Distributed Jammer Network in Opnet Based Wireless Sensor Networks

[1] **Dhanasekaran R,** [2] **Kesavamoorthy A**
[1 & 2]Assistant Professor of Computer Applications
[1 & 2] K.S.Rangasamy College of Arts and Science (Autonomous)
[1 & 2] Tiruchengode, India.

Abstract: Ad-hoc Networks are one of the most important achievements of current technology; they can provide communication without needing a fixed infrastructure, which makes them suitable for communication in disaster areas or when quick deployment is needed. One of these attacks is a kind of denial of service attack (DoS) that interferes with the radio transmission channel, this is also known as a jamming attack. In this kind of attack, an attacker emits a radio signal that disturbs the energy of the packets causing many errors in the packet currently being transmitted. Another version of this attack is to constantly emit random semi-valid packets to keep the medium busy all the time, preventing the honest nodes from switching from the listening mode to the transmitting mode. In rough environments where there is constant traffic, a jamming attack causes serious problems; therefore measures to prevent this attack are required. The purpose of this thesis is to explore the underlying principles of jamming attacks using Opnet as the simulation tool. This work will be helpful so that in future research a useful, practical and effective solution can be created to countermeasure the effects of jamming attacks. The objective here is to understand, modify, and employ the models in OPNET to simulate jamming attacks and understand the limitations of the available models.

Keywords: Jammer, WSN, Opnet Modeler, Denial of Service.

1. Introduction

DJN is different from traditional jammers used by the military, which are typically located outside the target network and cause inference by beaming high-power radio signal over long distance using directional antenna. DJN is also different from the kind of in-network jamming studied recently, which uses jammers of similar size as DWN devices whereas DJN can use much smaller, lower-power devices than DWN nodes. More importantly, existing works on jamming are mostly from the perspective of individual jammers. DARPA realized the importance of DJN in future battlefields and founded the WolfPack program, which is essentially a high power, large-node version of DJN but of which not much technical detail is available in the public. Despite DJN's importance, not much work on the subject has emerged in the research community. This paper intends to advocate studying jamming from a network perspective, rather than from the perspective of individual jammers. A large number of jammers have a network effect which cannot be fully accounted by that of individual jammers. The network approach is conducive to broaden the problem scope considerably and increases the likelihood of obtaining important/interesting results. The advantages of DJN are reminiscent of those of DSN. First, DJN is robust because it is composed of a large number of devices with ample redundancy. Second, DJN nodes emit low power, which is advantageous because of health, self-interference concerns. Third, DJN is hard to detect because of nodes' small size and low power emission. Forth, DJN provides extended coverage with high energy efficiency.

2. Literature Survey

Jamming is defined as a DoS attack that interferes with the communication between nodes. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets. Adversaries can launch jamming attacks at multiple layers of the protocol suite.

Author	**Method**	**Advantages**
Sudip Misra et al	Proposed mechanism for jamming attack detection for wireless sensor networks based on fuzzy inference system-based jamming detection method which follows a centralized approach, wherein the jamming detection is done by the base station based on the input values of the jamming detection metrics received by it from the respective nodes.	Discriminating edge and corner nodes from the rest and allotting various allowances to them for loss of prospective jammed or un-jammed neighbors.
Mingyan Li et al	Proposed optimal jamming attack strategies and network defense policies in wireless sensor network which discuss about the controllable jamming attacks that are easy to launch but are difficult to detect.	Optimal jamming attack and defense policies as solution to optimization problems are analyzed for constant jamming power with one monitor node, constant jamming power with multiple monitor nodes and finally controllable jamming power with multiple jamming nodes.
Cagali et al	Proposed a wormhole based anti jamming technique for sensor networks. An adversary can easily mask the events that the sensor network detects by stealthily jamming an appropriate subset of the	Three solutions have been proposed based on wired pairs of sensors, frequency hopping and uncoordinated channel hopping. These solutions to detect jamming attack involve more complex computations and overhead.

