Journal of Network and Computer Applications 61 (2016) 133–141

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Null-frequency jamming of a proactive routing protocol in wireless mesh networks

Shruti Lall*, B.T.J. Maharaj, P.A. Jansen van Vuuren

Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa

ARTICLE INFO

Article history:
Received 5 December 2014
Received in revised form
10 October 2015
Accepted 20 October 2015
Available online 4 November 2015

Keywords:
Null-frequency
Optimised link state routing
Proactive routing
Wireless jamming
Wireless mesh networks

ABSTRACT

Disrupting network communication of adversarial networks is of increasing interest and importance. The use of jamming devices is a viable method for disabling the communication capabilities of enemy networks. This paper proposes a jamming technique which targets the periodic nature of the routing protocol residing in the network layer. The technique is based on the concept of null-frequency jamming which refers to periodic attacks targeting specific protocol period/frequency of operation. The effects of this jamming technique are investigated in stack, half-diamond, full-diamond, full-mesh and random topologies employing the optimised link state routing protocol. OMNeT++ 4.3 was chosen as the network simulation platform in which to conduct the investigations. It was found that when jamming at the 2 s null-period for a length of 0.5 s, there was a substantial drop in overall network performance. This technique was then compared to constant, deceptive and random jamming techniques and was shown to outperform the techniques in terms of the energy expended by the wireless nodes in the networks.

1. Introduction

Wireless networks are gaining widespread use and popularity because of their progressive increase in affordability and convenience. Owing to the improved facilitation of communication and data transfer, wireless networks are being deployed in numerous modalities, ranging from wireless local area networks (WLANs) to mesh and sensor networks (Xu et al., 2005). Wireless networks are often seen as a more attractive option to their wired network counterpart due to their increased mobility, expandability, cost efficiency and ease of integration. As a result of the need for mobility, data is broadcast using radio technology, which implies that any receiver in range will be able to, not only listen in on the transmission, but manipulate or alter the ongoing transmission. Wireless mesh networks (WMNs) are networks which consist of peer-to-peer wireless mobile node interconnections that collectively form an intelligent, large-scale and broadband wireless network. The shared and easy to access medium, while being the most beneficial characteristic of WMNs, makes it extremely easy for an adversary to launch an attack. Consequently, jamming attacks are most effective in these networks. Jamming is defined to be any activity that seeks to deny service to legitimate users by generating signals, noise or malicious packets in an effort to disrupt communication services (Prasad and Thuente, 2011). The device that transmits jamming pulses, signals and packets to disrupt the service is known as a jammer or a jamming node. Wireless network jamming has essential military application for disrupting enemy battlefield communication services (Commander et al., 2007). It is therefore pertinent that the jamming scheme is energy efficient and difficult to detect in order to ensure their longevity. Although security and energy efficiency are two research areas that have largely been addressed as separate entities, it is important to consider and propose energy-aware attack schemes that jointly address energy efficiency and the impact of the attack (Palmieri et al., 2015). A jamming attack is classified as being effective when it is energy efficient, has a low probability of being detected and has a high level of undesirable impact on network operation. There are a number of different types of jamming attacks namely, *constant jamming*, *deceptive jamming*, *random jamming*, *reactive jamming*, and *scheduled jamming* (Xing and Wang, 2006).

Constant jamming is the simplest kind of jamming attack in that it continually transmits an interference signal, in order to degrade the capacity of the wireless channel (Xing and Wang, 2006). It disregards the protocols in the physical and link layers of the nodes. The main disadvantage of constant jammers is that the energy consumption is excessive, as it continually transmits high-power noise. This causes significant interference which prevents the reliable delivery of data packets on the channel (Altman et al., 2009). *Deceptive jamming* is an attack in which the jammers continually inject legitimate packets with valid headers into the

* Corresponding author.
E-mail addresses: shruti.lall11@gmail.com (S. Lall), sunil.maharaj@up.ac.za (B.T.J. Maharaj), pieter.jansenvanvuuren@up.ac.za (P.A.J.v. Vuuren).

http://dx.doi.org/10.1016/j.jnca.2015.10.009
1084-8045/© 2015 Elsevier Ltd. All rights reserved.

channel. As a result, the receiving node thinks that it is receiving a legitimate packet and will therefore be restricted to the receiving mode. As with *constant jamming*, *deceptive jamming* is a continuous jamming attack and as such, it expends a large amount of energy to continually send out these packets. In addition, continuous jammers are easy to detect as a result of the constant presence of these high-power interference signals. There are numerous studies detailing methods on how to mitigate these types of attacks. Examples include the use of spread spectrum communications (Belouchrani and Amin, 2000) and spatial retreats (Wood et al., 2004) to aid in mitigation as well as mitigation through the localisation and removal of the jamming nodes (Proano and Lazos, 2004).

Random jamming addresses the large energy expenditure of *constant* and *deceptive jamming* by alternating the jammer between sleep mode and jamming mode. The random jammer performs the attack for a random period after which it shuts down for an arbitrary amount of time before continuing the attack. However, *random jamming* attacks are not as effective in degrading the performance of the network as continuous jamming attacks (Wang and Wyglinski, 2011). *Reactive jamming* involves listening to the network transmissions, deciphering the packets and reacting to the subsequent network state (Xing and Wang, 2006). This type of attack proves to be more difficult to implement than other attacks as it requires the ability to decode the packet information and react accordingly with malicious intent. The primary advantage of a reactive jammer is that it is more difficult to detect, however, it does not conserve any more energy than continuous jammers as it constantly needs to listen to the channel. Scheduled jammers send out bursts of jamming packets for a specific period of time, based on a predefined schedule (Balakrishnan et al., 2012). This type of attack does not require packet decoding capabilities or reactive intelligence. It is also significantly more energy efficient than both continuous and reactive jammers. The effectiveness of this attack depends on the pre-set schedule of the jamming packet bursts. This aims to target the timer-based operation of the protocols implemented in the physical layer, transport layer or network layer of the wireless nodes.

