Jurnal Teknologi

Full Paper

THE EFFECT OF JAMMING ATTACK DETECTION AND MITIGATION ON ENERGY POWER CONSUMPTION (CASE STUDY IEEE 802.11 WIRELESS AD HOC NETWORK)

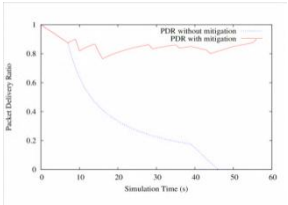
Article history
Received
27 April 2015
Received in revised form
15 June 2015
Accepted
25 November 2015

Nur Cahyono Kushardianto[a*], Yudhi Kusnanto[b], Elvian Syafrurizal[c], Ahmad Hamim Tohari[c]

*Corresponding author
anung@polibatam.ac.id

[a] Department of Informatics Engineering, Politeknik Negeri Batam, Batam, Indonesia
[b] Department of Computer Engineering, STMIK AKAKOM, Yogyakarta, Indonesia
[c] Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia

Graphical abstract



Abstract

Quality of Service for data traffic is an important facet of a network, which in the case of a wireless network can easily be disrupted by applying a device to broadcast signals. The authors believe that the increased of the energy consumption, when a jamming attack occurs, can be used as a guiding indicator in order to mitigate the attack. The authors show that when a reactive jamming attack occurs on a wireless network unmitigated, it can easily block the entire data traffic to the point there is no data can be delivered. The authors also show that, using NS3 simulation, in an event where a reactive jamming attack to the network happened, the source of the attack can be identified through the increased of energy consumption , and successfully mitigated by avoiding sending data traffic through the same channel used by the attacker, by executing channel hopping.

Keywords: Quality of Service; jamming; energy consumption; channel hopping

1.0 INTRODUCTION

For the last few of years, wireless communication usage trends, has been increasing significantly. It is inevitable because nearly every aspect of our world today become more and more needy towards network communication. The existence of better protocols for wireless network also give us the freedom of movement besides the reliability of communication. The debatable factor for some people still, was held by wired communication. But as everything in the world goes, there is no such thing as a free lunch. For every improvement, it will be also followed by some form of drawback. The obvious drawback in wireless communication is security, due to the fact that this method of communication uses air as a medium, which availability for access is a given for each and every person.

One of the easiest mean to disturb network communication is through denial of service attack [1] . This is in wireless communication can be done by applying jamming signal device(s). This is according to the research done by Benslimane *et al*. (2011), where the jamming attack was implemented in the physical layer of the wireless network, and the severity of the attack can be even observed on the MAC layer above it [2] .

Latest research shown that jamming attacks have become more sophisticated which capable to do the same action with less resource expenditure. The effort of mitigating such an attack by beam forming orspread-spectrum techniques become ineffective

[3] .
This situation is becoming more complicated with the fact that the source device of the jamming attack might be mobile, thus making the effort to track and pin pointing it, is a very complicated task [3-6]. The jamming attack may be coming from a group of devices, not just a single one, as such the effort to mitigate it becomes a daunting task [1, 7]. This is all before the authors consider that jamming attack may also launch their attack simultaneously through a number of different protocols on multiple layers of the network [1]

2.0 RELATED WORKS

One of the previous works on jamming mitigation was the work of Tague *et al*. (2011), in which they proposed a way of mitigating jamming attack by aggregating the jamming impact experienced locally by each node in the wireless network to determine the source of the attack [3] . The mathematical model of their work was based on the portfolio selection theory to allow data sources to balance the expected data throughput with the uncertainty in the achievable traffic rates. This model will be used in multiple-path routing algorithms to avoid data being sent through the jammed wireless network area.

Hamieh (2012), in his research on jamming in wireless ad-hoc network, proposed a way to defend the wireless network from jamming attack based on the increased power used by the devices in the network when they are under jamming attack. The basic idea is to hide the network when it is under attack from the jammer devices, which signified by the increased power usage for data transmission, by changing their transmission power. Thus, become invisible from the attacker's point of view [8] .