	nodes; in this way, it prevents them from reporting what they are sensing to the network operator.	
Wood et al	Presented DEEJAM, a novel MAC-layer protocol for defeating efficient jamming in networks based on IEEE 802.15.4 compatible hardware. It uses four defensive mechanisms together to defeat or diminish the effectiveness of jamming by attackers in the same capability class as network nodes.	Each additional defense addresses different jamming attack mechanisms to hide communication from a jammer, evade its search, and reduce its impact. Four complementary solutions are frame masking, channel hopping, packet fragmentation and redundant encoding that together significantly reduce the probability of a successful jamming attack.
Wenyuan Xu et al	PSR and PDR for constant, deceptive, random and reactive jammers for BMAC and MAC protocols for varying distances between the transmitting-node and the jammer. They considered additional jammer parameters like on-off periods for the random jammer and different packet sizes for the reactive jammer.	The levels of carrier sensing time, energy consumption, and the received signal strength as well as the received signal spectrum under normal and jamming conditions for two application layer protocols namely Constant Bit Rate (CBR) and Maximum Traffic, and tried to identify the jammer type through spectral discrimination using the Higher Order Crossing (HOC) method.
Xu et al	Proposed a channel hopping and physically moving away from a jammer in Mica2 networks focus on determining when jamming is occurring rather than avoiding it altogether. Two strategies are presented that are employed by wireless devices to evade a MAC/PHY-layer jamming-style wireless Denial of Service attack.	Strategies, channel hopping overhead increases and spatial retreats require node mobility which consumes more energy in sensor networks.
Law et al	Proposed Link layer jamming using MAC layer semantics is a complex type of reactive jamming attacks. A link layer jammer switches between the sleeping and active modes and also adjusts its operation to the MAC layer rules of the participants in the communication.	S-MAC is analyzed for less number of attackers and the sensor nodes exchange messages that are not encrypted.

3. Research Methodology

OPNET Modeler was used to establish and analyze five scenarios which include three client-server and two ad-hoc network scenarios.

➢ Wireless LAN models supported by OPNET Modeler library, in order to test how WLANs were affected by jammers and varying characteristics. Established as a simple client-server network. By changing the parameters of the access point and the distance between the nodes and the access point, multiple experiments were simulated. A fixed pulse jammer was added to the network based on generating jamming attack in the network. How characteristics of the jammer vary the performance of jamming attack was compared in several experiments. In order to test mobile pulse jammer was simulated in OPNET Modeler. Based on client-server network with a mobile pulse jammer used ad-hoc network style.

➢ Including single band jammer, pulse jammer, and sweep jammer. After simulation with all possibilities and changed characteristics, a comparison of different jammers was drawn. Channels were switched in Scenario 4 to test if switch channel could be done in order to avoid jamming attacks.

➢ Communication channels in the networks were switched in order to avoid jamming attacks. Experiments were done to test if switching channel works for every 4 type of jammer. In order to simulate random trajectories for users and jammers, a new method to generate networks and trajectories had been applied. This method was implemented in the ad-hoc experiment.

4. Experimental Results

Signal Strength

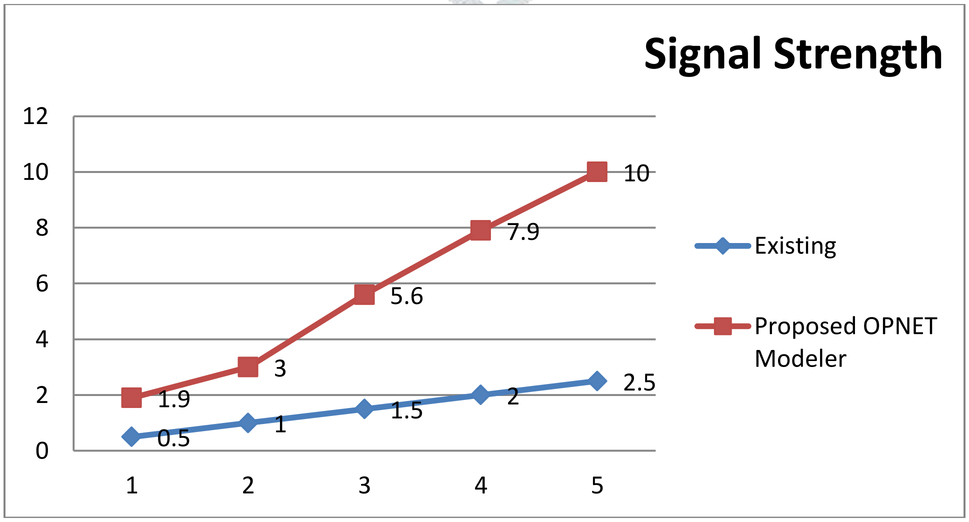

Figure 1: Signal Strength

One of the methods is to determine the strength of the signal by measuring the signal strength and analyzing the signal strength distribution to have the account of the presence of the attacking jammer. The approaches to identify the jamming signal involve comparing average signal magnitude with that of the threshold calculated from the overall noise level. With the study on this method it has been found that the reactive jammer can keep the increase in the effective RSS (Received signal Strength) value very low and hence it avoid being detected.