A large portion of the work done on jamming in wireless networks focuses on jamming at the physical and link layers (Ahmed and Huang, 2009). This includes the use of intelligent jammers that exploit link layer protocol rules (Gupta et al., 2002; Muogilim et al., 2011; Kim et al., 2013; Avelara et al., 2014; Xu and Saadawi, 2002). There have been several studies of protocol-aware jamming attacks on the link layer, while fewer studies focused on the network layer (Jae-Joon and Jaesung, 2013). One of the main reasons for the lack of sufficient study on network layer jamming strategies is the notion that a routing protocol can effectively construct alternate routes. This implies that the routing protocol can exclude routes involving the jamming nodes, and thus, provide reliable data delivery defeating the purpose of the jamming attack (Jae-Joon and Jaesung, 2013). However, certain vulnerabilities of routing protocols, resulting from the use of internal states and timers for network coordination, can be exploited and used to increase the efficiency of the jamming nodes. Jamming at the network layer includes sending extra control or data packets to degrade network performance as was presented in Desilva and Boppana (2005) where a malicious node constantly initiates route discovery requests but ignores any replies to them. A jamming node can also act as the originator of a large number of junk data packets, which are then injected into a path and result in resource deprivation of intermediate routing nodes (Gu et al., 2005). An added advantage of the network layer based jamming scheme is that energy-saving techniques and methods, which are largely targeted for higher layers, such as the transport and network layer, can be easily adopted to increase the energy efficiency of the proposed jamming attack (Oulmahdi et al., 2014; Ricciardi et al., 2015).

Balakrishnan et al. (2012) have investigated null-frequency jamming (NFJ) in wireless ad hoc networks employing a reactive routing protocol, namely, the dynamic source routing (DSR) protocol. The investigation proposed by Balakrishnan et al. is based on the concept of low-rate DoS attacks targeted at transmission control protocol (TCP) flows, named shrew attacks, which were proposed by Kuzmanovic (2006). NFJ is a scheduled jammer which targets the periodic operation of the routing protocol residing in the network layer. It is energy efficient and difficult to detect as a result of the short, infrequent, low-power jamming pulses broadcast by the jammer.

The jamming technique proposed in this paper is unique with respect to the approach and method used to implement the NFJ. The effectiveness of the proposed technique is investigated in WMNs employing a proactive routing protocol. NFJ has only previously been tested in wireless ad hoc networks which employed a reactive routing protocol as shown in Balakrishnan et al. (2012). Furthermore, the effectiveness of the jamming technique presented in this paper is demonstrated by analysing not only the overall throughput of the network, but also the energy expended by the jamming nodes, thereby enhancing the uniqueness of this paper. In addition, this paper reports on the probability of detecting the jamming nodes in comparison to other jamming techniques namely, *constant jamming*, *random jamming* and *deceptive jamming*.

In summary, this paper investigates the effectiveness of NFJ targeting the proactive optimized link state routing (OLSR) protocol for various WMN topologies namely, stack, half-diamond, full-diamond, random, and full-mesh topologies. OLSR is an optimisation of a pure link state protocol and makes use of multipoint relaying technology to efficiently and economically disseminate control information throughout the network. It is therefore well suited for large and dense wireless mesh networks (Jacquet and Muhlethaler, 2001). The effects of changing several parameters pertaining to the jamming technique are analysed in terms of network performance. A comparison of the NFJ to constant, deceptive and random jamming techniques is also presented.

2. Method

The proposed jamming technique targets the OLSR protocol in order to prevent the reception and transmission of protocol control packets from neighbouring nodes. The control packets that are targeted are the neighbour discovery packets, or the *Hello* packets. As a result, incomplete topological information is distributed throughout the network. This then facilitates the propagation of partial routing tables amongst the nodes in the network. Due to the fact that not all routes are available, packets are dropped and a significant degradation in network communication is observed. It is important to note that this jamming technique can potentially be applied to any periodic routing protocol in which the protocol specific neighbour discovery packets are targeted. Examples of period routing protocols include the Routing Information Protocol (RIP), Internet Gateway Routing Protocol (IGRP), and Exterior Gateway Protocol (EGP). The Ad-hoc On-Demand Distance Vector (AODV) protocol and variations thereof share some common characteristics with proactive routing protocols and can also be targeted by this jamming attack (Ong et al., 2011).

2.1. Objective

The objective of this work is to propose and investigate a jamming technique that is energy efficient, has a low probability of detection and has a high level of impact on network communication degradation. This technique is based on NFJ as proposed by Balakrishnan et al. (2012) which aims to exploit the periodic nature of the routing protocol. The jamming technique involves sending jamming packets based on a predefined schedule to affect the transmission of control packets in order to have a detrimental effect on the throughput of the network.

2.2. Null-frequency jamming

The NFJ node is designed to be a malicious node that employs an interference mechanism in addition to acting as a non-malicious internal node. All nodes will implement the user datagram protocol (UDP) in the transport layer, the OLSR protocol in the network layer and the IEEE 802.11 protocol in the link-layers as seen in Fig. 1.

The wireless nodes in the network employ the IEEE 802.11 distributed coordination function (DCF) protocol in the link layer. The IEEE 802.11 DCF is one of the most common wireless communication standards and governs the rules regarding the exchange of data amongst nodes via radio signals. The standard employs the carrier sense multiple access/collision avoidance (CSMA/CA) protocol with a binary exponential backoff scheme that specifies how the nodes access the shared wireless medium. CSMA/CA requires that the wireless nodes sense the channel before that transmit a packet. If the channel is sensed to be idle for a period of time greater than the distributed interframe space (DIFS), then the node proceeds with the transmission. According to the IEEE 802.11g standard, the DIFS period is set to 50 s. If the channel is busy during the sensing period, the node defers its transmission until the channel is sensed to be idle again. The node waits for the channel to remain idle for a random backoff period before trying to transmit again. The backoff period is calculated as shown in the following equation:

$$Backoff = random(0, CW - 1) \times aSlotTime, \tag{1}$$

where *CW*, the *contention width*, is an integer in the range of *CWmin* to *CWmax*. The *CW* is initially set to *CWmin* and is doubled each time a collision is detected on the channel, until the *CW* equals *CWmax. CWmin* and *CWmax* is set to 31 and 1023 respectively, based on the IEEE 802.11g standard. The slot time (*aSlotTime*) with which this random integer is multiplied, is set to 9 s. Upon successful data transmission, an acknowledgement (ACK) packet is sent from the destination node to the source node; if no ACK packet is received by the source node, the data is assumed to be lost and a retransmission is scheduled.

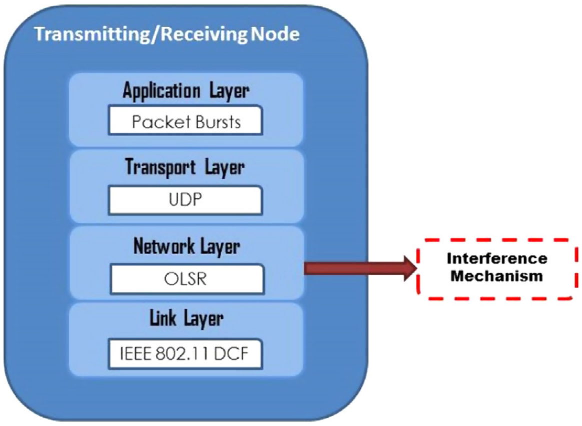

Fig. 1. Block diagram of wireless node with NFJ mechanism implemented in the network layer.

