.

In [13], Salameh et al. proposed an intelligent and security-aware routing scheme (called Probability of Success in Security (SAPoS)) for interference perception in IoT-based cognitive radio networks (CRNs), which can also prevent against active jamming attacks. Their scheme considers some cognitive radio link quality conditions as well as some interference attacks without additional resources. For each cognitive radio IoT source–destination pair, the proposed algorithm assigns the safest channel for each hop as the result of an optimization problem, then chooses the best route from the possible ones. The algorithm aims to improve the network performance by considering jamming attacks in its screening process [11].

In [14], Gao et al. proposed a Spoofing jamming attack based on wireless network cross-technology communication. In their scheme, a single WiFi frame is used to deceive the ZigBee devices on two channels, while blocking them on five channels at different frequencies by controlling the non-contiguous frequency bands of the subcarriers. A channel coding simulation and a post QAM simulation for the WiFi frame of the ZigBee signal are proposed. Subsequently, the process of using WiFi devices to conduct parallel

Table 1
Comparison of related works.

Author	Parameters				
	Technique	Threshold required	Overhead	PDR	Energy consumption
Altaweel et al. [5]	Kolmogorov Smirnov test	Yes	High	NA	High
AbdelRaheem et al. [6]	Jammer framework	Yes	High	High	Low
Parris et al. [7]	Game theory approach	Yes	Low	NA	Low
Kasturi et al. [8]	Machine learning-based	Yes	High	NA	Low
Lalropuia et al. [9]	LAPSE	Yes	Low	Low	High
Salameh et al. [13]	PDR based	Yes	Low	Low	High
Gao et al. [14]	Spoofing jamming attack-based	Yes	High	High	High
Mishra et al. [15]	PDR based	Yes	Low	High	High
Ravishankar et al. [16]	Game theory-based	Yes	Low	NA	Low
Proposed JADT Scheme	Statistical Process Control	Yes	Low	Low	Low

spoofing attacks [12] on ZigBee devices is described and experimented, showing how to use a single WiFi frame to block the ZigBee nodes running on five different channels.

In [15], Mishra et al. proposed a preventive detection strategy using honey nodes and a response mechanism based on existing channel navigation algorithms to protect wireless nodes from interference. In their scheme, the honey nodes generate virtual communications at a frequency close to the real operating frequency and warn the real nodes of an imminent attack so that these nodes can switch to another frequency before the jammer starts scanning their frequency. Here, the selection of the next frequency, which uses a combination of active and reactive channel selection procedures.

In [16], Ravishankar et al. proposed a game theoretic-based scheme to defend against jamming attacks in delay tolerant networks. In their approach, the game involved two parties, namely the transmitter–receiver pair and the jamming node. In the presence of a jammer, the transmitters are responsible for the selection of the optimal time needed for scheduling the message transmission from source to destination in a secure manner, in such a way as to increase the message delivery probability.

Our proposed JADT scheme differs fundamentally from the above discussed protocols since it relies on the use of some statistical measures collected from relay nodes and a prescribed threshold on the packet delivery ratio (PDR) to discover a jamming attack and avoid the participation of the jamming nodes in the message routing and forwarding process. A comparison of these related works is given in Table 1.

3. Proposed jamming attack detection technique

In an OppNet, the nodes share their summary vectors intermittently when transmitting a message over a wireless medium [1]. Thus, the radio transmissions can be jammed or interfered with each other, resulting in message corruption or message loss. Taking this fact into account, our proposed jamming detection approach relies the use of a statistical process control (SPC) method to control the variation in the packet drop ratio (PDR) as a mean to identify a jamming attack, where the PDR is defined as the number of dropped packets divided by the total number of packets delivered. Indeed, the SPC method consists in supervising the PDR using the so-called control limits graph [2], where the detection of deviation is the basic principle of control and the upper control limit (UCL) and lower control limit (LCL) parameters, are given by [2]:

$$UCL = p + \sqrt[3]{\frac{p(1-p)}{n}} \tag{1}$$

$$LCL = p - \sqrt[3]{\frac{p(1-p)}{n}} \tag{2}$$

Based on the calculations of UCL, LCL and PDR, a node is then classified in either of the following zones: No-jamming zone, Suspicious zone, or Jamming zone. Basically, when the simulation starts, all the nodes are in Stage 1 (referred to as *No Jamming zone*). At a certain time t (in minutes), the jammer node is activated, and the changes are observed in the behaviour of nodes. Some of these nodes who behave maliciously are identified and qualified as suspicious, then put in the so-called *Suspicious zone* (Stage 2). If the UCL value of a particular node is high (compared to a predefined threshold), then this node is considered as jammer and put in the *Jamming zone* (Stage 3). Therefore, Stage 3 consists all the jamming nodes that are present in the simulation environment. These nodes are isolated and the message is forwarded to the destination node without involving their participation. The pseudo-code of the proposed JADT scheme is given in Algorithm 1.

Various routing attributes such as movement, remaining energy and remaining buffer, are used in the selection of the next best hop to carry the message forward to the destination. Besides, two fuzzy controllers are used in the proposed scheme.

1. *Movement fuzzy controller:* Movement is a critical attribute in this model since it provides a measure of how much a relay node is likely to move towards the direction of the destination node. The movement fuzzy controller is used to get the movement of a node as output (here termed as movement). Its input variables are the direction and speed of the node as follows: (a) the *node's direction* represents the angle between the line connecting the sender node to the geocast area centre and the line along which the receiver node is now travelling is the direction of the next hop. It should be noted that the narrower the angle,

Algorithm 1 Proposed jamming attack detection technique.

Begin N nodes (S_0, S_1, S_2, S_3, …, S_n) in OppNet. H_i represents the intermediate node used for message forwarding.
Message m generated by source node S_i and source node wishes to transmit the message to destination node.
for Encounter between nodes **do**
    Calculate the likelihood L(H_i, m) and L(H_s, m) of the encountered and source nodes respectively.
    if (L(H_i, m) > L(H_s, m)) **then**
        Collect the PDR of the encountered node
        Calculate the parameters UCL and LCL according to Equations (1) and (2).
        if (PDR of the encountered node ≤ LCL) **then**
            No jamming zone exist
            Exchange the summary vectors among the nodes
            Forward the message m to H_i.
        else
            Suspicious zone exist
            No message exchange among the nodes
            Make an entry of the encountered node in the suspicious zone
            Check next neighbour of the node
            Go back to line 3
        end If
        if (PDR of the encountered node ≥ UCL) **then**
            Jamming zone exist
            No message exchange among the nodes
            Make an entry of the encountered node in the jamming zone
            Check next neighbour of the node
            Go back to line 3
        end If
endfor
        Message delivered successfully to the destination.

Table 2
Movement controller.

Movement controller		
Direction	Speed	Movement
VL	L	L
VL	M	L
VL	H	L
L	L	L
L	M	L
L	H	M
M	L	L
M	M	M
M	H	H
H	L	M
H	M	H
H	H	H

the more likely a message will reach its intended recipient. The direction variable's input ranges from 0 to 180 degrees. This variable is classified into four output, namely: very low, low, medium, and high; and (b) the *node's speed* variable values is taken in the range [0 ms–15 ms]. The output of this controller (i.e. movement) is divided into three fuzzy classes (low, medium, and high). Once the movement is finalized, it is used as the input variable for a second fuzzy controller called the Likelihood fuzzy controller.

2. *Likelihood fuzzy controller:* This controller takes three input variables, namely movement (i.e. node's movement), node's remaining energy, and node's remaining buffer space. These variables are classified into three categories, namely low, medium, or high. This controller's output is the likelihood of the node to forward the message towards its destination. There are five levels of likelihood, i.e. very low, low, medium, high, and very high. If the likelihood of the receiver node is larger than the likelihood of the sender node, the message will be sent to the recipient. The outputs of the proposed Movement and Likelihood fuzzy controllers are described in Tables 2 and 3.

