Investigating the Effect of Jamming Attacks on Wireless LANS

Suresh Bandaru
Anglia Ruskin University
United Kingdom

ABSTRACT

WLANs (Wireless local area networks) are the most widely used networks in homes as well as in commercial areas. WLANs suffer from various security threats. One of the most important attacks in denial of service (DOS) attacks are jamming attacks. As the communication in wireless networks are based on radio channels, jamming attacks interfere with the transmission channels by sending semi-valid packets (useless) in order to disturb the communication between actual nodes.

The main objective of this paper is to explain frequency sweep jammer working and how it affects the performance of a network using OPNET simulation tool. For this purpose wireless networks are simulated by flooding the network with frequency sweep jammer and to determine whether switching channels can avoid jamming attack. In the simulations, initially network is configured to communicate in channel 1 and comparisons were made for network throughput and delay with and without jammer, which has demonstrated that jamming effects the performance. To avoid jamming attack communication channel is changed to 6 and the results of switching channels are explained.

General Terms

Throughput, Delay, Performance.

Keywords

WLAN, Throughput, DOS,OPNET, Jammers, Jamming, Attacks.

1. INTRODUCTION

Wireless local area network (WLAN) links one or more computers in a network. Usually the WLANs are connected to wider internet with the help of access point. WLAN provides the users to move within the local area and can connect to the internet. Due to mobility in WLAN, they enjoy widespread implementation throughout the world.

The main use of WLANs is to transfer data between devices linked in the network, so they are expected to provide confidentiality and data integrity. Therefore the security of WLANs is most important. Most common attacks are denial of service attacks to make the resource unavailable to users. Data transmission between nodes is communicated by using channels in wireless networks. IEEE (Institute of Electrical and Electronics Engineers) states that in all the wireless networks transmission of data using channels are defined by frequencies (IEEE Org., 2012). Out of different types of denial of service attacks, jamming attacks are most common type of attacks on wireless LANs which utilises frequency flooding. Jamming attacks causes the system to break down by sending unnecessary packets. Switching to a different channel is one method to avoid jamming attacks, because jamming attack concentrates on single frequency to block the network. The frequency sweep jammer generates continuous transmission over a range of frequencies at a particular rate. The frequencies are swept by sampling the bandwidth at a particular number of frequency intervals and by repeatedly cycling during these intervals at fixed length at every step

Previous researchers studied about wireless LAN working, some of them like Amit Nagpal, Pooja Nagpal, Yashkaran Rathore (2012) explained that WLANs are also designed to support 4G heterogeneous networks. The mobility of users in 4G networks with WLAN can be implemented by using vertical handover decision algorithm. Further research on WLAN was discussed in San Diego, Cisco Live (Conf, 2012) to improve radio frequency and spectrum in order to provide stable spectrum for applications like video and voice. Araujo (2012) explained about new emerging technology called CWSN (Cognitive Wireless Sensor Network) for improving security and he also analysed various types of attacks and security measures to handle the attacks on CWSN. Lin (2012) proposed a new protocol to avoid internal attacks like flooding attack and route disruption attacks; he also stated that the new protocol has better packet delivery ratio. A new algorithm was proposed for channel allocation by Monteiro (2012) called DCAA-O (Distributed Channel Allocation Algorithm), which defines a new solution to avoid interference between access points in a network

A group based channel assignment method to improve performance in wireless networks was suggested by Kim, Kim, Suh (2012). In their proposed method group channel assignment uses algorithm to divide data rate by multiple channels. Fu Quan, Zhang (2012) described in a paper that ad-hoc networks suffer from severe bottle neck attacks which cause degradation in the network. So they proposed a scheme to utilize the network in terms of concentric tiers called tier-based proactive path selection mode.