The routing protocol which is employed by the wireless nodes in the network is the OLSR protocol. OLSR relies on the exchange of control packets at regular intervals in order to maintain topology information of the network at each node. OLSR is a proactive, or table-driven protocol, in that it employs the periodic distribution of control messages to enable the immediate retrieval of routes by nodes in the network. There are no further messages, apart from the periodic control messages, sent when a link failure or an additional link is detected.

OLSR is an optimisation of a pure link state protocol as it compacts the amount of information sent in the control packets and also reduces the overall retransmissions to broadcast the control messages throughout the network. This optimisation is achieved through the use of nominated multipoint relays (MPRs) which are responsible for broadcasting control packets through the network. Each node nominates a set of nodes to act as the MPRs. The MPRs are selected in such a way that all the neighbours that are two hops away are only able to be accessed through the MPRs.

Neighbour sensing and routing table calculations are achieved through the periodic exchange of *Hello* and *Topology Control* (*TC*) messages. *Hello* messages contain information about the neighbours of the node and their link status. These messages are received by all one-hop neighbours every 2 s with a positive 0.5 s jitter. The selection and declaration of the MPRs is accomplished through the use of the *Hello* Packets. The *TC* messages are sent every 5 s with a 0.5 s jitter and are used in the construction of the intra-forwarding database each node maintains. It is used to declare the MPR selector set which is a list of neighbours that have selected the sender node as a MPR. The routing table for each node is computed based on the information of the MPRs that the node records from the *TC* messages.

The transport layer protocol is the UDP connectionless protocol. A connectionless protocol implies that no prior arrangement is required between the source and destination nodes. It is responsible for sending data traffic, in the form of datagrams, to nodes within the network. The application layer sends out 512-byte packets at a specified interval to randomly chosen nodes in the network.

The jamming node is designed to be internal to the network in that it acts as an existing legitimate node, and implements jamming functionality within the network layer. This type of node calls the jamming functions to send jamming packets at the null-frequency in addition to sending out regular control and application packets. The additional jamming functions will be incorporated into the network layer of the node and will only be called if that particular node has been selected as the jamming node. The jamming node will send a stream of packets for a particular period of time, in essence, preventing the transmission or reception of neighbour discovery packets. This will deny the victim node the ability to construct a proper routing table, effectively disconnecting it from the network.

The jamming node is designed to transmit a stream of jamming packets for the jamming length specified, at the scheduled jamming period. The jamming scheme is shown in Fig. 2. The packets continuously being sent out by the jamming node, for the jamming length, are the *Hello* packets generated by the nodes themselves. This implies that the jamming node does not use any invalid packets to jam the network and in effect, behaves as a scheduled deceptive jammer.

3. Simulation overview

3.1. Experimental setup

NFJ was tested in various WMN topologies namely, the stack, half-diamond, full-diamond, full-mesh and random topologies.

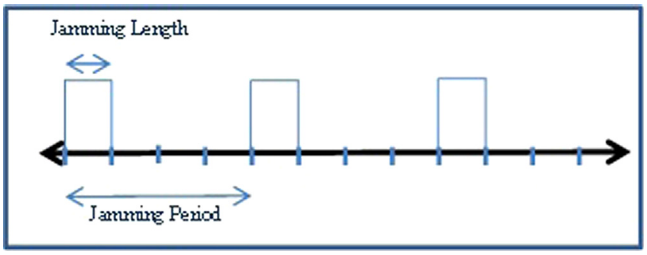

Fig. 2. Jamming stream transmitted for a specified jamming length at a scheduled jamming period.

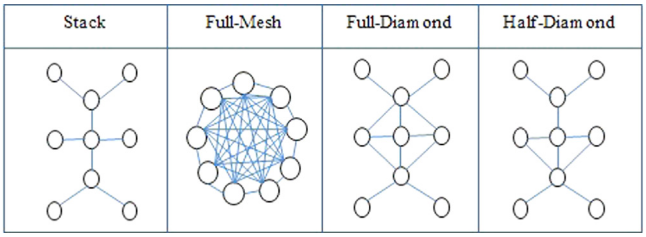

Fig. 3. Wireless mesh network topologies used in evaluating the performance of the NFJ technique.

The four fixed 9-node topologies are shown in Fig. 3. It was also tested in random topologies of up to 20 nodes. In such topologies, the locations of the jamming nodes are randomly placed throughout the area with each node having the same coverage area. The nodes are placed in an area with the chosen dimensions of 250 m by 250 m. Given that the number of nodes in any WMN topology is limited to 20 nodes, the chosen area size is considered to be reasonable. It allows for sufficient investigation into the effects of NFJ in WMNs to be conducted without the simulation utilising an excessive amount of time and resources.

The most effective location of the jammer was determined for each of the topologies by using the packet loss ratio (PLR) as the metric to measure the efficiency of the jamming attack. Each node in the networks was set as the jammer after which the simulation was run and the PLR noted. The node that resulted in the highest PLR exhibited by the network was deemed as the most effective jammer for that particular topology. The three metrics used to measure the effectiveness of the jamming under various conditions is a measure of the throughput of the network, the PLR experienced by the network and the average end-to-end delay the application packets undergo.

The throughput of the network is calculated using the total bytes received by each node. The size of the application packets received by each node is recorded during the simulation run. The throughput for the entire network is calculated using the following equation:

$$Throughput = \sum_{k=0}^{n-1} \frac{(ReceivedBytes)_k}{Simulation\ RunTime} \tag{2}$$

where n is the total number of nodes in the network and k is the current node number. The average throughput is calculated for multiple simulation runs for the topologies.

In order to determine the total PLR experienced by the network, the following equation is used:

$$PLR = \frac{\sum_{k=0}^{n-1}(P_{sent})_k - \sum_{k=0}^{n-1}(P_{received})_k}{\sum_{k=0}^{n-1}(P_{sent})_k} \tag{3}$$

where n is the total number of nodes in the network and k is the current node number. The total packets sent, P_{sent} , and the total packets received, $P_{received}$, by each node in the network are used in the calculation of the PLR for the entire network.