Carrier Sensing Time

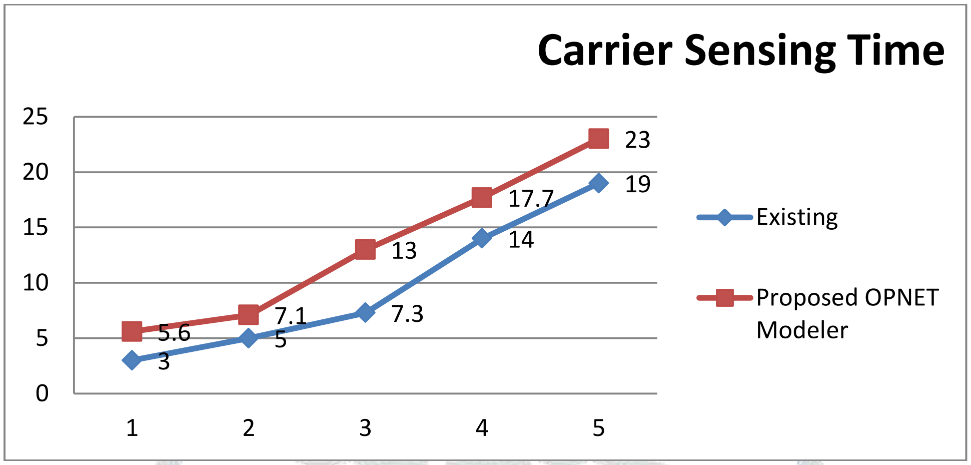

Figure 2: Carrier Sensing Time

A constant Jammer keep the channel constantly busy thus preventing the source to send out packets hence carrier sensing time can be used to know whether the device is jammed or not. Similar to the Signal strength method a channel is idle or not can be determined by comparing the noise level with the fixed threshold. To distinguish between a congestion and jammed scenario carrier sensing time can be used as the sensing time in first will be bounded and in later sensing time will be unbounded.

Packet Delivery Ratio

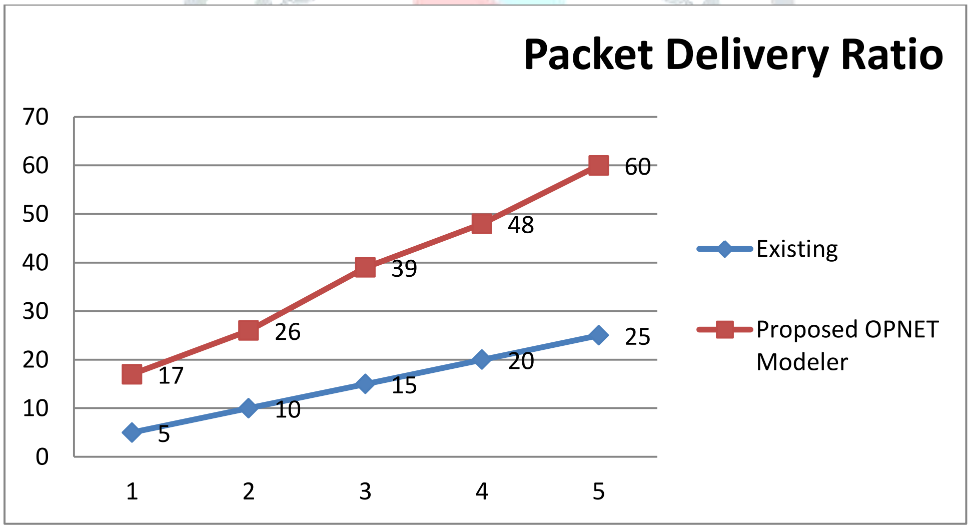

Figure 3: Packet Delivery Ratio

PDR refers to the ratio of packets that successfully delivers to a destination compared to the number of packets that have been sent out by the sender. But here detecting the reactive jammer is a mere challenge because in this the messages are sent very rarely and typically only when it is triggered by some another signal. However PDR can be used to distinguish between the jamming attack and a congested network scenario