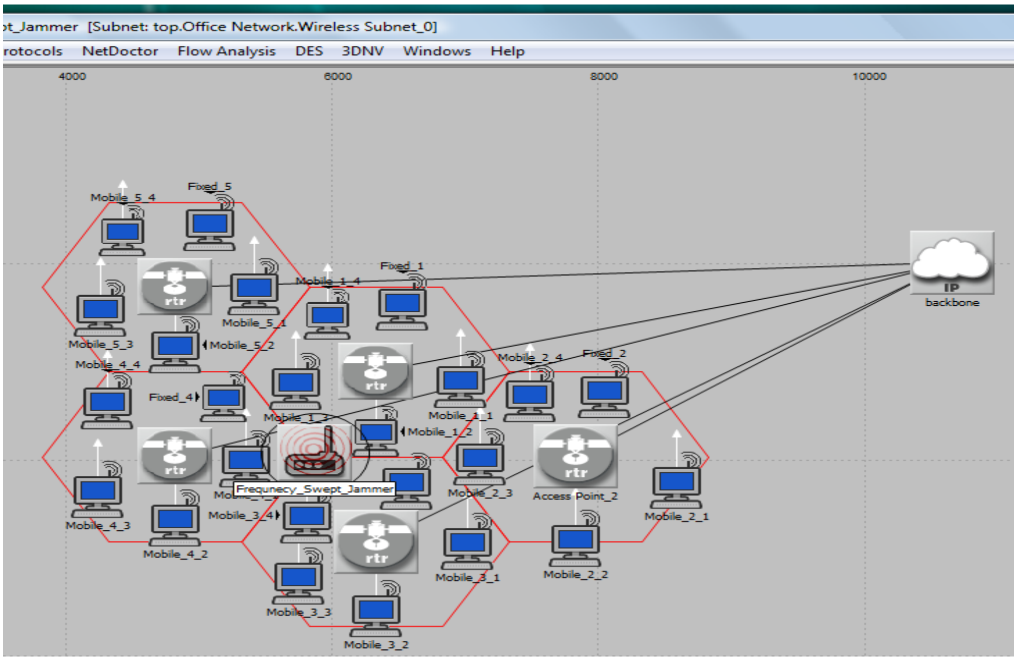
When a network is attacked by a jammer in one channel then switching to the other channel can protect the network from being attacked. When the node in a network detects jamming attack then they jump to other channels and resume their communication as usual and the research was done by Beg, Ahsan, and Mohsin (2010) showed that the amount of packets dropped reduced instantaneously without delay. Jamming attacks is the most common type of attacks and easy to implement. Jamming attacks can cause severe problem to the network. In some cases these attacks causes break down of the entire network. Typically jammer is a small device like a node, sends radio signals that interfere with legitimate signals in the network. Buchbinder (2012) suggested in a paper about varying channels to increase data throughput and also decreasing power. He considered single transmitter power by varying time channels. Counter measures for jamming by detecting them by received signal strength. He simulated various experiments in real time for detecting jamming.

Rest of the paper is organised as follows. Section II describes the experimental setup in which how WLAN has been configured. Section III presents and discusses the various performance results and finally section IV concludes the paper.

2. RESEARCH WORK

This section explains the design methodology of the network. The whole network consists of 20 mobile nodes, 5 fixed nodes, 5 access points and an IP backbone with a jammer in the middle of the network.

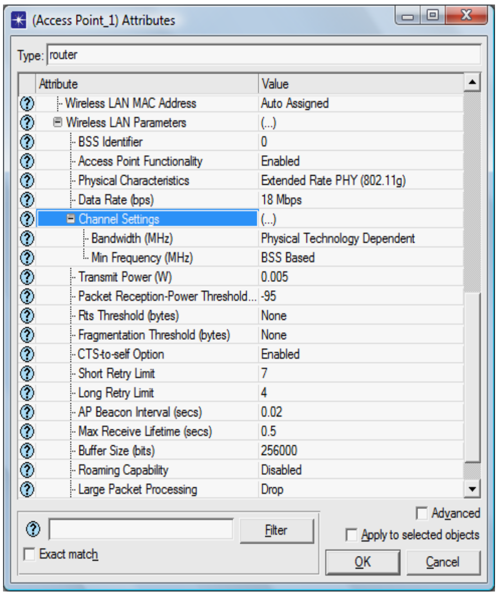
Figure 1. Wireless LAN Network



2.1 Access Points

Access point in a network is also called as BSS, which means it acts as a base station to all other network nodes. In this network each access point provides connection to 5 nodes. As per the standard of IEEE 802.11g, access point can cover up to 75meters distance. In this network as the default power level is changed to 0.005W, the access point can cover 500meters. The characteristics of access point are shown in the below table:

Table1. Access Point Characteristics



Type: router

Attribute	Value
Wireless LAN MAC Address	Auto Assigned
⊟ Wireless LAN Parameters	(...)
BSS Identifier	0
Access Point Functionality	Enabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	18 Mbps
⊟ Channel Settings	(...)
Bandwidth (MHz)	Physical Technology Dependent
Min Frequency (MHz)	BSS Based
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop

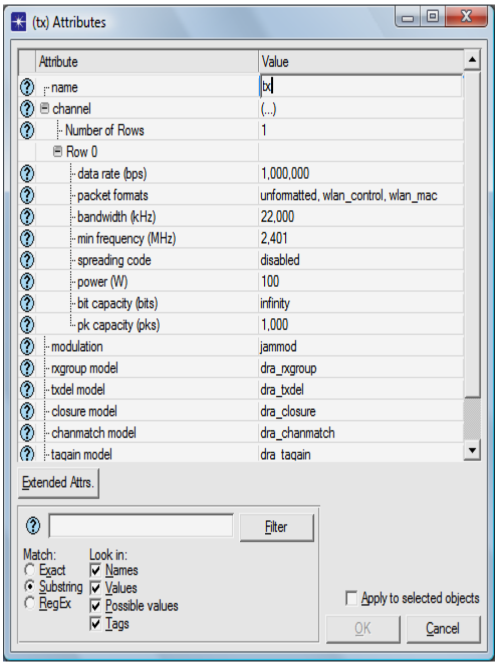
The nodes in the network are connected to the access point by using BSS identifier, which is a unique WLAN MAC address. The channel for communication is automatically assigned and configured throughout the network which can be changed as per the user needs. In this network initially channel 1 is assigned for the communication.

2.2 Frequency Sweep Jammer

The frequency sweep jammer generates continuous transmission over a range of frequencies at a particular rate. The frequencies are swept by sampling the bandwidth at a particular range of frequency intervals and continuously cycling through these intervals at fixed length at every step. The jammer frequency is set to 2,401MHz. The performances of both mobile and fixed nodes results are compared.

The characteristics of transmitter are same as other jammers as shown below.

Table 2. Jammer Characteristics



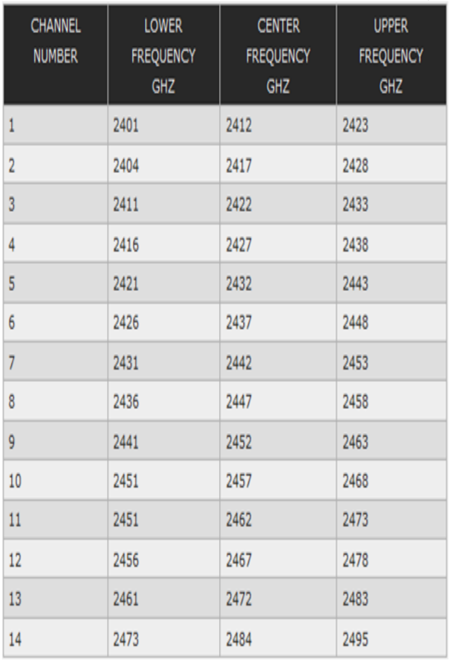
(tx) Attributes

Attribute	Value
name	tx
channel	(...)
Number of Rows	1
Row 0	
data rate (bps)	1,000,000
packet formats	unformatted, wlan_control, wlan_mac
bandwidth (kHz)	22,000
min frequency (MHz)	2,401
spreading code	disabled
power (W)	100
bit capacity (bits)	infinity
pk capacity (pks)	1,000
modulation	jammod
rxgroup model	dra_rxgroup
txdel model	dra_txdel
closure model	dra_closure
chanmatch model	dra_chanmatch
tagain model	dra_tagain

2.3 Channel Switching

The main objective of this experiment is to find the best route to prevent jamming attack on the network. As per IEEE 802.11 standards, wireless devices communicate with each other or with network by using channels. The channels are defined by frequencies. Each channel has its range of frequency.