The previous similar research was conducted by Xu *et al*. (2006), in which MICA2 motes were used as data sources and receivers instead of ad-hoc wireless. Th researchers note that in order to be effective in competition against jamming attack source, power-control based defense will also need to have a feedback based power control protocol [9] .

This project, in essence, also try to approach the jamming attack mitigation problem from power transmission point of view [10]. First, basing on the research done by others previously, the authors will identify and isolate the wireless network area under attack from the jamming device. Then, instead of competing with the power transmission generated by the attacker, the authors will try to find the most suitable route to avoid the area under attack

3.0 SYSTEM MODEL AND JAMMING STRATEGY

Due to similarity with Tague *et al*. (2011), strategy in attack mitigation, the authors will also use similar physical wireless network models, which include four wireless data source, and one jamming signal generator device. This wireless jamming models already available at www.nsnam.org, which can be implemented in NS-3.

Jamming in a wireless network is achieved by deliberate transmission of radio signals to disrupt the communication in a wireless network by decreasing the signal-to-interference-noise ratio (SINR). Jamming leads to corrupted packets at the receiver, which results in a lowered throughput [11] .

The NS-3 jamming attack detection and mitigation model hierarchy consists of the following base class components:

- Jamming intelligence (jammer)
- Jamming detection/mitigation intelligence (mitigation)
- Wireless module utility (utility)
- Energy model

Jamming intelligence and jamming detection/mitigation reside in the intelligence layer and provide interfaces to wireless module utility (see Figure 1). Besides, the wireless module utility provides a set of functions for jamming mitigation classes to utilize for implementing their strategies. This class acts as a bridge between the intelligence layer and the physical (PHY) layer.

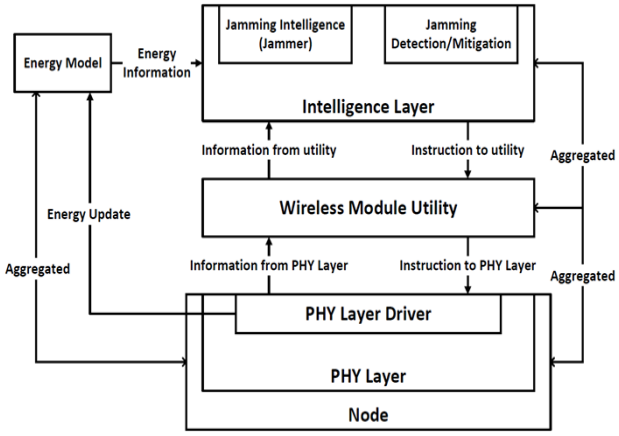


Figure 1 Jamming model hierarchy [11]

3.1 Jamming Intelligence

This base class provides jamming strategies, which will be used in this research. The authors focus on three different jamming attack strategies such as:

- Reactive jammer
  This type of jammer sends jamming signal of certain duration only when communication is present in the channel.
- Constant jammer
  This type of jammer sends jamming signal of certain duration at a constant interval.
- Random jammer
  This type of jammer sends jamming signal of certain duration at a randomly chosen interval.

The jamming intelligence class is designed to abstract the detail of sending jamming signals and extracting information from the channel [9, 11].

3.2 Jamming Detection/Mitigation Intelligence

This base class provides strategies to detect and mitigate the jamming attack. The presence of jamming attack will be detected using the decreasing of Received Signal Strength (RSS) only, or Packet Delivery Ratio (PDR) only, or by both of them.

Mitigating strategies, which provided in this base class is Channel Hopping. This strategies scheme is simply done by detecting on which channel the jammer device is attacking, and then based on this information, the honest nodes in the network will be urged to use a different channel than the one used by the jammer device to avoid being jammed [5, 8, 12-14].

The work flow of the base class jamming detection/mitigation is started from PHY layer driver who connect directly with wireless module utility. The packet information will follow this route until reach mitigation step in order to decide whether channel hopping is needed or not. See Figure 2.