Channel Surfing

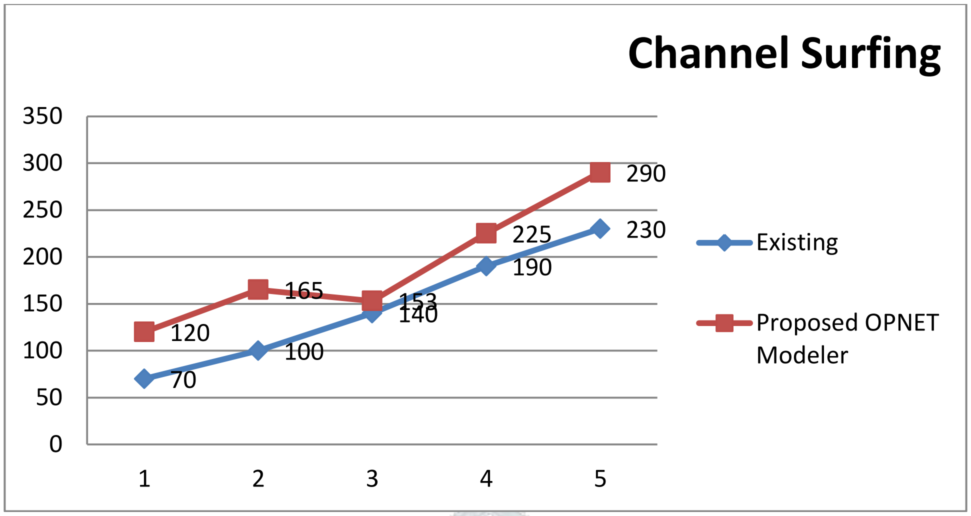

Figure 4: Channel Surfing

Radio communication operates on the single channel therefore if any third party comes in the range of the communication the communicating device may migrate to another channel which is free. This happens in the physical layer of the network and is called as the frequency hopping. Using these technique jammers can be evaded by continuously switching from one frequency channel to another until it finds the free channel to transmit its signal.

Spatial Retreats

This technique is best suitable in a mobile network where the communicating nodes are mobile. This technique is used when there is a jammed area in a mobile network such as user with cell phones or WLAN if the mobile nodes are disrupted by the jammer nodes then the mobile nodes should simply escape to a safe location.

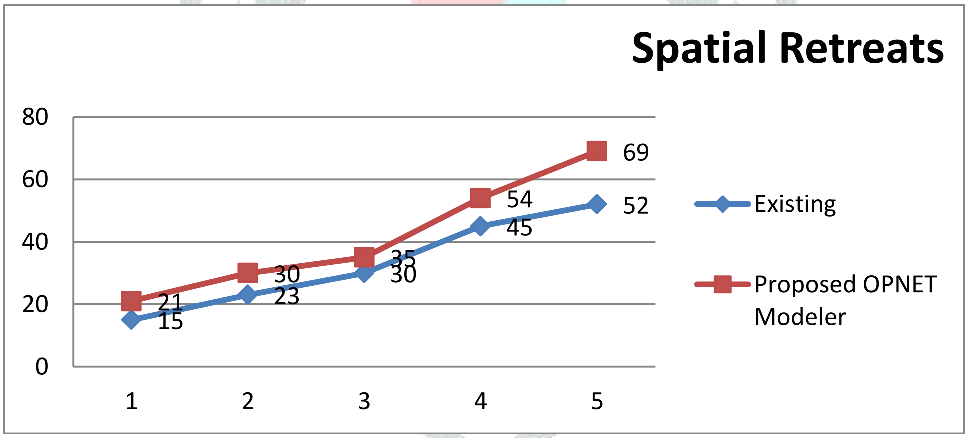

Figure 5: Spatial Retreats

Region Based Signal to Noise Ratio

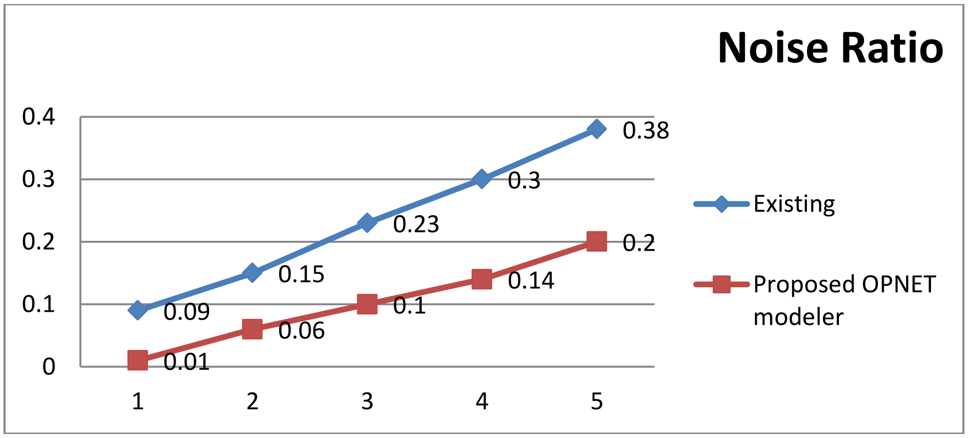

Figure 6: Region Based Signal to Noise Ratio

To now the jamming effects based on the level of disturbance the network can be divided into three categories: unaffected nodes, jammed nodes and boundary nodes. And consider two jamming models region based and signal-to noise- ratio, here the region based model determines the impact of jamming by examining received jammed signal strength. While the SNR based model determines the SNR at the receiver which can estimate the jamming effects more accurately