The end-to-end delay is the time taken for an application packet to reach its destination. The time is recorded for each packet transmitted for all the nodes in the network. The average end-to-end delay of all the application packets for each node is then calculated. The end-to-end delay is summed for all the nodes and the average for the network is obtained. This value is calculated for all the simulation runs and averaged over the simulation runs.

Numerous simulations with the same jamming parameters and configuration are run in order to obtain mean values for the PLR, throughput and end-to-end delay. This ensures that the data is statistically viable to therefore give a better indication of the true performance of the network under the varying jamming conditions.

3.2. Simulation model

OMNeT++ 4.3 with the INET framework (OMNET) has been chosen as the platform to simulate NFJ in the WMNs. Each of the layers as shown in Fig. 1 has been programmed for all the wireless nodes in the network. If a particular node has been chosen as the jamming node, the wireless node additionally sends out jamming packets for the jamming length and at the jamming period specified. The jamming ability of a node lies in the network layer along with the routing protocol. The parameters associated with each layer and pertaining to the operation of NFJ in the network are given in Table 1.

4. Results and discussion

4.1. Effect of jamming period

The jamming period of the jamming stream was varied from 0.5 s to 5 s in increments of 0.25 s for each of the topologies. The average throughput as calculated in Eq. (2) is plotted for each of the topologies and is shown in Fig. 4. The jamming burst length is set to 0.5 s so as to jam the entire period in which *Hello* packets are sent by the neighbouring nodes. The plots for the stack, half-diamond and full-diamond topologies, after setting the most effective jammer to send out the jamming packets, follow a relatively similar shape. There is a significant drop in the throughput when the jamming period is 0.5 s, 1 s and 2 s. This corresponds to the expected null-period of 2 s and its factors. The average throughput plot for the random topologies follows the same shape as with three above-mentioned topologies, however the throughput at the null-period and its factors, is higher. This is due to the fact the number of nodes in such topologies is higher than in the fixed topologies, as well as that the jamming node is randomly chosen, which implies that the jamming node may not be placed

Table 1
Parameters used in simulated network.

Layer	Parameter	Value
Application layer	Start time	15 s + 0.1 s jitter
	Send interval	2 s + 0.1 s jitter
	Message length	512 Bytes
Network layer	*Hello* interval	2 s + 0.5 s jitter
	TC interval	5 s + 0.5 s jitter
Network layer	Standard	IEEE 802.11g
	Bit rate	54 Mbps
	Basic bit rate	6 Mbps
	CWMin	31
	CWMax	1023
	Slot time	9 μs
	DIFS	50 μs
	Frequency	2.4 GHz
	Radio sensitivity	−85 dBm

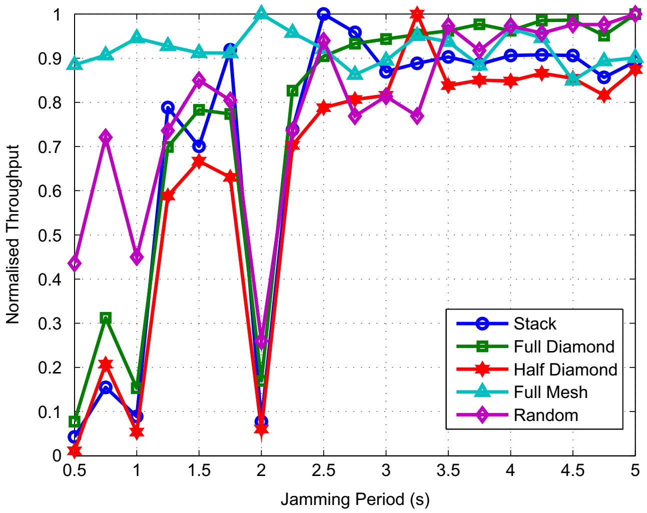

Fig. 4. Plot of network throughput against the jamming period.

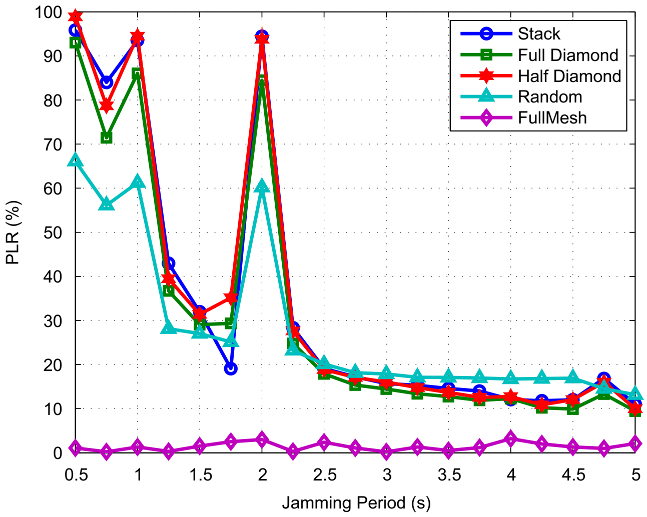

Fig. 6. Plot of the overall network PLR against the jamming period.

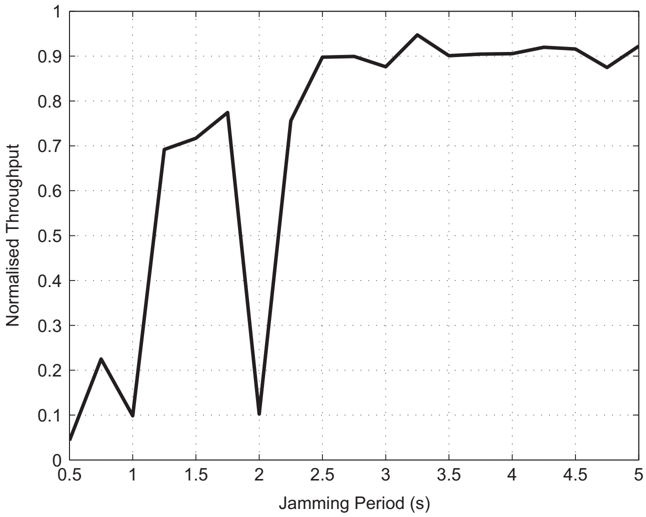

Fig. 5. Plot of average network throughput against the jamming period for fixed topologies.