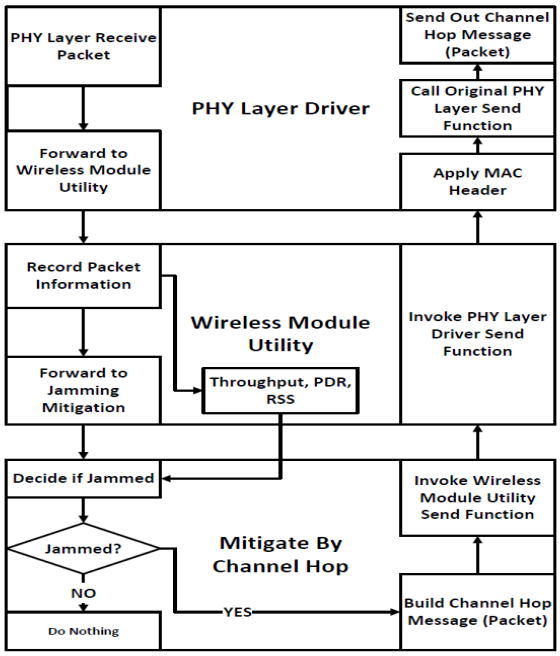


Figure 2 Mitigate by channel hop work flow [11]

3.3 Wireless Module Utility

This class provides essential functions for jamming intelligence and jamming detection/mitigation intelligence to operate. It can be installed separately for monitoring network performance such as throughput.

Callbacks are used to connect the Wireless Module Utility to the PHY layer and the intelligence layer (jamming, jamming detection/mitigation). By doing so, the Wireless Module Utility abstracts the underlying PHY layer protocol, providing unified APIs for different intelligence layer models [11] .

3.4 Energy Model

Energy model is the key element for wireless network simulation; it can be information metric for the performance of wireless network protocols. Energy model which already provided by NS-3 has information flow as figure 3.

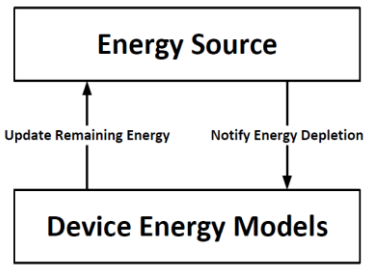


Figure 3 Energy model information flow [11]

The data collected should be in the form of power transmission increase and decrease of each node against time.

In order to measure the rise and fall of the data transmission power due to interference from jamming, the authors use power equation which also been used by Wu *et al*. (2011), which yield:

$$E_i + 1 = E_i + V \times (t_{i+1} - t_i) \times I_i$$

Where E_i is the energy consumption of the source at time stamp t_i, and V is the supply voltage [4] .

3.5 Jamming Strategy

As the systems model, the authors utilize four node in the ad hoc network. They are namely a source (node 0), destination (node 3), trusted relays (node 1 and node 2), and a jammer node. Each node is equipped with a single Omni-directional antenna and operates in a half-duplex mode. The authors assume that there is no direct link from node 0 to node 3. To deliver source message to the destination, the source first transmits its message to the relays, and then the relays forward the message to the destination. Especially for jammer node, the authors focus on three type's jammer: random, constant, and reactive.

Figure 4 presents the network configuration adopted for simulations. While Table 1 presents the common parameters used in this study.

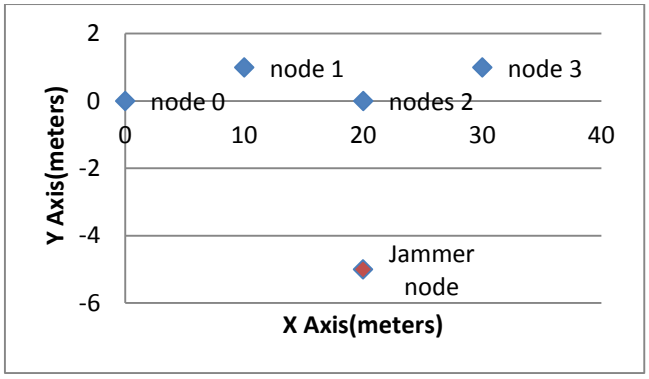


Figure 4 Topology of wireless ad hoc network

Table 1 Simulation parameters

Parameter	Value
number of packets	1000
packet size	200 bytes
Sent Jamming signal power	0.04 W
Jammer transmission signal power	0.001 W