Table 3. IEEE WLAN 2.4GHz Channels, Cisco(2012)

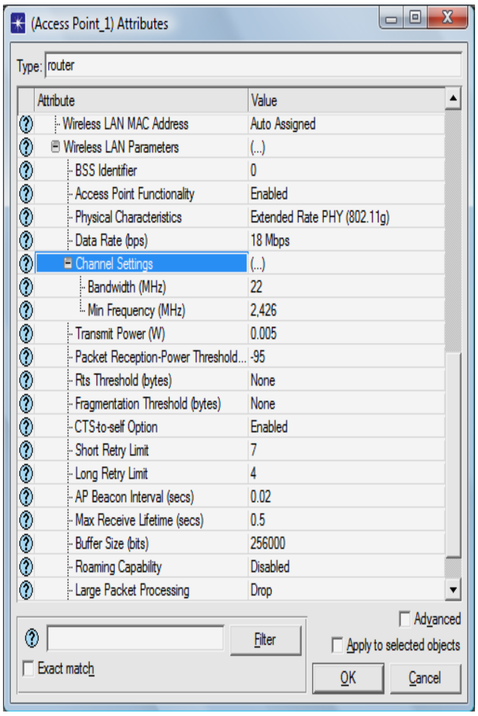


CHANNEL NUMBER	LOWER FREQUENCY GHZ	CENTER FREQUENCY GHZ	UPPER FREQUENCY GHZ
1	2401	2412	2423
2	2404	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2451	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

Channel 1 starts from 2401 MHz to 2423 MHz with a centre frequency of 2412 MHz. Each channel has an interval of 5MHz. Due to this interval only 3 independent channels exist which are channels 1, 6 and 11. In this network all the nodes and access points are automatically assigned by the wireless network wizard, which assigns channel 1 to the nodes and access points. Jammers in OPNET also use channel 1 which is 2,401 MHz frequency as shown in the above transmitter characteristics. Each access point in the network is assigned with channel 1.

When the channel assignment is changed to 6, then the frequency at which communication is also changed to 2426 MHz and with a bandwidth of 22 MHz (22,000 KHz) as shown below:

Table 4. Access Point Characteristics



(Access Point_1) Attributes

Type: router

Attribute	Value
Wireless LAN MAC Address	Auto Assigned
Wireless LAN Parameters	(...)
BSS Identifier	0
Access Point Functionality	Enabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	18 Mbps
Channel Settings	(...)
Bandwidth (MHz)	22
Min Frequency (MHz)	2,426
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop

3. SIMULATION RESULTS AND ANALYSIS

This section describes the experiment results and analyses the results. Different comparisons of results were done to analyse the throughputs at different situations. Frequency swept jammer is configured in the network to flood the network with useless packets. The time average output of wireless LAN is compared with performance of the network with and without the jammer.

Figure 2. Network throughput (With and without jammer)

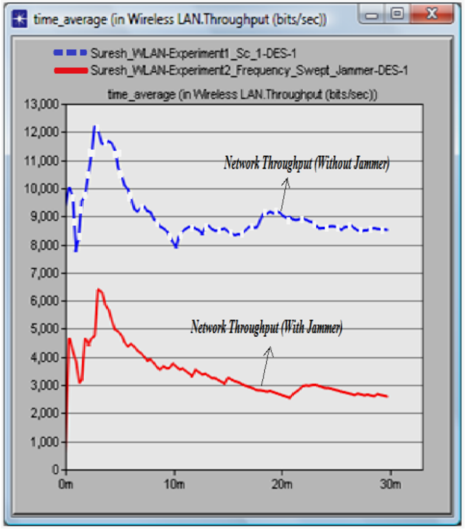
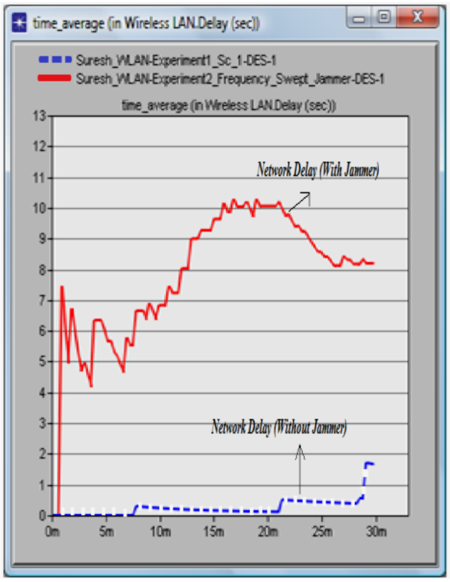


