On Denial of Service Attacks for Wireless Sensor Networks

Nischay Bahl
Department of Computer Science and Engineering, National Institute of Technology, Jalandhar, India

Ajay K. Sharma
Department of Computer Science and Engineering, National Institute of Technology, Jalandhar, India

Harsh K. Verma
Department of Computer Science and Engineering, National Institute of Technology, Jalandhar India

ABSTRACT
On denial-of-service (DoS) attacks for wireless sensor networks (WSNs), we investigated the security aspects of the physical layer. We conducted the simulative performance analysis of jamming attacks for signal-to-noise ratio (SNR), bit error rate (BER), network throughput and packet delivery ratio (PDR) using IEEE 802.15.4 based OPNET simulative model for WSN under constant and varying intensity of jamming attacks. Under constant jamming attack, simulations revealed that average sink node PDR degrades from 79.01% in a normal scenario, to 59.22% in jammed scenario. Also, normal scenario shows maximum PDR of 89.68% and minimum PDR of 70.02% while jammed scenario shows a maximum PDR of 64.93% and minimum PDR of 49.90%. Under varying intensity of jamming attack, simulations revealed that average sink node PDR decreases, from 79.01% in a normal scenario, by 5.54%, 4.53%, 6.36% and 3.35% with the introduction of one, two, three and four jammers respectively. Further, the average SNR decreases, from 73.59%, in a normal scenario, by 5.43%, 5.63%, 10.44% and 20.39% with the introduction of one, two, three and four jammers respectively.

Keywords
Wireless Sensor Network (WSN), ZigBee, Security, Denial of Service (DoS), Jamming Attack.

1.INTRODUCTION
The devices, called sensor nodes, find their wide-spread applications in local processing and wireless communications because they are economical, low-power consuming, small in size and easily deployable. Sensor network refers to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements [1, 2]. These networks constitute a large number of self-organizing, massively deployed, low-power, low-cost wireless nodes with applications in the ocean and wildlife monitoring, machinery performance monitoring, building safety monitoring, earthquake monitoring, and many more battlefields applications. Future applications may include highway-traffic monitoring, pollution monitoring, emergency response systems, disaster relief networks, forest-fire detection, land sliding monitoring, volcano-eruption monitoring systems, fault monitoring on railway tracks and environmental monitoring [3, 4].

Ensuring security in WSNs is a challenging task because of various constraints. First, sensor nodes usually have limited resources like - battery power, memory, and computational capabilities. Second, sensor nodes are usually deployed unattended hostile environment and are built without any intrusion detection and prevention in mind. An adversary can easily target a few sensor nodes without being easily noticed and hence, can launch a variety of attacks. Thus, any security mechanism for sensor networks has to be resilient to compromised sensor nodes. Third, most of the sensor applications are based on local computation and communication, while attackers have better computational and energy capabilities. Often, one has to use resource constrained sensor nodes to deal with very powerful attackers. So, traditional security techniques used in wired networks cannot be applied directly [5]. [6-14] discuss various related pieces of work in the WSN security domain. Diversifying application areas of WSNs, enthuse us to analyze the impact of various attacks on network performance with new horizon.

In this paper, we considered a particular class of DoS attacks called *jamming attacks* using IEEE 802.15.4 based OPNET simulative model for WSN, under constant and varying intensity of attacks. The effects of the number of attackers on SNR, BER, network throughput and PDR are inclusively evaluated for simulated scenarios.

The rest of the paper is organized as follow. In section 2 we mention the related work of WSN security. Various types of jamming attacks are described in section 3. We describe the system architecture in section 4. In section 5 we report results of our simulation study, and discuss the results, both for the constant and variable intensity of jamming attack. We conclude our study in section 6.