For analyzing the feasibility of this mitigation scheme, the authors use the assumption that all of the honest ones and the jammer node have 10 channels. Where every single one of these channels do not have any overlapping bands of frequencies to each other.

4.0 RESULT AND DISCUSSION

4.1 Implementation

Implementation of the jamming attack detection and mitigation in NS-3 simulation needs jamming model which consist of core module, network module, mobility module, wifi module, and internet module. In order to observe the effect of jamming attack on energy power consumption, the energy model framework is needed to support it.

In this research, the authors should modify the jamming model and energy model in order to be running well with the newest version of NS-3.

The jamming model is the original source from nsnam.org (jammer-example.cc). Several modification should be done to this code jamming model, such as :

- Initiate the NodeContainer variable with jammer node.
- Embed jamming mitigation scheme module.
- Embed energy module.
- Initiate simulator schedule for jamming mitigation.
- Activating trace module to capture the real time data of simulation time, packet delivery ratio, received signal strength, and energy consumption.

And all of this modification should be performed to three different jamming strategies modules : constant jammer, random jammer, and reactive jammer.

4.2 Parsing and Plotting Data

The data results from NS-3 simulation are very raw, and very hard to inspect, especially the energy consumption data. AWK application can be utilised to parse this raw data. In this research the authors develop simple code using Perl Programming to parse the data into the required result. The parsing code is as follow :

```
#!/usr/bin/perl
while (<>) {
        chomp;
        next if ! /^[^.]+s.*remaining energy/i;
        push @timed, [ /^([^.s]+).*= (.+)J,/ ];
};
#printf "%s\t%s\t%s\t%s\n", "sec", "delta", "old", "cur";
for $i (0..$#timed) {
        $delta = ($i > 0)?
                $timed[$i - 1][1] - $timed[$i][1]:
                0.1 - $timed[$i][1];
        $save = ($timed[$i - 1][0] == $timed[$i][0])?
                $save + $delta: $delta;
        printf "%s\t%.7f\t%.7f\t%.7f\n",
                $timed[$i][0],
```

```
                $save,
                $timed[$i][1],
                $timed[$i-1][1] if ($timed[$i + 1][0] !=
                $timed[$i][0]);
};
1;
```

This code will parse the energy consumption data and its time stamp, into the presentation data which easy to be observed.

Plotting the data result is not a hard task if the data already in the proper presentation. The authors use the Gnuplot aplication to make Graph plot PDR, RSS, and energy consumption from the simulation result.

4.3 Analysis

In this study the authors are interested in measuring the Packet Delivery Ratio (PDR), the Received Signal Strength (RSS) and the energy consumption at node 2 as an observation point.

PDR and the RSS will be measured on one type of jammer, just to show the effect mitigation in accordance with its packet delivery and signal strength. In the other hand, energy consumption will be measured on three types of jamming attack.

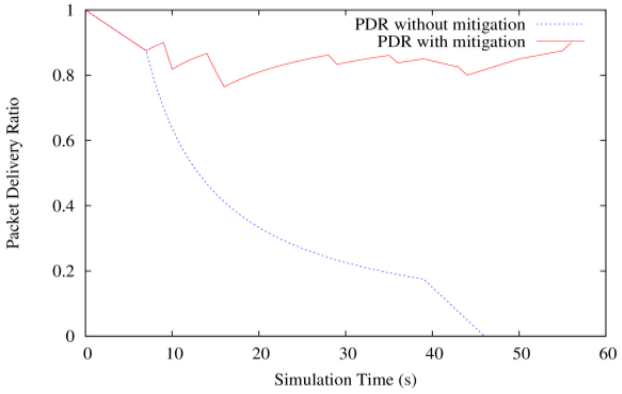


Figure 5 Packet delivery ratio comparison between mitigated and unmitigated network on reactive jamming