The proposed JADT technique is described in Algorithm 1, where the following notations have been considered: C: number of remaining replicas of a message, *VH*: very high, *H*: high, *M*: medium, *L*: low, *VL*: very low, *SN*: sender node, *RN*: receiver node, *m*: message, *L()*: likelihood function. The goal is to introduce a prediction model for a jammer node targeting an OppNet in a reactive

Table 3
Likelihood controller.

Likelihood controller			
Energy	Buffer	Movement	Likelihood
L	L	L	VL
L	L	M	L
L	L	H	M
L	M	L	VL
L	M	M	L
L	M	H	M
L	H	L	VL
L	H	M	M
L	H	H	H
M	L	L	L
M	L	M	M
M	L	H	H
M	M	L	L
M	M	M	M
M	M	H	H
M	H	L	L
M	H	M	M
M	H	H	H
H	L	L	L
H	L	M	M
H	L	H	M
H	M	L	L
H	M	M	H
H	M	H	VH
H	H	L	L
H	H	M	VH
H	H	H	VH

jamming manner. This model is based on some network performance indicators for identifying the aberrant node activity, namely the number of retransmissions, the energy consumption per node, the resilience (defined as the time it takes for the network to recover to a stable state), and the node's routing table changes. The originality of our proposed solution consists in examining these indicators, which in turn, can affect (directly or indirectly) the energy usage and provide some insights to the network's activity. When the network is jammed, those of the above indicators that have meaningful fluctuations are picked.

4. Performance evaluation of the proposed JADT scheme

The proposed JADT scheme is simulated using the ONE simulator [4] and compared against the F-GSAF protocol [17], in terms of PDR, average latency, delivery ratio, energy consumption, and overhead ratio. It should be emphasized that (1) the *average ratio* is defined as an estimation of the network's load cost in terms of control packets. This parameter affects the amount of collisions, and consequently has a direct impact on the packet retransmissions; (2) the energy consumption if the sum of the remaining energy calculated for each node; and (3) the delivery ratio is the ratio of delivery before and after a jamming attack has occurred. For this metric, the graphics depicts the direct effect of the packet jammers on the packet delivery.

The system model consists of a set of 6 groups of nodes (electric motor cars, pedestrian, bicycles, tram, vehicles, and office workers) that may leave or join the network at any time. The map-Based movement model is utilized by each group with various speed values. The Helsinki city map is used for the simulation area with region dimension 4500 m × 3400 m, segmented into 16 casts. Two wireless interfaces are considered, namely Wi-Fi 802.11ac with a transmission speed of 433 Mbps and a range of 20 m; and Bluetooth 802.16 v4.0, with transmission speed of 2 Mbps and a range of 10 m. The simulation time for one run is 57600 s; the warm-up and cool-down periods for every simulation are respectively 2 h. Also, 8 levels of host density, i.e. 126, 189, 252, 315, 378, 441, 504, 567, with 195 as default number of hosts, are utilized. The device buffer sizes (in Mb) are: 5, 10, 15, 20, 25, 30, 35, 40 Mb, 10 Mb being the default. Different message lifetimes (in mins) are utilized, namely 30, 60, 90, 120, 150, 180, 210, 240, the default being 120 min. For the messages scheduling, a sender and a destination cast are selected uniformly and randomly from the set of nodes and predefined casts. The message payload is set to 500 KB, a new message is generated every 25 to 35 s, and the random scheduling policy is considered. Finally, 5% of malicious nodes are considered for each iteration. Additional simulation parameters are given in Table 4.

Table 5 shows that number of nodes present in different zones, when we injected 5% malicious nodes to the network. All the nodes are divided into three categories based on their behaviour. First, all nodes are in no-jamming zone; and when we start the simulation, all nodes are in Stage 1 (i.e. No Jamming Zone). When the simulation time is 20 min, the jammer is activated, and the changes are seen in the behaviour of the nodes. Few nodes, categorized as *suspicious nodes*, are behaving maliciously. Such type of nodes are put in the so-called Suspicious Zone (Stage 2). If UCL statistical measure value of a particular node is high, then this node is considered as a jamming node and put in the Jamming Zone (Stage 3). Hence, Stage 3 consists all the jamming nodes present in

Table 4
Simulation parameters.