2. RELATED WORK
[6] explores the DoS threats and defenses by concluding that effective security mechanisms must be considered at the time of network design in order to reduce vulnerabilities to DoS attacks. In [7], the authors investigate that, the Base Station (BS) aggregates sensor readings and conducts control task, hence it is a central point of failure and is vulnerable to jamming attack. Therefore, it is very important to counter attacks pointed at these data-aggregation junctions. In [8], two defense strategies namely, channel surfing and spatial-retreats are used to evade jamming attack. In [9], authors represented a mobile jamming attack with multi-dataflow topologies scheme, where the BS can receive messages from the affected area continuously and the affected sensor nodes need not to re-route under the mobile jamming attack. [10, 11] propose two defense strategies - secure multipath routing to multiple destination BSs, and, anti-traffic analysis strategies to disguise the location of the BS. In [12], the mapping protocol for nodes that surround a jammer, is proposed. In [13], network routing security is analyzed and a countermeasure is proposed. Here, a defense mechanism for different DoS attacks such as spoofing, wormhole, sybil, selective forwarding etc., are presented. A hybrid model of defense against BS jamming attack in WSN is proposed in [14], wherein; the authors

suggest a combination of defense techniques like replication, evasion and multipath routing to counter jamming.

3.JAMMING ATTACKS

Jamming is an attack to deny service to legitimate users by generating noise or fake protocol packets or legitimate packets with spurious timing. As per the definition given by Xu *et al* [15]: "A jammer is an entity which is purposefully trying to interfere with the physical transmission and reception of wireless communications". An ideal jamming attack should have a high energy efficiency (i.e., consume low power), low probability of detection (preferably close to 0), high levels of DoS (i.e., disrupts communication to the desired extent) and it should be resistant to physical layer anti-jamming techniques (i.e., does not allow signal processing techniques to overcome the attack) [16].

Jamming attacks can disrupt communications in any wireless network easily. Any good security design must understand the behavior of various jammers. Jammers are classified as (1) Constant jammers that constantly emit a radio signal, (2) Deceptive jammers that constantly inject fake packets into the network without following the medium access control (MAC) protocol, (3) Random jammers that randomly choose a period of time to sleep and jam and (4) Reactive jammers, which when sense that the channel has a valid traffic being exchanged, they start jamming, (5) Static jammers that are located at fixed location while performing jamming, (6) Mobile jammers that are mobile while performing jamming [17, 18].

4.SYSTEM DESCRIPTION

The simulation model implements physical (PHY) and MAC layers defined in IEEE 802.15.4 specifications using the OPNET Modeler to develop WSN scenarii. These specifications have recently been adopted as a communication standard for low data rate, low power consumption and low cost WSNs. This standard specifies the PHY and MAC sub layers for the Low Rate Wireless Personal Area Networks (LR-WPANs). The ZigBee standard is closely associated with the IEEE 802.15.4 protocol and specifies the network layer (including security services) and the application layer (including objects and profiles). The PHY layer is responsible for data transmission and reception using a certain radio channel according to a specific modulation and spreading techniques. The MAC protocol supports beacon-enabled and non-beacon enabled mode. In beacon-enabled mode, beacon frames are periodically sent by coordinators to synchronize the data sensing nodes with the advantage that all nodes can wake up and sleep at the synchronized time allowing very low duty cycles and hence saving energy. In non beacon-enabled mode, nodes stay active all the time and the devices can simply send their data by using un-slotted CSMA/CA mechanism without using a super-frame structure [19].

IEEE 802.15.4 specifications support both *star* as well as *peer-to-peer* topologies. In the star topology, the communication model is centralized; that is, each node joining the network must send its data to the PAN coordinator for communication purposes, which will then send it to the sink or destination nodes. In peer-to-peer topology, the communication model is de-centralized, and, any device can communicate with any other device within its radio range directly. The *cluster-tree* topology is a special case of the peer-to-peer topology with a distributed synchronization mechanism [20]. Figure 1 depicts the structure of the IEEE 802.15.4 based nodes (PAN coordinator, Guaranteed Time Slot (GTS) nodes, and non-GTS nodes) and analyzer node used in the simulations.