Figure 5 shows the PDR of the network where node 2 is jammed. In this scenario where mitigation does not occur, the jammer acts with a power transmission 0.001 W and starts its activity at time 7s. The authors observe that the PDR at the node 3 is penalized and decreasing. Until the PDR reaches the value of 0 at time 45s. 15 second earlier from time 60s where the observation supposed to end.

On the same table, the authors can also observe that when a mitigation scheme does occur, the PDR managed to relatively stay at 0.8 values until the observation ended at time 60s. The saw tooth like spikes are formed due to the nature of the reactive jammer which tried to re-jammed the network at those time point every time the wireless network managed mitigate it's attack, by choosing a different channel than the channel used by the jammer, to transmit data through channel-hopping scheme.

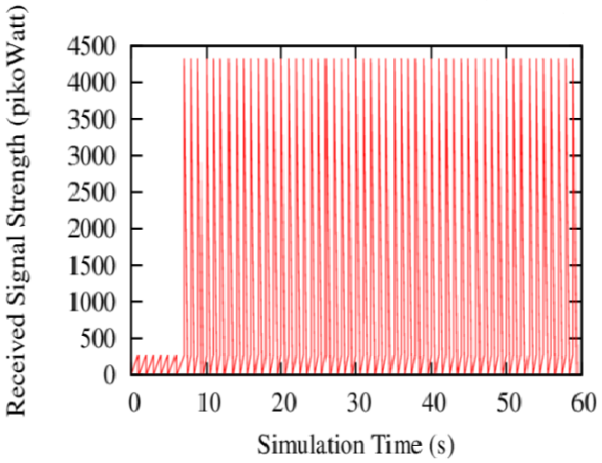


Figure 6 Received signal strength before mitigation on reactive jammer attack

Figure 6 shows that the RSS power increase significantly at observation point in the network due to the disturbance created by jammer device, when the mitigation scheme is not implemented. It increased up to 4500 pikoWatt from the time 7s when the jammer device turned on and continued to stay at such manner until the end of the observation.

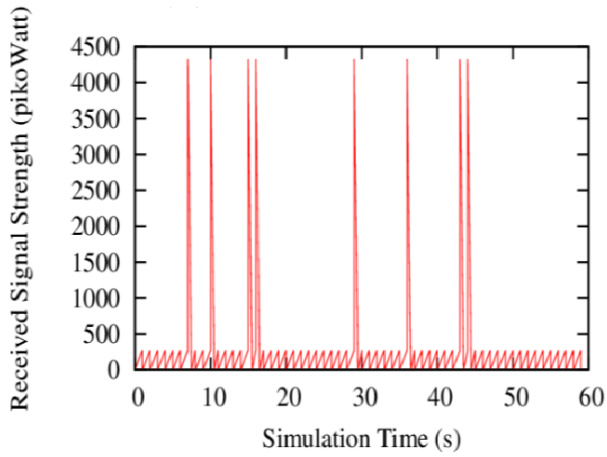


Figure 7 Received signal strength after mitigation

Figure 7 shows the how the mitigation scheme's effect on the observed RSS. After the mitigation scheme implemented, the Received Signal Strength observed is almost always stays at under pikoWatt. With a few exception at a few points in time such as 7s & 10s, where the RSS spiking up to 4500 pikoWatt, resembling the condition before the mitigation scheme implemented. The cause of these RSS value

spikes are also due to the effort of the jammer device to jam and re-jam the wireless network after being mitigated.

Before doing the experiment and collecting the data on energy consumption for a wireless network system under attack from a reactive jammer device, a few preliminary experiments are conducted to test the soundness of the idea of detection and mitigation for jammer device.