Conclusion

Jamming attacks launched by different jammers in WLANs were studied and analyzed. A pulse jammer was used in a client-server network. The result proved that jamming attacks did influence the communication between legitimate nodes. When a node traveled toward the pulse jammer, the throughput of the node dropped significantly. The data dropped by the node increased depending on the distance between the node and jammer. The closer the distance was, the more data was dropped. Also, the power level of the jammer varied the performance of the nodes as well. The more powerful a jammer was, the wider the influence would be. A mobile jammer was utilized in a client-server network. The result of this experiment demonstrated how much jamming attacks can influence a network. The legitimate nodes received fewer packets while the mobile jammer was in close proximity, and communications returned to normal as the jammer traveled out of range.

References:

[1] Tamoghna Ojha, Sudip Misra a , Narendra Singh Raghuwanshi b," Wireless sensor networks for agriculture Elsevier, July 2015

[2] Mingyan Liu, " wireless sensor network", IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Volume: 3, Issue: 4, Dec. 2010.

[3] Law et al" Security in Wireless Sensor Networks" 2004.

[4] Wood et al" Security Schemes for Wireless Sensor Network" Feb. 20-22, 2006

[5] H. S. Dhillon, R. K. Ganti, F. Baccelli and J. G. Andrews, "Modeling and Analysis of K-Tier Downlink Heterogeneous Cellular Networks," IEEE J. Sel. Areas Commun., vol. 30, no. 3, pp. 550-560, Apr. 2012.

[6] H. S. Dhillon, R. K. Ganti and J. G. Andrews, "Load-aware modeling and analysis of heterogeneous cellular networks," IEEE Trans. Wireless Commun., vol. 12, no. 4, pp. 1666-1677, Apr. 2013.

[7] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "Stochastic analysis of spatial and opportunistic Aloha," IEEE J. Sel. Areas Commun., vol. 27, no. 7, pp. 1105-1119, Sept. 2009. [8] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: a survey," IEEE Commun. Survey, Tut., vol. 15, no. 3, pp. 996-1019, Jul. 2013.

[9] H. Inaltekin, M. Chiang, H. Poor, and S. Wicker, "The behavior of unbounded path-loss models and the effect of singularity on computed network characteristics," IEEE J. Sel. Areas Commun., vol. 27, no. 7, pp. 1078-1092, Sept. 2009.

[10] B. Blaszczyszyn and M. K. Karray, "Quality of service in wireless cellular networks subject to log-normal shadowing," IEEE Trans. Commun., vol. 61, no. 2, pp. 781-791, Feb. 2013.

[11] H. S. Dhillon and J. G. Andrews, "Downlink rate distribution in heterogeneous cellular networks under generalized cell selection," IEEE Commun. Lett., vol. 3, no. 1, pp. 42-45, Feb. 2014.

[12] I. S. Gradshteyn and I. M. Ryzhik, "Tables of Integrals, Series and Products." Academic Press, Elseiver, 2007.

[13] R. Vaze, "Throughput-Delay-Reliability Tradeoff with ARQ in Wireless Ad Hoc Networks," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2142-2149, Jul. 2011.

[14] M. Di Renzo, F. Graziosi, and F. Santucci, "On the cumulative distribution function of quadratic form receivers over generalized fading channels with tone interference," IEEE Trans. Commun., vol. 57, no. 7, pp. 2122-2137, Jul. 2009.

[15] J. Schloemann, H. S. Dhillon and R. M. Buehrer, "Towards a Tractable Analysis of Localization Fundamentals in Cellular Networks", submitted to IEEE Trans. Wireless Commun., Feb. 2015, available at arXiv:1502.06899.

[16] A. Papoulis and S. U. Pillai, "Probability, Random Variables and Stochastic Processes." 4th edn, New York, NY, McGraw Hill, 2002.

[17] A. Winkelbauer, "Moments and Absolute Moments of the Normal Distribution," in arXiv:1209.4340, Jul. 2014.

Dr.R.Dhanasekaran received his Bachelor of Science degree in Computer Science from Bharathiyar University in the year 2003 and Master degree in Computer Applications from Bharathiyar University in the year 2007. He has received his Ph.D in the field of Computer Networks from Anna University in the year 2017.

Mr.A.Kesavamoorthy received his Master degree in Software Science from Periyar University in the year 2008. He has received his Master Philosophy in the field of Computer Networks from Prist University in the year 2010.