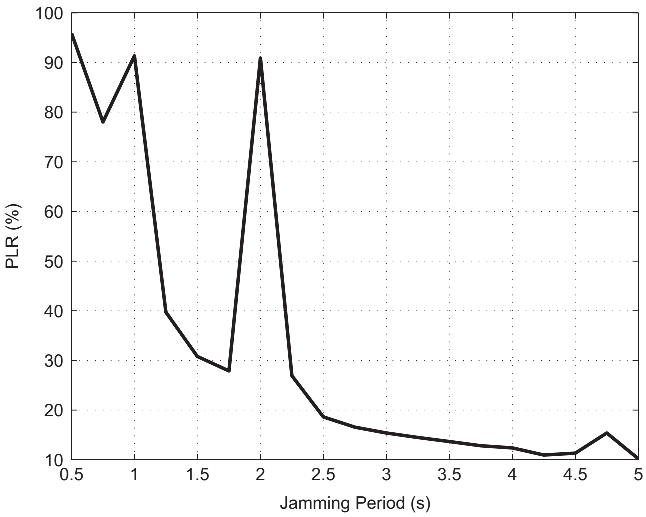

Fig. 7. Plot of the average overall network PLR against the jamming period for fixed topologies.

in an optimal location for the particular random topology. The plot for the full-mesh network in which the jamming node was randomly chosen, shows a fairly high and stable throughput and is not affected by the jamming. This is because all the nodes are directly connected with each other and as a result, there is no additional computation regarding the calculation of routes necessary from the OLSR protocol. The NFJ scheme which targets the routing protocol thus has no effect in such a configuration. The effect of jamming in such a topology is therefore not considered for further investigation.

The average throughput of the three fixed topologies is depicted in Fig. 5 and serves as means of illustrating a summarised effect the jamming period has on the throughput of the WMNs. The results validate the claim that when jamming at the null-period, the throughput of the network is near-zero. The frequency of the jamming attack which results in such severe network communication degradation is termed as the null-frequency.

The average PLR plotted against the jamming period for the five different topologies can be seen in Fig. 6. The graph depicts an inverse behaviour to that shown in Fig. 4. A high PLR indicates a high level of jamming effectiveness which corresponds to a low throughput value. A peak in the average PLR is seen at the null-period and its factors. The PLR peaks at approximately 92% for the fixed topologies. This is seen in Fig. 7 which depicts an average PLR for the fixed topologies.

The average end-to-end delay associated with the application packets for the varying jamming period is shown in Figs. 8 and 9. Fig. 8 shows the delay for the different topologies and Fig. 9 is an average plot of the end-to-end delay for the fixed topologies excluding the full-mesh topology. A slight peak in the end-to-end delay is observed at the null-period for the application packets that do manage to reach the destination nodes. This is indicative of poor network performance as a result of the NFJ. The end-to-end delay is significantly higher when the jamming is in the period from 0.5 s to 1 s. This results from the fact that the jamming packets interfere with the application packets themselves and not just the control packets.

4.2. Effect of jamming length

The effect of changing the jamming length was investigated in a similar manner as was conducted for the jamming period. The average plot of the throughput and the PLR for the different topologies is shown in Figs. 10 and 11 respectively. The jamming length was varied from 0.3 s to 0.8 s. There is a linear decrease in the throughput when the jamming length is between 0.3 s and

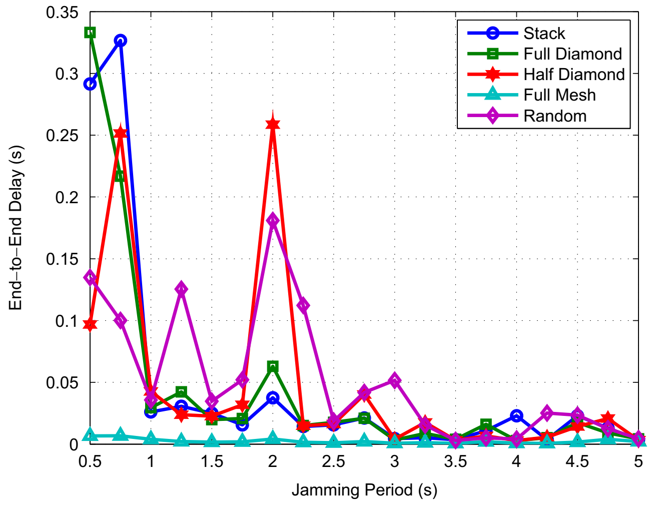

Fig. 8. Plot of the average end-to-end delay against the jamming period.

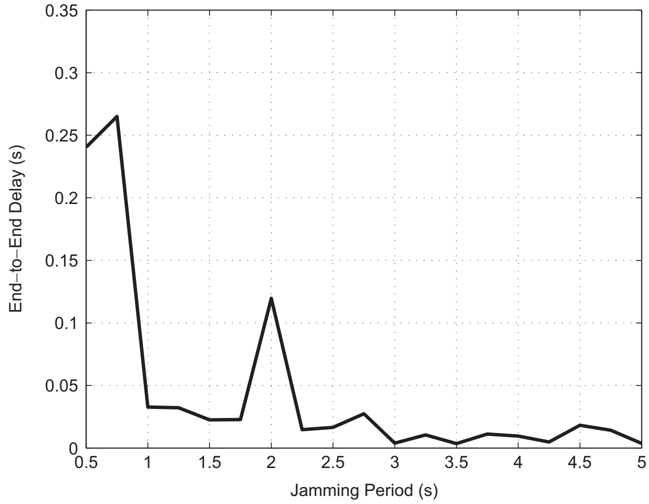

Fig. 9. Plot of the average end-to-end delay for the fixed topologies against the jamming period.

0.5 s, after which it stabilises. The inverse effect can be seen for the PLR plot which shows a linear increase from 0.3 s to 0.5 s and stabilisation from 0.5 s onwards. This is because the *Hello* packets are sent with a 0.5 s jitter, and so the jamming is most effective when the jamming length is 0.5 s or longer. This implies that a high percentage of the *Hello* packets that are sent out during this 0.5 s period are blocked.

4.3. *Effect of jamming stream start point*

To further verify that as a result of only jamming the *Hello* packets of neighbouring nodes, a drop in the overall throughput of the network is observed, the starting point of the jamming stream is altered while maintaining the 2 s jamming period and 0.5 s jamming length. As the *Hello* packets are sent periodically every 2 s, with a 0.5 s jitter, moving the staring point of the jamming stream results in partial or no jamming of the *Hello* packets. Fig. 12 illustrates the effect that the change in the starting point of the jamming stream has in relation to the periods in which *Hello* packets are sent by nodes.The shaded region is the time period that *Hello* packets are sent by all the wireless nodes, the jamming stream is overlayed and depicted as a square wave. The starting time in the first timeline is at 2 s, and therefore the jamming stream lies directly over the *Hello* message sending interval. The jamming stream is then shifted by 0.25 s in the timeline below, this means that half the *Hello* message sending interval is being jammed. The timelines below show the effect of shifting the jamming stream by a further 0.25 s each time. The jamming stream start point is altered from 2 s to 4 s for the stack, half-diamond, full-diamond and random topologies and the effects on the throughput are shown in Fig. 13.