First, the wireless system to a jamming attack by a constant jammer is exposed. Constant jammer is defined as a jammer device which tried to send a jamming signal only from a single channel.

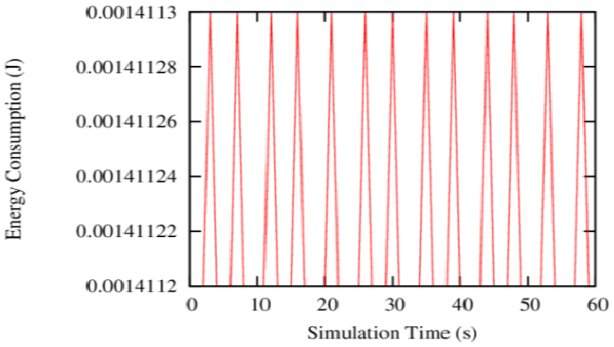


Figure 8 Systems energy consumption before mitigation on constant jamming

As shown in Figure 8, unmitigated, the energy consumption of the receiver quickly spiking up at the moment the constant jammer turned on and continue to stay on that level until the observation ended at time 60s.

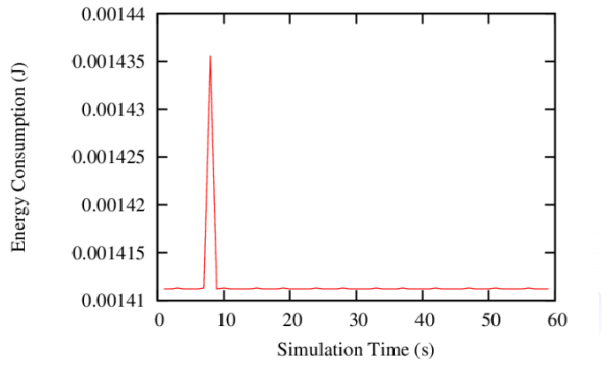


Figure 9 Systems energy consumption after mitigation on constant jamming

In Figure 9, after the constant jammer's existence detected through the spike of energy consumption, the system is simply mitigating the attack by hopping to a different channel, other than the one used by the jammer. Since the jammer device is committed only attacking from a single channel, it is no longer interference the signal sent by the honest nodes, hence the energy consumption become low after the attack mitigated.

Next, the authors try to expose the network to an attack from a random jammer. A random jammer which defined as a jammer which tried to send its jamming signals while randomly hopping from channel to channel, regardless whether it is successfully mitigated or not.

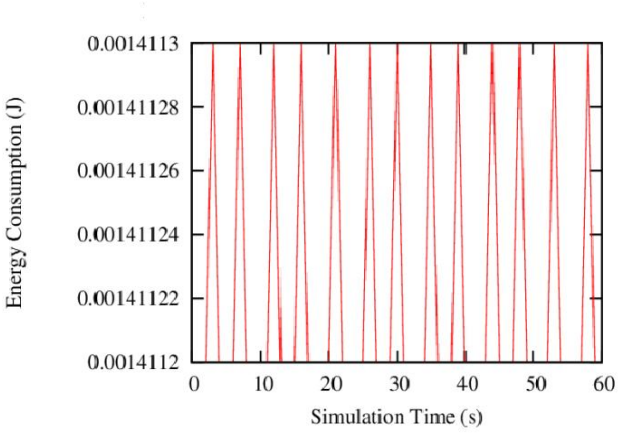


Figure 10 Systems energy consumption before mitigation on random jamming

As predicted, as it is shown in Figure 10 when unmitigated, the Random Jammer successfully increased the energy consumption significantly from the moment it is turned on.