Parameter	Value
Trace format	Standard events reader
Trace fields in each line	5
Communication interface	Bluetooth
Transmission range	10 m
Number of nodes	40
Number of contacts	1210
Simulation time	3600 s
Transmission speed	250 Kbps
Message size	500 Kb up to 1 Mb
Buffer capacity	5 Mb
Movement model	Shortest path
Message Time-to-Live (TTL)	100–300 min
Warmup time	300 s
Number of interfaces	1
Group Send Queue	1

Table 5
Time vs number of nodes present in different zones.

Time	No jamming zone	Suspicious zone	Jamming zone
5	40	0	0
10	40	0	0
15	40	0	0
20	34	5	1
25	32	6	2
30	29	7	4

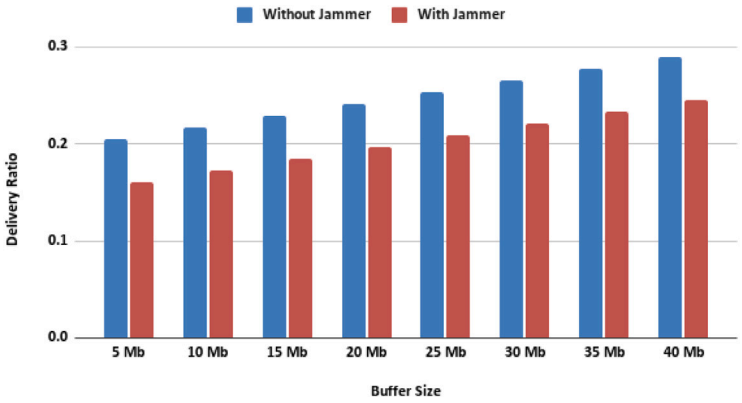

Fig. 1. Delivery ratio vs buffer size.

the simulation environment. We can easily isolate these nodes, and forward the message to the destination without involving the participation of these nodes.

Fig. 1 shows that as the buffer size increases, the delivery ratio increases since the more the buffer size of a node is, the more the messages it can support; and this leads to an increase in the delivery of messages. However, since the jammers are present, the delivery ratio decreases because the jammers try to stop or drop messages in the network. This result shows that the jammers create a large impact in the network performance.

Fig. 2 shows that the jammers increase the overhead ratio because when a message is dropped in the network, it gets reproduce in the source node; and this creases the overhead ratio. This figure also shows that as the buffer size increases, the overhead ratio decreases. This is due to the fact that a bigger buffer size holds the packets for a longer period of time, resulting in less packet drop, i.e. less overhead.

Fig. 3 shows that when the jammers are present in the network, the remaining energy of the nodes are affected due to the fact that a node drains out its energy faster due to continuously dealing with a jammer. This results in low remaining energy in the nodes. Indeed, a node will drain some energy in scanning other nodes, and sending and receiving packets. Because the jammers are present, they continuously send signals to others nodes, making them busy in the network. In turn, the signals receiving nodes continuously drain the energy, results in faster energy drainage.

Fig. 4 shows that as the TTL increases, the delivery ratio increases because the bigger is the TTL of a packet, the higher is the chances of delivering a packet to the destination. This results in increased delivery of the messages. However, when the jammers

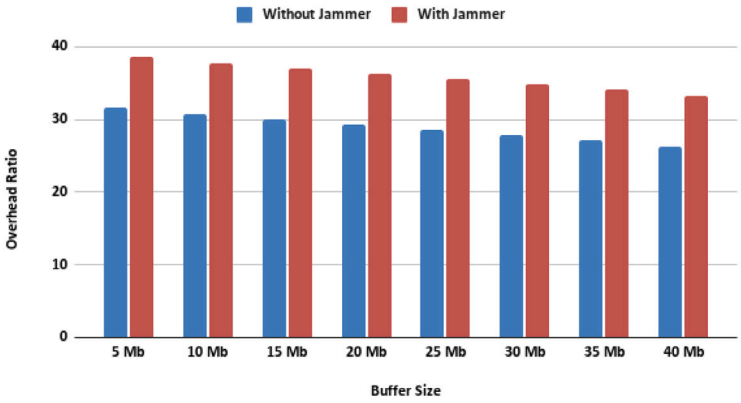

Fig. 2. Overhead ratio vs buffer size.