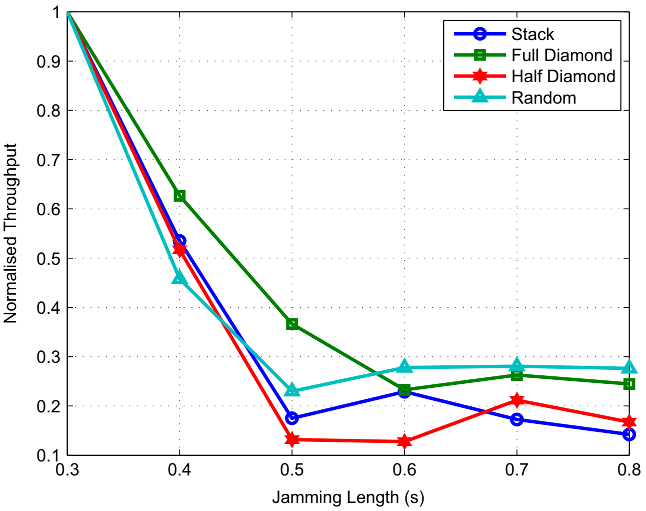

Fig. 10. Plot of network throughput against the jamming length.

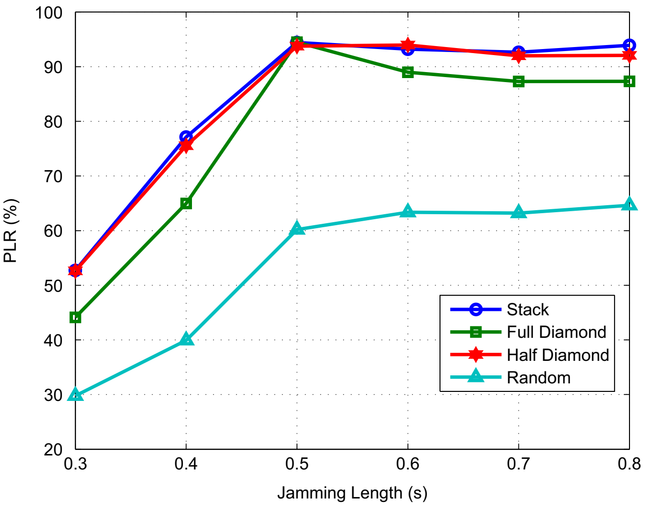

Fig. 11. Plot of the overall network PLR against the jamming length.

A convex parabolic shape is observed for each of the plots in Fig. 13. This corresponds to the notion that the jamming effectiveness is directly proportional to the percentage of control packets that are blocked.

4.4. *Optimal jamming performance*

Table 2 summarises the effect the proposed jamming technique has on the overall network performance. A significant increase in both the PLR and end-to-end delay is exhibited for all network topologies except the full-mesh network topology. In the full-mesh network topology, a jamming node needs to jam significantly more channels as opposed to the other topologies. In addition, each node is directly connected to every other node in the network; this significantly increases the probability of a particular node obtaining information about neighbours that are two

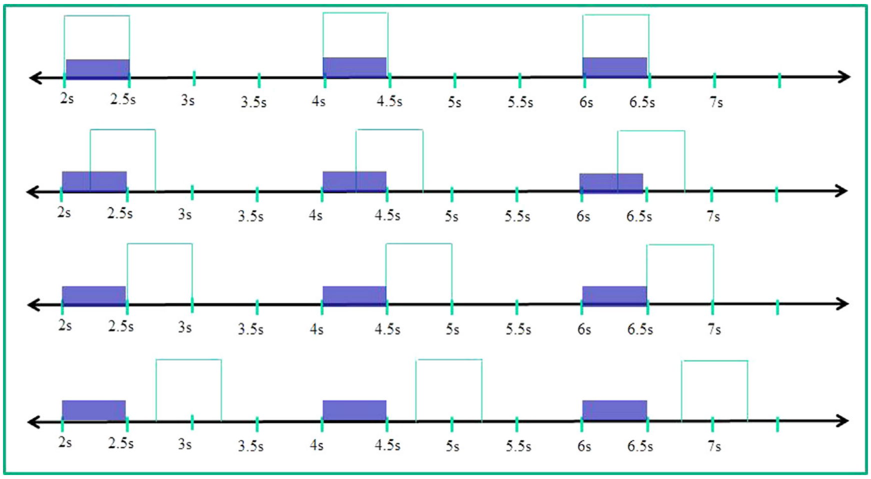

Fig. 12. Timelines illustrating the effect of changing the starting point of a jamming stream.

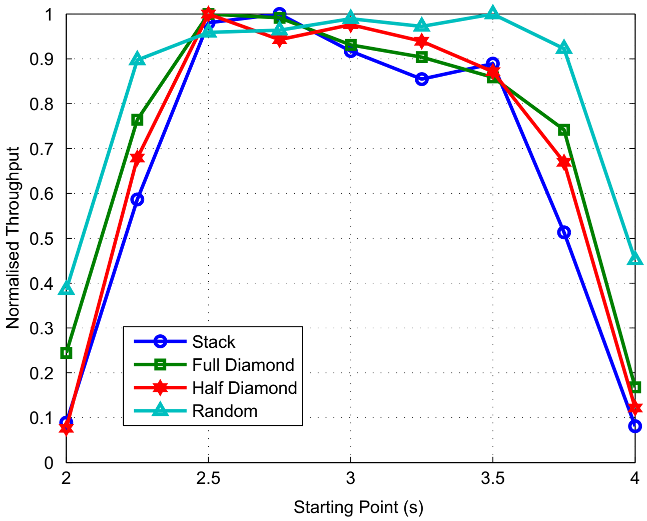

Fig. 13. Plot of network throughput against the jamming stream starting point.

Table 2
Jamming performance analysis.