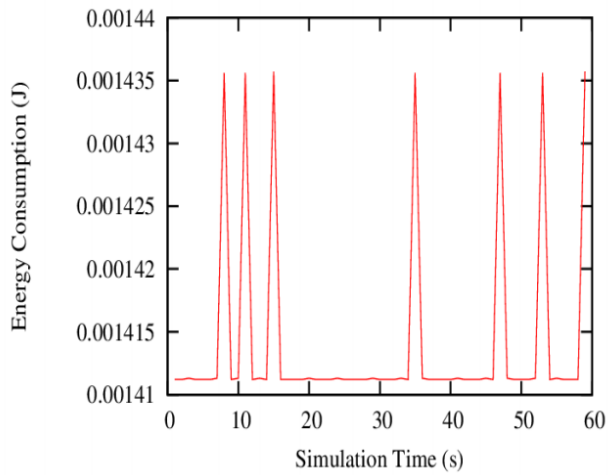


Figure 11 Systems energy consumption after mitigation on random jamming

Figure 11 shows that after mitigation by channel hopping implementation, the energy consumption level ceased from being continuously high. But, unlike the mitigation results for the constant jammer, energy consumption spikes still sometimes occurred after the first mitigation. This is due to random jammer suddenly changing its signal sending channel, and had to be re-mitigated.

The main test for energy consumption due to the reactive jammer was done after the authors are confident with the reading of mitigation results from the constant jammer and random jammer. The reactive jammer itself is defined as a jammer which will continuously sending its jamming signal from channel, until it is able to receive a packet from a sending honest node, which indicates its effort for jamming the network traffic have been mitigated. In such event, a random jammer will try to hop to higher channel number than the one it is currently sending its signal form.

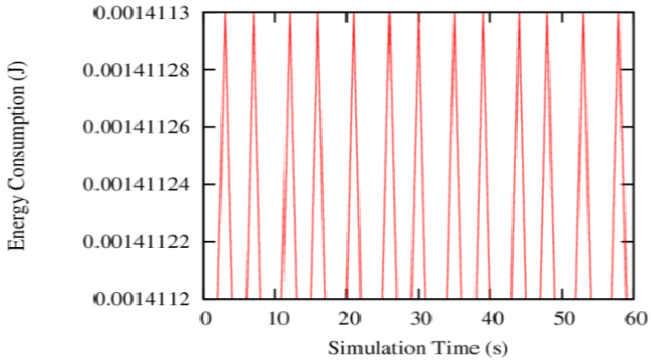


Figure 12 Systems energy consumption before mitigation on reactive jamming

Figure 12 shows how much energy consumption needed by the network before the mitigation scheme implemented. Since most energy consumption in wireless network is needed to maintain adequate signal strength it is stands to reason that the plotted data for energy consumption will look similar to RSS's. In addition, as shown the energy consumption of the network will be raised to a steady high point when disturbance from the jammer device is left unmitigated.

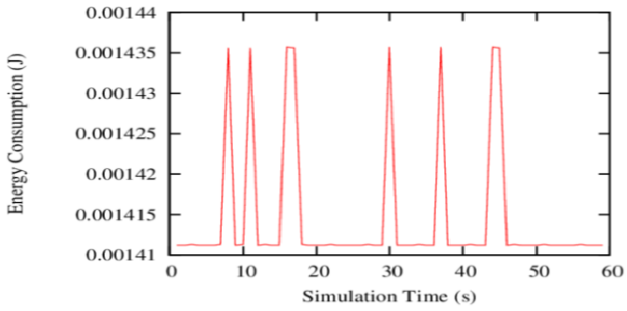


Figure 13 Systems energy consumption after mitigation on reactive jamming

Figure 13 shows the networks energy consumption when the mitigation scheme implemented in the wireless device in the network. As the authors can see, it also follow similar pattern with the RSS when the mitigation implemented. The authors see power consumption spiking up immediately after jammer device tried to jammed the network, and as quickly turned down when the mitigation scheme urged the wireless devices in the network to transmit their data on a different channel other than the one used by jammer device. Afterwards, the power consumption is spiking up again when the jammer device recalibrating it's parameters to the new channel used by the network, as an effort to re-jammed the networks data traffic. This action is followed by the network, which hopping its channel to a new one. This sets of action will done repeatedly as long as the jammer device still active, which resulting the significant decrease of networks power consumption.