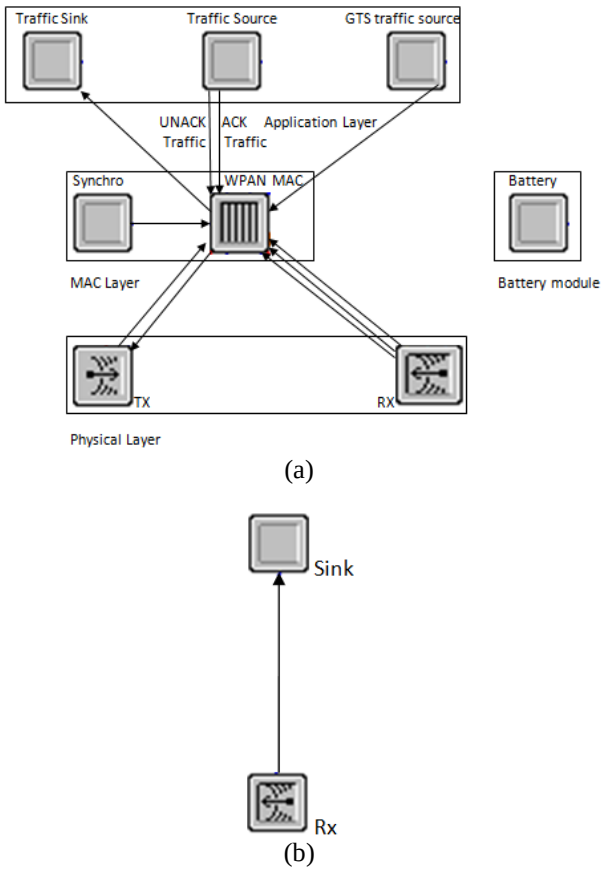

Fig 1: Structure of the IEEE 802.15.4 simulation model (a) PAN coordinator, GTS and non GTS end device (b) Analyzer node

In the simulation design we used the IEEE 802.15.4 based star topology spread over the region 100x100m wide including analyzer node, PAN coordinator and sensing nodes. The normal scenario design consisted of one analyzer node, one Full Function Device (FFD) - PAN coordinator and 16 wireless sensor nodes (Reduced Function Device (RFD)). Jammed scenario design consisted of one analyzer node, one FFD node (PAN coordinator) and 16 wireless sensor nodes (including malicious nodes). Different scenario designs used varying intensity of jamming attack. Malicious nodes used JAMMOD modulation, whereas, the normal sensor nodes used Quadrature-phase-Shift-Keying (QPSK) modulation. The JAMMOD modulation technique causes simulation run to interpret all traffic with interference or noise which degrades the network performance. Table 1 enlists various simulation parameters used in the simulation for PAN coordinator, GTS nodes, non-GTS enabled nodes and jammer nodes.

Table 1. Simulation parameters for PAN coordinator, sensing nodes and jammer nodes

Parameter	PAN Coordinator	GTS enabled end device	Non GTS end device	Jammer device
Mode	Full Function Device (FFD)	Reduced Function Device (RFD)	Reduced Function Device (RFD)	Reduced Function Device (RFD)
Modulation	QPSK	QPSK	QPSK	JAMMOD
Acknowledged traffic source				
Destination MAC address	Broadcast	PAN coordinator	PAN coordinator	PAN coordinator
MSDU inter-arrival time (sec)	Exponential(0.2)	Exponential(0.2)	Exponential(0.2)	Exponential(0.2)
MSDU size (bits)	Poisson(1024)	Poisson(1024)	Poisson(1024)	Poisson(1024)
Start time (sec)	0	0	0	0
Stop time (sec)	Infinity	Infinity	Infinity	Infinity
Unacknowledged Traffic Source				
MSDU inter-arrival time (sec)	Exponential(0.2)	Exponential(0.2)	Exponential(0.2)	Exponential(0.2)
MSDU size (bits)	Poisson(1024)	Poisson(1024)	Poisson(1024)	Poisson(1024)
Start time (sec)	0	60	0	0
Stop time (sec)	Infinity	180	Infinity	Infinity
CSMA/CA Parameters				
Maximum back-off number	4			
Minimum back-off exponent	3			
IEEE 802.15.4				
Device mode	PAN coordinator	End device	End device	End device
MAC address	Auto assigned			
WPAN settings				
Beacon order	7	7	7	7
Super frame order	6	6	6	6
PAN ID	0	0	0	0
Logging				
Enable logging	Enabled			
GTS settings				
GTS permit	Enabled			
Start time	0.0	0.0	Infinity	0.0
Stop Time	Infinity			
Length(slots)	1	1	0	1
Direction	Receive	Transmit	Transmit	Transmit
Buffer Capacity(bits)	5000	1000	1000	1000
GTS Traffic Parameters				
MSDU Inter-arrival Time (sec)	Exponential(0.2)	Exponential(0.2)	Constant(1.0)	Exponential(0.2)
MSDU size (bits)	Poisson(1024)	Poisson(1024)	Constant(0.0)	Poisson(1024)
Acknowledgement	Enabled	Enabled	Disabled	Enabled