Figure 3. Network Delay (With and without jammer)



The graph compares the overall throughput of network with and without jammer. Straight line represents the overall throughput of wireless LAN with jammer and dashed line represents the throughput of wireless LAN without jammer. Without jammer in the network the throughput is around 8500bits/sec, but when jammer is applied in the network, the throughput is decreased to less than 3000bits/sec. This shows that network performance is degraded and network is severely affected. The delay in the network has increased from 2seconds to 10seconds.

In order to prevent the network from being attacked by the jammers, switching channels for communication is an efficient method. The main objective of the next simulation is to determine the best method to avoid jamming when different jammers are used to flood the network. All the simulations were made with different jammers by changing the channel to 6.

In the experiment comparison of two different simulations were made between two networks. Both networks have common jammer in place (frequency sweep) but different in channels.

Figure 4. Network Throughput (Before and After Channel Switching)

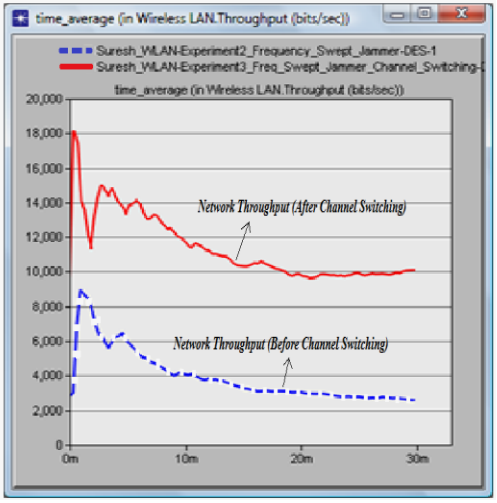
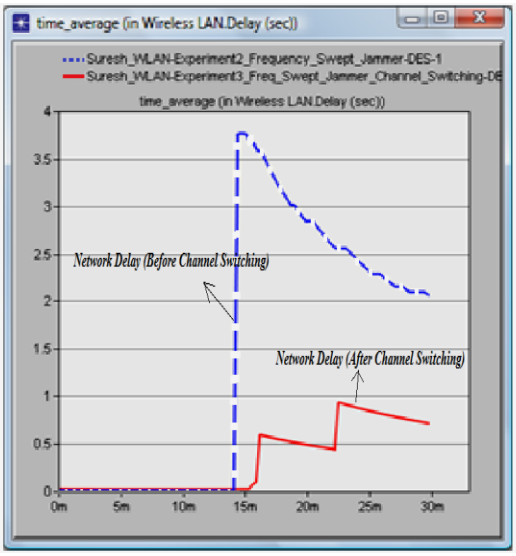


Figure 5. Network Delay (Before and After Channel Switching)



In the above figure, straight line represents throughput after switching channel and dashed line represents before channel switching. when a jammer is attacking the network The network throughput is increased from 3000 bits/sec to 10,000 bits/sec which is best performance with jamming attack. The graph also shows that the jamming has almost no effect on the network. In terms of delay also network has at its best state. Delay in the network is decreased from 2sec to 1sec.

The above results conclude that to avoid jamming attack channel switching is a good method for infrastructure wireless network and also the throughput is increased higher than the network performance in channel 1.