Topology	Increase in PLR (%)	Decrease in throughput (%)	Increase in end-to-end delay (%)
Stack	754.6	92.3	971.4
Half-diamond	836.8	93.9	$> 8 \times 10^3$
Full-diamond	792.08	85.6	$> 2 \times 10^3$
Full-mesh	17.7	0.1	562.4
Random	357.8	74.1	$> 5 \times 10^3$

hops away, thereby gaining knowledge of the topology of the network. A large drop in the throughput is experienced when jamming at the null period of 2 s with a jamming length of 0.5 s and a starting time of 2 s. This is seen for the stack, half-diamond, full-diamond and random WMN topologies.

Table 3 provides a statistical analysis on the results obtained from the investigations conducted on the fixed networks. This includes the stack, full-diamond and half-diamond topologies. It serves as means of analysing the jamming technique when jamming at the null-period of 2 s with a 0.5 s jamming length. The mean value of the PLR is greater than 90% whereas the mean throughput value drops to approximately 10%. The relatively low standard deviation and variance, in comparison to the mean, root-mean square and median for the two metrics, indicate a detrimental impact on network communication degradation when jamming at the optimal configuration.

Table 3
Statistical analysis of optimal jamming configuration.

Statistic	PLR(%)	Normalised throughput
Mean	90.93	0.1024
Standard deviation	5.56	0.0588
Variance	30.96	0.0035
Root-mean square	91.01	0.1131
Median	93.78	0.0770

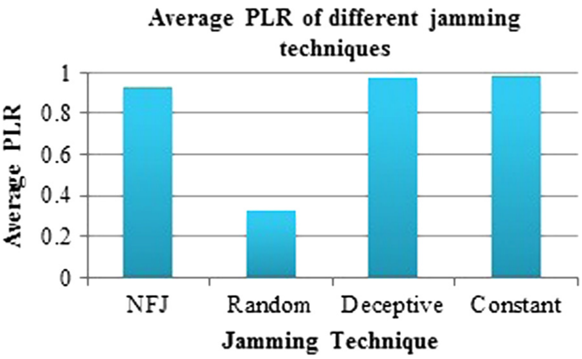

Fig. 14. Comparison of the performance of NFJ to random, deceptive and constant jamming techniques in terms of average PLR.

5. Comparison to other jamming techniques

A comparison of NFJ to constant, deceptive and random jamming techniques is presented in Fig. 14. Constant, deceptive and random jamming techniques were implemented in the stack topology network with the same node set as the jamming node as was used in the simulation runs and graph plots for the investigation of NFJ presented. The average PLR for the network was computed and plotted.

The graph shows that the constant and deceptive jamming techniques are the most effective jamming techniques with the highest percentage of packet losses. NFJ exhibits an approximately 4% lower PLR of 94%, indicating severe network communication degradation. With deceptive jamming, the jammer is set to send out valid jamming packets continuously which results in four times higher energy expenditure than the null-frequency jammer owing to the fact that the null-frequency jammer is only actively sending out jamming packets for quarter of the time that the deceptive jammer is. The energy expended by wireless nodes is proportional to the transmitting power as well as the time the node is active. As a result of the constant presence of a deceptive jammer, the probability of detecting such a jammer is also significantly higher than with a NFJ jammer.

The constant jammer continuously adds noise to the channel thereby dropping any packets that are transmitted and received on that channel. It behaves as a deceptive jammer. However there is an increase in the probability of detecting the node as a jammer because random noise is added to the channel, whereas with deceptive jamming, valid packets are used to jam the channel. The use of these valid or legitimate packets results in an overhearing node viewing the transmission as a valid one.

The average PLR of the random jammer is approximately 33% which is significantly lower that the PLR achieved with NFJ. The effectiveness of a random jammer is dependent on the schedule that the jammer follows (the jamming length as well as the jamming period) and as a result, the performance of such a jammer is significantly lower than a null-frequency jammer which is specifically designed to exploit the periodic nature of the routing protocol.

The energy expended by the jamming node is calculated as given in the following equation:

$$Energy = p \times t \tag{4}$$

The transmission power, p, of the jamming node is set to 0.1 mW and the active time, t, refers to the time the node spends in jamming the channel during the 120 s simulation period. The graph shown in Fig. 15 illustrates the energy expended by the jamming node in each of the four jamming techniques. It can be seen that the NFJ technique is the most energy efficient of the four jamming techniques. The random jamming technique is more energy expensive while both the continuous jamming techniques, although exhibits approximately the same performance in terms of the PLR as the null-frequency jamming method, expends the most energy and is also the easiest type of jamming to detect (Pelechrinis et al., 2011).

Typically, jamming is considered a physical layer attack as opposed to network layer based attacks such as wormhole attacks, jelly-fish attacks, blackhole attacks and flooding attacks. As a result, there are few detection techniques available in literature that target jamming attacks which reside on the network layer. In order to study how the proposed jamming technique fares against other jamming techniques in term of jammer detection, a basic and widely used jamming detection technique using the signal strength of the jamming node or ambient energy to detect the presence of jamming in the network is considered (Xu et al., 2005). Each node in the network is required to sample the noise levels numerous times during a specified time interval so as to gather statistics that can be used for jamming detection. The received energy levels of the channel, $s(t)$, are collected at uniform time intervals for N samples to form a window of samples $s(n), s(n-1), \ldots, s(n-N+1)$. The average signal strength is used and the detection statistic, $\Gamma(k)$, is defined as shown in the following equation:

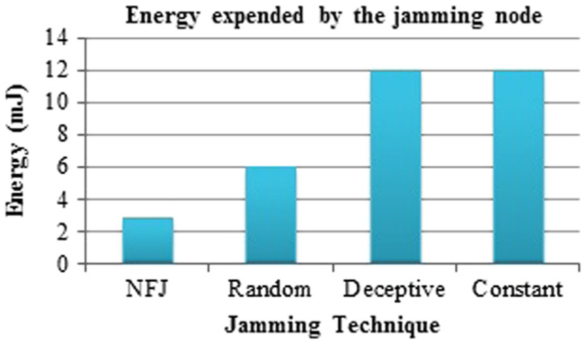

Fig. 15. Comparison of the energy expended by the jamming node for NFJ, random, deceptive and constant jamming techniques.

$$\Gamma(k) = \sum_{k=n-N+1}^{n} \frac{s(k)}{N} \tag{5}$$

The signal strength increases when the jamming node emits a noise-like signal, such as white Gaussian noise. The detection statistic, $\Gamma(k)$, is shown in Eq. (6) in such a scenario. The detection statistic is compared to a suitably chosen threshold value; if the detection statistic is higher than the threshold value, then jamming is detected

$$\Gamma(k) = \sum_{k=n-N+1}^{n} \frac{s(k)^2}{N} \tag{6}$$

Even though signal strength detection is largely used as a physical-layer detection technique, it can be used as a ubiquitous platform for determining and comparing the probability of detection of constant, deceptive and random techniques against the proposed null-frequency technique. From Eqs. (5) and (6), it can be inferred that the constant jamming technique, which continuously emits a noise-like signal, is the easiest jamming technique to detect. The deceptive jamming technique employs the detection statistic as specified by Eq. (5) and is considerably easier to detect than both the random jamming and NFJ techniques as a result of continuously sending out jamming packets. The random jamming technique is active for approximately half the time in a chosen time interval and is therefore twice as easy to detect than the NFJ technique, which is active for a quarter of the time in a given time interval. In addition, there are few jamming detection techniques that have been presented in the literature which considers the possibility that the jamming node is internal to the network. The NFJ nodes that have been designed to operate as the non-jamming transmitting/receiving nodes, in addition to having jamming functionality.