5. RESULTS AND DISCUSSION

5.1 Case I: Under constant jamming attack

Here, we performed the simulation runs with constant intensity of jamming attacks and recorded statistics for receiver throughput and packet loss ratio.

5.1.1 Receiver throughput

Figure 2 depicts the results obtained from the simulation runs of normal and jammed scenarii. It is observed that jamming attack deters the sink node radio receiver throughput drastically. The normal WSN scenario used QPSK modulation while scenario with malicious nodes used JAMMOD modulation which created noise or interference in the transmission path and hence deteriorated the network performance. Simulations revealed that average PDR degrades, from 79.01% in normal scenario, to 59.22% in jammed scenario. Also, normal scenario shows maximum PDR of 89.68% and minimum PDR of 70.02%, while, jammed scenario shows a maximum PDR of 64.93% and minimum PDR of 49.90%.

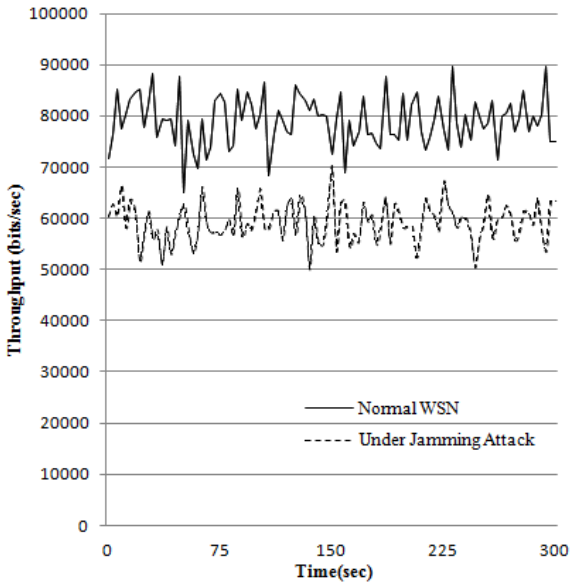

Fig 2: Sink Node Radio Receiver throughput for normal and jammed WSNs

5.1.2 Packet loss ratio

Figure 3 depicts the Packet loss ratio (PLR), from the simulation runs of normal and jammed scenarii. The simulations revealed that average PLR in the jammed scenario is 3.13% higher than that of normal scenario PLR.

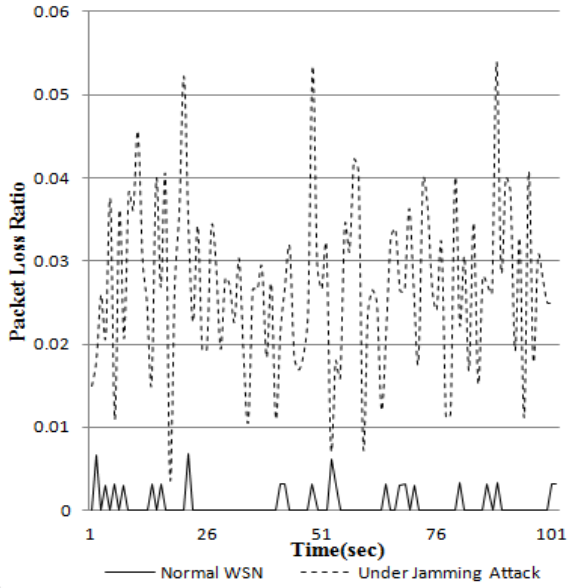

Fig 3: Packet loss ratio for normal and jammed WSNs

5.2 Case II: Under varying intensity of jamming attack

Here, we performed the simulation runs by varying the intensity of jamming attacks. The strength of jamming attack was increased by increasing the number of jamming nodes in scenario design, to study the impact on the packet delivery ratio and signal-to-noise ratio.