4. CONCLUSION AND FUTURE DIRECTIONS

The aim is to study the effect of frequency sweep jammer on the performance of WLANs. Beginning of the research started with analysing and by understanding the concepts of wireless LANs and their working principles. The next stage is to investigate the effect of frequency sweep jammer, because of frequency sweep jammer the network throughput is decreased significantly. This stage in the research clearly demonstrated that jammers can affect the wireless network. If jammers are used with more power or for particular amount of time continuously the network can be destroyed by the attacker which is a serious concern. To avoid jamming effect on the network, channel switching is one of the prescribed techniques to avoid jamming by many researchers. When a jammer is attacking the network, to prevent the network communication from being interfered, channel for communication is switched to another. By switching channels network performance can be increased.

Further research can also be done by developing the wireless devices to communicate in varying channels. With varying time, channel of communication is also need to be changed which can prevent the attacker to sense the communication channel characteristics. But in order to develop this type of method in nodes by varying channels, power consumption will be high which needs to be investigated further.

5. REFERENCES

[1] 2012. IEEE Draft Standard for IT - Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications - Amd: Enhancements for Very High Throughput for operation in bands below 6GHz. In: IEEE P802.11ac/D2.0, January 2012. [e-]. pp.1-359. Available through: IEEE,.

[2] 802.11 WLAN Model [on-line] Available at: <http://www.opnet.com/solutions/network_rd/simulation_model_library/wireless_lan.html>

[3] Cisco Live 365 Presentations : Cisco Live!™ 2010 - 2011 - 2012 Conference Session, Speaker and Exhibitor Presentations [on-line] Available at: <https://www.ciscolive365.com/connect/sessionDetail.ww?SESSION_ID=4260&tclass=popup>

[4] Amit, Nagpal, Pooja Nagpal and Yashkaran Rathore. , May,2012. IJCA - Vertical

[5] Araujo, A., 2012. Security in cognitive wireless sensor networks. Challenges and open problems. EURASIP Journal on wireless communications and networking, [e-journal] 2012(1), pp.1-8. Available through: SFX, .

[6] Beg, S., Ahsan, F. and Mohsin, S. eds., 2010. Emerging Technologies (ICET),20106thInternational Conference on [on-line] .

[7] Buchbinder, N., 2012. Dynamic power allocation under arbitrary varying channels: an online approach. IEEE/ACM Transactions on Networking, [e-journal] 20(2), pp.477-487.

[8] Fu Quan, Z., 2012. Tier-based proactive path selection mode for wireless mesh networks.(Technical report). Transactions on internet and information systems, [e-journal] 6(5), pp.1303. Available through: SFX, .

[9] Lin, H., 2012. PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks. EURASIP Journal on wireless communications and networking, [e-journal] 2012(1), pp.1-16. Available through: SFX, .

[10] Monteiro, T.L., et al., 2012. Channel allocation algorithms for WLANs using distributed optimization. AEU - International Journal of Electronics and Communications, [e-journal] 66(6), pp.480-490. Available through: ScienceDirect, at:http://www.sciencedirect.com/science/article/pii/S1434841111002640>.

[11] Kim, S., Kim, D. and Suh, Y., 2012. A group-based channel assignment protocol for rate separation in IEEE 802.11-based multi-radio multi-rate ad hoc networks. Ad Hoc Networks, [e-journal] 10(1), pp.95-110. Available through: ScienceDirect, at: <http://www.sciencedirect.com/science/article/pii/S1570870511001235>.

[12] Yang, F., Y, Xiao, J., Luan, P.,L and Pend, L., June 2011. Research on Detection Scheme for Denial of Service Attacks in Wireless Mesh Networks| Whitepapers | TechRepublic [e-journal] 5(6)(9/9/2012), pp.290-296. Available through: RefGrab-It, at: <http://www.techrepublic.com/whitepapers/research-on-detection-scheme-for-denial-of-service-attacks-in-wireless-mesh-networks/4097451>

[13] Zhao, W. and Xie, J., 2011. OPNET-based modeling and simulation study on handoffs in Internet-based infrastructure wireless mesh networks. Computer Networks, [e-journal] 55(12), pp.2675-2688. Available through: ScienceDirect, at: <http://www.sciencedirect.com/science/article/pii/S1389128611001502>.