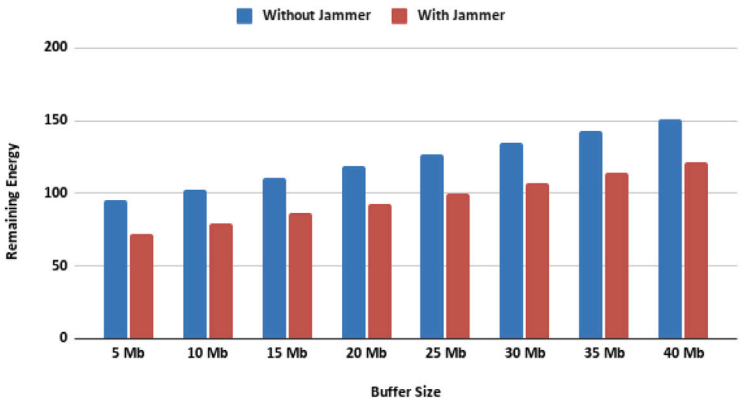

Fig. 3. Remaining energy vs buffer size.

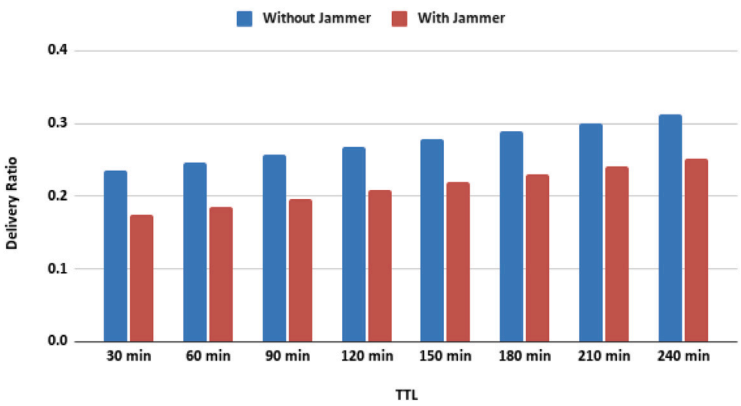

Fig. 4. Delivery ratio vs TTL.

are present, the delivery ratio decreases because these jammers try to stop or drop the messages in the network by keeping the node busy in receiving the false signals sent by these jammers.

Fig. 5 shows that as the TTL increases, the overhead ratio decreases. This is due to the fact that as the TTL of a message is increased, the message stays in the network for a longer period of time, leading to less message drop during this time.

Fig. 6 shows that as the TTL increases, the remaining energy of nodes are decreased in a fast manner. In this case, a node drains out its energy faster due to continuously dealing with a jammer, which results in low remaining energy of nodes.

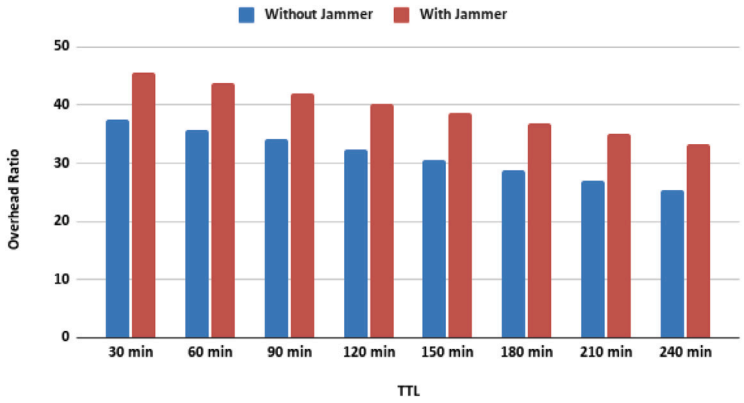

Fig. 5. Overhead ratio vs TTL.