5.2.1 Packet delivery ratio

Figure 4 below, shows that the average PDR decreases with increase in jamming strength. It is observed that average sink node PDR decreases, from 79.01% in normal scenario, by 5.54%, 4.53%, 6.36% and 3.35% with introduction of one, two, three and four jammers respectively.

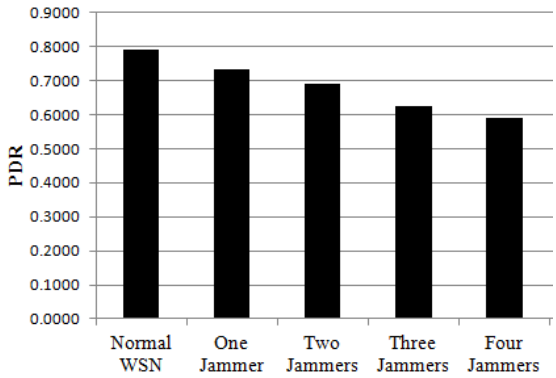

Fig 4: Sink node average PDR for normal and jammed WSNs

5.2.2 Signal-to-Noise Ratio

Figure 5 depicts that the average SNR also decreases with increase in jamming strength. It is observed that average SNR decreases, from 73.59% in normal scenario, by 5.43%, 5.63%, 10.44% and 20.39% with introduction of one, two, three and four jammers respectively. Simulations clearly reveals that increase in intensity of jamming, sharply deters the SNR values.

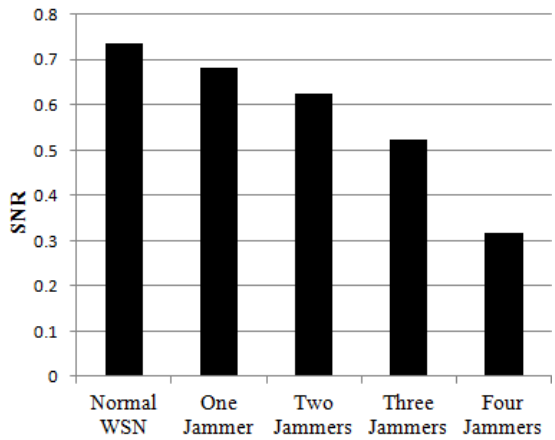

Fig 5: SNR for normal and jammed WSNs

6. CONCLUSIONS

In this paper, the impact of a constant and varying intensity jamming attacks over WSNs have been studied using OPNET simulation software. It is observed that the presence of malicious nodes bring down WSN performance drastically as jamming attack limits the amount of legitimate sensing data reaching the analyzer node. Under constant jamming attack, simulations revealed that average sink node PDR degrades, from 79.01% in normal scenario, to 59.22% in jammed scenario. Also, normal scenario simulations show a maximum PDR of 89.68% and minimum PDR of 70.02% while jammed scenario simulations show a maximum PDR of 64.93% and minimum PDR of 49.90%. Under varying intensity of

jamming attack, simulations revealed, that average sink node PDR decreases, from 79.01% in normal scenario, by 5.54%, 4.53%, 6.36% and 3.35% with introduction of one, two, three and four jammers respectively. Further, the average SNR decreases, from 73.59% in normal scenario, by 5.43%, 5.63%, 10.44% and 20.39% with introduction of one, two, three and four jammers respectively. Future work may involve the study of the effects of mobile jammers on the WSN performance and mechanisms for effectively mitigating these attacks. Further we plan to develop models for the different defense and attack strategies and use these models to adapt dynamically system behavior.

7.REFERENCES

[1] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy (2010): "Denial of Service Attacks in Wireless Networks: The Case of Jammers". In: IEEE Communications surveys & tutorials 2010.