6. Conclusion

This paper proposed and investigated a scheduled jamming technique for WMNs which exploits the periodicity inherent in wireless nodes employing a proactive routing protocol. The jamming technique aimed to be energy efficient, have a low probability of being detected and have a high level of undesirable impact on network operation. The technique was tested in various topologies while varying parameters such as the jamming length, period and start time. It was found that when jamming at a particular jamming period, termed the null-period, the network exhibited a severe degradation in network communication. This technique was then compared to *deceptive*, *constant* as well as *random jamming* techniques. The performance compared favourably with both *deceptive* and *constant jamming* with an added advantage of expending four times less energy, and reducing the probability of jamming detection. Owing to the fact that the jamming node is viewed as an internal entity of the network, jamming detection is further impeded. Thus it is concluded that this jamming technique has a significant negative impact on network performance and can effectively be used to disrupt adversary network communication while being energy efficient and difficult to detect.

References

Ahmed N, Huang H. Distributed jammer networks: impact and characterization. In: Proceedings of the IEEE military communications conference; 2009. p. 237–42.

Altman E, Avrachenkov K, Garnaev A. Jamming in wireless networks under uncertainty. In: Proceedings of the international symposium on modeling and optimization in mobile ad hoc and wireless networks; 2009. p. 1–7.

Avelara E, Marquesa L, osPassosa Dd, Macedob R, Diasa K, Nogueira M. Interoperability issues on heterogeneous wireless communication for smart cities. Comput Commun 2014;58(1):4–15.

Balakrishnan M, Huang H, Asorey-Cacheda R, Misra S, Pawar S, Jaradat Y. Measures and countermeasures for null frequency jamming of on-demand routing protocols in wireless ad hoc networks. IEEE Trans Wireless Commun 2012;11 (11):3860–8.

Belouchrani A, Amin MG. Jammer mitigation in spread spectrum communications using blind sources separation. Signal Process 2000;80(4):723–9.

Commander CW, Pardalos PM, Ryabchenko V, Uryasev S, Zrazhevsky G. The wireless network jamming problem. J Combinat Optim 2007;14(4):481–98.

Desilva S, Boppana RV. Mitigating malicious control packet floods in ad hoc networks. In: Proceedings of the IEEE wireless communications and networking conference; 2005. p. 2112–7.

Gu Q, Liu P, Zhu S, Chu C. Defending against packet injection attacks unreliable ad hoc networks. In: Proceedings of the IEEE global telecommunications conference; 2005. p. 5–28.

Gupta V, Krishnamurthy S, Faloutsos M. Denial of service attacks at the mac layer in wireless ad hoc networks. In: Proceedings of the IEEE military communications conference; 2002. p. 1118–23.

Jacquet P, Muhlethaler P, Laouiti A, Clausen T, Qayyum A, Viennot L. Optimized link state routing protocol for ad hoc networks. In: Proceedings of the IEEE INMIC; 2001. p. 62–8.

Jae-Joon L, Jaesung L. Effective and efficient jamming based on routing in wireless ad hoc networks. IEEE Commun Lett 2013;16(11):1903–6.

Kim YS, DeBruhl B, Tague P. Meshjam: intelligent jamming attack and defense in ieee 802.11 s wireless mesh networks. In: Proceedings of the IEEE international conference on MASS; 2013. p. 560–64.

Kuzmanovic A, Knightly EW. Low-rate tcp-targeted denial of service attacks and counter strategies. IEEE/ACM Trans Netw 2006;14(4):683–96.

Muogilim O, Loo K, Comley R. Wireless mesh network security: a traffic engineering management approach. J Netw Comput Appl 2011;34(2):478–91.

OMNET++, INET framework. ⟨http://inet.omnetpp.org/⟩.

Ong H-L, Natsheh E, Wan T-C. Routing with a density-based probabilistic algorithm for mobile ad-hoc networks. J High Speed Netw 2011;18(2):83–114.

Oulmahdi M, Chassot C, Exposito E. Energy saving mechanisms on high communication layers. J High Speed Netw 2014;20(2):113–29.

Palmieri F, Ricciardi S, Fiore U, Ficco M, Castiglione A. Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. J Supercomput 2015;71(5):1620–41.

Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of service attacks in wireless networks: the case of jammers. IEEE Commun Surv Tutor 2011;13(2):245–57.

Prasad S, Thuente DJ. Jamming attacks in 802.11 g—a cognitive radio based approach. In: Proceedings of the IEEE military communications conference; 2011. p. 1219–24.

Proano A, Lazos L. Selective jamming attacks in wireless networks. In: Proceedings of the IEEE international conference on communication; 2004. p. 80–9.

Ricciardi S, Palmieri F, Castiglione A, Careglio D. Energy efficiency of elastic frequency grids in multilayer ip/mpls-over-flexgrid networks. J Netw Comput Appl 2015;56:41–7.

Wang L, Wyglinski AM. A combined approach for distinguishing different types of jamming attacks against wireless networks. In: Proceedings of the IEEE Pacific Rim conference on communication, computers and signal processing; 2011. p. 809–14.

Wood T, Trapper W, Zhang Y. Channel surfing and spatial retreats: defenses against wireless denial of service. Proc. WiSe 2004:80–9.

Xing F, Wang W. Understanding dynamic denial of service attacks in wireless networks: The case of jammers. In: Proceedings of the IEEE military communications conference; 2006. p. 791–802.

Xu S, Saadawi T. Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks. Comput Netw 2002;38(4):531–48.

Xu W, Trappe W, Zhang W, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. Proc. MobiHoc 2005:46–57.