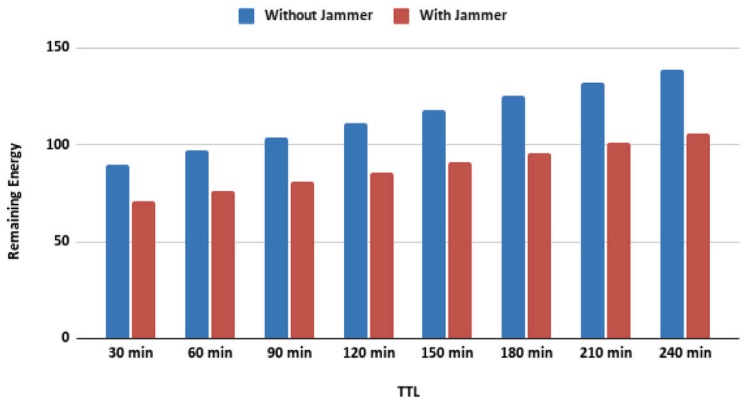

Fig. 6. Remaining energy vs TTL.

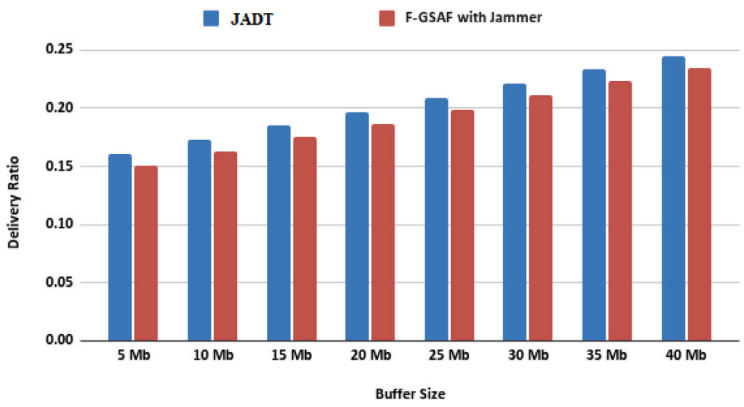

Fig. 7. Delivery ratio vs buffer size for JADT vs. F-GSAF protocols.

Fig. 7 shows that as the buffer size increases, the delivery ratio increases as well. This is because the bigger the buffer size is, the more messages it can store, leading to an increase in the delivery of messages. However, when the jammers are present, the delivery ratio decreases because these jammers try to stop or drop the messages in the network, resulting to less message delivery to the destination.

Fig. 8 shows that as the buffer size increases, the overhead ratio decreases. This is due to the fact that the bigger the buffer size is, the longer it can hold the packets, which results in less packet drop, thereby less overhead.

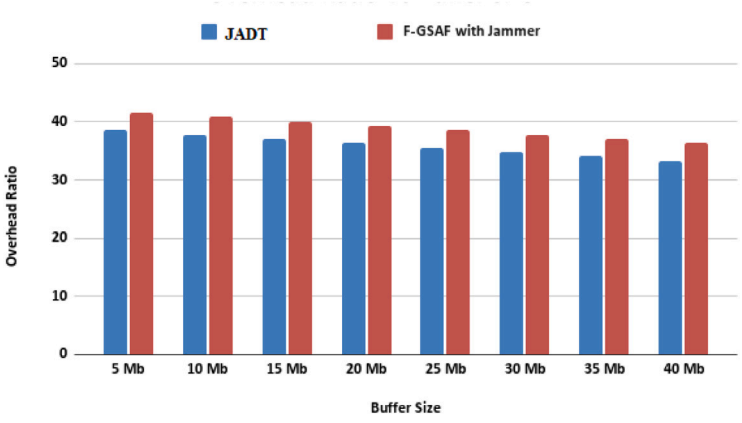

Fig. 8. Overhead ratio vs buffer size for JADT vs. F-GSAF protocols.