5.0 CONCLUSION AND FUTURE WORK

In this paper, the authors proposed a reactive jamming attack mitigation scheme for a wireless network, which consists of 4 honest nodes and one jammer node. The authors showed that the algorithm used for mitigating the attack in simulation is successfully increasing the networks overall Quality of Service. As shown by the data gathered in the form of Received Signal Strength and Packet Delivery Ratio. Thus, the authors proof that the jamming attack detection and mitigation based on power consumption level is a feasible way to maintain an acceptable Quality of Service level in wireless network under attack from a reactive jammer.

For future studies the authors should also study the feasibility of using power consumption for jamming attack mitigation for multiple and/or mobile jammer signal source, where the frequency channels used by the devices resembling more like the actual real life condition. Such as every device has at least 11 channels, and some part of each channel is overlapping.

References

[1] Houle, K. J. and Weaver, G. M. 2001. Trends in Denial of Service Attack Technology. *CERT Coordination Centre, Carnegie Melon University*.

[2] Benslimane, A., El Yakoubi, A. and Bouhourma, M. 2011. Analysis of Jamming effects on IEEE 802.11 Wireless Networks. *IEEE International Conference on Communications Proceedings*. 1-5.

[3] Tague. P, Nabar, S, Ritcey. A. J, and Povendran, R. 2011. Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection. *IEEE/ACM Transactions On Networking*. (19)1: 184-194.

[4] Wu, H., Nabar, S. and Poovendran, R. 201. An Energy Framework for the Network Simulator 3 (ns-3). *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*. 222-230.

[5] Misra, S., Dhurandher, S. K., Rayankula, A., Agrawal, D. 2010. Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks. *Journal Computers and Electrical Engineering*. 36(2): 367–382.

[6] Heusse, M., Rousseau, F., Berger-Sabbatel, G. and Duda, Andrzej. 2003. Performance Anomaly of 802.11b. 22nd *Annual Joint Conference of the IEEE Computer and Communications, IEEE Societes*. 2: 836-843.

[7] Bandyopadhyay, A., Vuppala, S. and Choudhury, P. 2011. A Simulation Analysis of Flooding Attack in MANET using NS-3. *International Conference on Wireless VITAE, IEEE*. 1-5.

[8] Hamieh. A. 2012. POWJAM: A Power Reaction System against Jamming Attacks in Wireless Ad Hoc Networks. *9th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*. 9-11.

[9] Xu, W., Ma, K., Trappe, W. and Zhang, Y. 2006. Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network*. 41–47.

[10] Muraleedharan, R. and Osadciw, L. A. 2006. Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System. *Wireless Sensing And Processing, Proceedings Of the SPIE*. 6248.

[11] Network Security Lab, University of Washington (2012, May 10). NS-3 wireless jamming model [Online]. Available: http://www.nsnam.org/wiki/index.php/NS3_wireless_jamming_model.

[12] Ikeda, M., Hiyama, M., Kulla, E., Barolli, L. and Takizawa, M. 2011. Multi-hop Wireless Networks Performance Evaluation via NS-3 Simulator. *International Conference on Broadband and Wireless Computing, Communication and Applications, IEEE*. 243-249.

[13] Bayraktaroglu,E., King, C,. Liu,X., Noubir, G., Rajaraman, R. and Thapa, B. 2008. On The Performance of IEEE 802.11 under Jamming. *The 27th Conference on Computer Communications. IEEE*.

[14] *Qureshi, M. I., Khan, N. U., Rasli, A. M., & Zaman, K. 2015. The battle of health with environmental evils of Asian countries: promises to keep. Environmental Science and Pollution Research, 1-8.*

[15] Qureshi, M. I., Rasli, A. M., Awan, U., Ma, J., Ali, G., Alam, A.. & Zaman, K. 2014. Environment and air pollution: health services bequeath to grotesque menace. *Enviromental Science and Pollution Research.* 22(5): 3467-3476.