[2] Vassilaras Spyridon and Yovanof Gregory: "Wireless Innovations as Enablers for Complex & Dynamic Artificial Systems". In: Wireless Personal Communications, Volume 53, Number 3, pp. 365-393 (2010).

[3] Robert Szewczyk, Joseph Polastre, Alan Mainwaring and David Culler: "Lessons from a sensor network expedition". In: Wireless Sensor Networks Lecture Notes in Computer Science, Vol. 2920, pp. 307-322 (2004).

[4] Adrian Perrig, John Stankovic, David Wagner: "Security in Wireless Sensor Networks". In: Communications of the ACM, Vol. 47, No. 6 (2004).

[5] JP Walters, Z Liang, W Shi, V Chaudhary: Chapter 17 Wireless Sensor Network Security: A Survey, In: Security in Distributed, Grid, and Pervasive Computing Yang Xiao, (Eds.), Auerbach (2006).

[6] Anthony D. Wood, John A. Stankovic: "Denial of Service in Sensor Networks". In: IEEE Computer, Vol. 35, No.10, pp.54-62 (2002).

[7] Sherif Khattab, Daniel Mosse, and Rami Melhem: "Honeybees: Combining Replication and Evasion for mitigating Base station Jamming in Sensor Networks". In: Proceedings of the 20th international conference on Parallel and distributed processing, p.174-174, April 25-29, Rhodes Island, Greece (2006).

[8] Wenyuan Xu, Timothy Wood, Wade Trappe, and Yanyong Zhang: "Channel surfing and spatial retreats: Defenses against wireless denial of service". In: Proceedings of ACM workshop on Wireless security, pp. 80 - 89 (2004).

[9] Hung-Min Sun, Shih-Pu Hsu, and Chien-Ming Chen: "Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks". In: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, Vol. 1, pp. 457-462 (2007).

[10] Jing Deng, Richard Han, and Shivakant Mishra: "Enhancing base station security in wireless sensor networks". In: Technical Report CU-CS 951-03, Department of Computer Science, University of Colorado, Boulder, CO (2003).

[11] Jing Deng, Richard Han, Shivakant Mishra: "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks". In: Proceedings of International Conference on Dependable Systems and Networks, p.637 (2004).

[12] A.D. Wood, J.A. Stankovic and S.H. Son: "JAM: A Jammed-Area Mapping Service for Sensor Networks". In: 24th IEEE International Real-Time Systems Symposium (RTSS) Cancun, Mexico (2003).

[13] C. Karlof and D.Wagner: "Secure Routing in Sensor Networks: Attacks and Countermeasures". In: Elsevier Ad Hoc Networks, Vol. 1, pp. 293–315 (2003).

[14] Sushil Kumar Jain and Kumkum Garg: "A Hybrid Model of Defense Techniques against Base Station Jamming Attack in Wireless Sensor Networks". In: Proceedings of First International Conference on Computational Intelligence, Communication Systems and Networks, pp. 102-107 (2009).

[15] W. Xu, W. Trappe, Y. Zhang, and T. Wood (2005) "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in MobiHoc, Urbana-Champaign, Illinois, USA, pp 46-57 , May 25-27, 2005.

[16] M. Acharya and D. Thuente, "Intelligent Jamming Attacks, Counterattacks and (Counter) 2 Attacks in 802.11bWireless Networks", in Proceedings of the OPNETWORK-2005 Conference, Washington DC, USA, August 2005.

[17] Xu W, Ma K, Trappe W, Zhang Y.: "Jamming sensor networks: attack and defense strategies". In: IEEE Networks 20(3), pp. 41–47 (2006).

[18] Ghada Alnifie, Robert Simon: "A multi-channel defense against jamming attacks in wireless sensor networks". In: Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks, Chania, Crete Island, Greece (2007).

[19] P.Jurcik, A. Koubaa, (2009): "The IEEE 802.15.4 OPNET Simulation Model: Reference Guide v2", Technical report HURRAY-TR-070509.

[20] Boris Mihajlov and Mitko Bogdanoski: "Overview and Analysis of the Performances of ZigBee based Wireless Sensor Networks". In: International Journal of Computer Applications (0975 – 8887) Volume 29– No.12, September 2011.