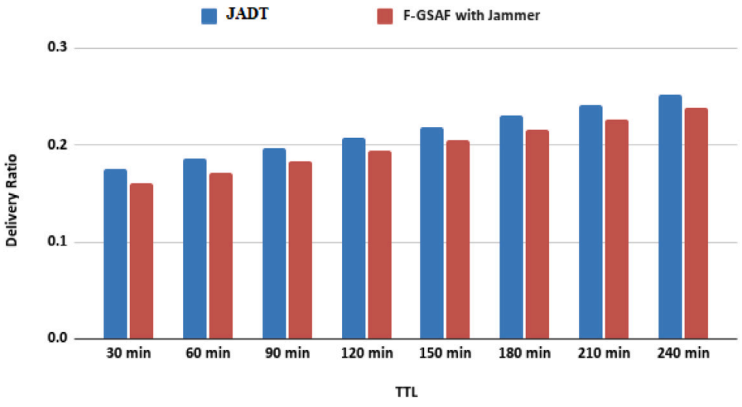

Fig. 9. Delivery ratio vs TTL for JADT vs. F-GSAF protocols.

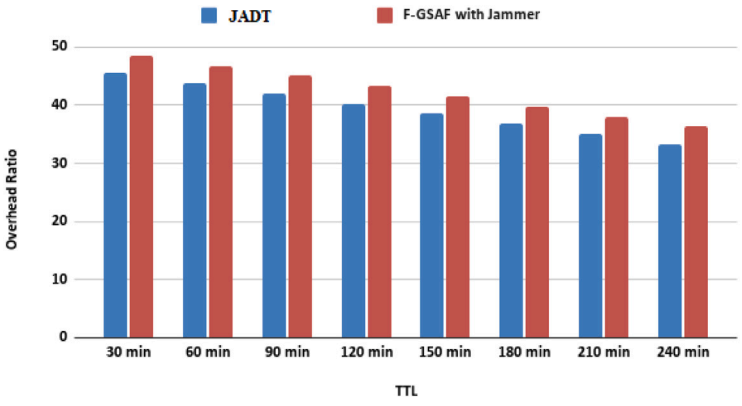

Fig. 10. Overhead ratio vs TTL for JADT vs. F-GSAF protocols.

Fig. 9 shows that as the TTL increases, the delivery ratio increases because the bigger the TTL of a packet, the more are the chances to deliver the packet to the destination. However, when the jammers are present, the delivery ratio decreases because these jammers try to stop or drop the messages in the network. Indeed, JADT outperforms F-GSAF in terms of delivery ratio by 22.10%.

Fig. 10 shows that as the TTL increases, the overhead ratio decreases. This is due to the fact that as the TTL of a message is increased, it stays in the network for a longer period of time, which results in less message drop during this time. It is also observed that in terms of overhead ratio, JADT is 8.75% better than F-GSAF in the presence of jammers. Hence, the above simulations results show that JADT outperforms F-GSAF in the presence of jammers.

5. Conclusion

In this paper, we have proposed a jamming attack detection technique (called JADT) in OppNets that relies on some statistical measures to quarantine the jamming nodes, preventing them from participating to the message routing and forwarding process. Through simulation, we have shown that the proposed JADT scheme outperforms the F-GSAF scheme in terms of packet delivery ratio and overhead ratio, under varying TTL by 22.10% and 8.75% respectively. As future work, a performance comparison of the proposed JADT scheme vs. the F-GSAF scheme on real mobility traces models can be investigated.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Nessrine Chakchouk, A survey on opportunistic routing in wireless communication networks, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2214–2241.
[2] El Houssaini, Mohammed-Alamine, Abdessadek Aaroud, Ali El Hore, Jalel Ben-Othman, Detection of jamming attacks in mobile Ad Hoc Networks using statistical process control, Procedia Comput. Sci. 83 (2016) 26–33.
[3] Zhuo Lu, Wenye Wang, Cliff Wang, Modelling, evaluation and detection of jamming attacks in time-critical wireless applications, IEEE Trans. Mob. Comput. 8 (2013) 1746–1759.
[4] Ari Keränen, Jörg Ott, Teemu Kärkkäinen, The ONE simulator for DTN protocol evaluation, in: Proceedings of the 2nd International Conference on Simulation Tools and Techniques, Rome, Italy, 2009, 1–0.
[5] Ala Altaweel, Radu Stoleru, Guofei Gu, Arnab Kumar Maity, Collusivehijack: A new route hijacking attack and countermeasures in opportunistic networks, in: Proc. of IEEE Conference on Communications and Network Security (CNS), IEEE, Washington D.C. USA, 2019, pp. 73–81.
[6] Mohamed Abdel Raheem, Mohammad Mahmoud Abdellatif, Cooperative anti-jamming for secondary opportunistic networks: A Colonel Blotto game model, in: 13th IEEE Intl. Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, Rome, Italy, 2017, pp. 1–8.
[7] Iain Parris, Tristan Henderson, Friend or flood? social prevention of flooding attacks in mobile opportunistic networks, in: Proc. of IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE, Madrid, Spain, 2014, pp. 16–21.
[8] G.S. Kasturi, Ansh Jain, Jagdeep Singh, Detection and classification of radio frequency jamming attacks using machine learning, J. Wirel. Mob. Netw., Ubiquitous Comput. Dependable Appl. (JoWUA) 11 (4) (2020) 49–62.
[9] K.C. Lalropuia, Vandana Gupta, A Bayesian game model and network availability model for small cells under denial of service (DoS) attack in 5G wireless communication network, Wirel. Netw. 26 (1) (2020) 557–572.
[10] Jagdeep Singh, Sanjay Kumar Dhurandher, Isaac Woungang, Shivin Diwakar, Periklis Chatzimisios, Energy efficient multi-objectives optimized routing for opportunistic networks, in: ICC 2021-IEEE International Conference on Communications, Montreal, Canada, IEEE, 2021, pp. 1–6.
[11] G.S. Kasturi, Ansh Jain, Jagdeep Singh, Machine learning-based RF jamming classification techniques in wireless ad hoc networks, in: International Conference on Wireless Intelligent and Distributed Environment for Communication, Durban, South Africa, 2020, pp. 99–111.
[12] Sanjay Kumar Dhurandher, Jagdeep Singh, Petros Nicopolitidis, Raghav Kumar, Geetanshu Gupta, A blockchain-based secure routing protocol for opportunistic networks, J. Ambient Intell. Humaniz. Comput. (2021) 1–13.
[13] Haythem Bany Salameh, Safa Otoum, Moayad Aloqaily, Rawan Derbas, Ismaeel Al Ridhawi, Yaser Jararweh, Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks, Ad-Hoc Netw. 98 (2020) 102035.
[14] Demin Gao, Shuai Wang, Yunhuai Liu, Wenchao Jiang, Zhijun Li, Tian He, Spoofing-jamming attack based on cross-technology communication for wireless networks, Comput. Commun. (2021) 1–10.
[15] Sudip Misra, Sanjay Kumar Dhurandher, Avanish Rayankula, Deepansh Agrawal, Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks, Comput. Electr. Eng. 36 (2) (2010) 367–382.
[16] Jonathan Ng, Ziyuan Cai, Ming Yu, A new model-based method to detect radio jamming attack to wireless networks, in: 2015 IEEE Globecom Workshops (GC Wkshps), IEEE, 2015, pp. 1–6.
[17] Khuram Khalid, Isaac Woungang, Sanjay Kumar Dhurandher, Jagdeep Singh, Joel J.P.C. Rodrigues, Energy-efficient check-and-spray geocast routing protocol for opportunistic networks, in: Information 2020, 2020, pp. 1–18.