I. J. Computer Network and Information Security, 2012, 7, 51-56
Published Online July 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.07.06

Impact of Physical Layer Jamming on Wireless Sensor Networks with Shadowing and Multicasting

Nischay Bahl, Ajay K. Sharma, Harsh K. Verma
Dr. B.R. Ambedkar National Institute of Technology, Jalandhar 144011, Punjab, India
bahl_nischay@rediffmail.com, sharmaajayk@nitj.ac.in, vermah@nitj.ac.in

Abstract — This paper analyzes the impact of a physical layer jamming on the performance of wireless sensor networks by performing exhaustive comparative simulations using multicasting and by employing varying intensity of shadowing (constant and log normal). Comprehensive result analysis reveals that jamming drastically degrades the legitimate traffic throughput in a network, and, the constant shadowing approach is a better fit for a static network, both, under static as well as mobile jammer environments, as compared to the log normal one. An improvement in sink-node packet delivery ratio by 15.02 % and 16.58 % was observed with static and mobile jammer environments respectively, under multicasting and constant shadowing mean of 8.0. Further, average sink-node packet delivery ratio with constant shadowing shows an improvement of 4.15% and 5.94%, using static and mobile jammer environment respectively, in comparison to the values obtained under log normal shadowing based network.

Index Terms — Denial-of-Service, physical layer jamming, constant shadowing, log normal shadowing, multicasting, wireless sensor networks

I. INTRODUCTION

Recent technological innovations have led to the proliferation of wireless mobile devices that enable plentiful of new applications and services. As technology mushrooms, more and more wireless applications start to become an essential part of our everyday life. Technology has made it feasible to deploy small, low-power consuming, inexpensive computational devices called sensor nodes, which are capable of managing local processing and wireless communication [1, 2]. Because of these attributes, wireless sensor networks (WSNs) are used in diverse applications areas like environment monitoring and control, home automation, intelligent buildings, building crack monitoring, automated lighting control, medical body sensors, and surveillance and maintenance among others [3-4]. The constraints of WSN nodes (e.g. Limited battery lifetime, memory space and computation capabilities) and the fact that they are often deployed in a hostile or insecure environment, also increases their vulnerability to attacks and makes the application of traditional security methods used in wired networks, problematical [4]. Glutting application domains of constrained WSNs prompt us to focus on protecting these networks from possible threats and vulnerabilities.

WSNs are prone to a variety of Denial-of-Service (DoS) attacks across different network layers. Jamming is a special form of DoS attack in which an adversary can hamper network performance by creating noise or interference [5]. One can study Jamming both in context of protecting a network against such attacks or, on the contrary, intentionally hampering the communication of some adversary. This paper explores the jamming in the former sense. Jamming attacks targeting the physical layer or the Medium Access Control (MAC) layer are the areas of special research interest across the globe. On the physical layer, an attacker basically jams the radio band whereas, and, on the MAC layer, more sophisticated attacks targeting the protocols are employed. The main contributions of this paper are: comprehensive performance evaluation of WSN using both static as well as mobile jammer environments and performance improvements from physical layer jamming by employing a hybrid technique of shadowing and multicasting.

The rest of the paper is organized as follows. Section II, mentions the related work. Section III, describes the system architecture and the simulation design configuration parameters related to physical layer jamming, routing, multicasting and shadowing. Section IV, presents the results of the simulation study, and discusses the results for the WSN environment, both, with static jammer and with the mobile jammer separately. Section V, concludes the present study.

II. RELATED WORKS

There are several significant contributions made by the research community in the area of the jamming in communication networks. Jamming has been used as a DoS attack to hamper communication since decades [6, 7]. Recently, several jamming related studies have been undertaken in [8-11]. In [12], the authors investigated DoS attacks at MAC layer in wireless networks and classified the jammers 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 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 valid traffic being exchanged, start jamming.

In [13], the authors explored selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops by achieving selectivity with inference from the transmitted control messages. In [14], the authors deal with trivial jamming, simple periodic jamming and intelligent jamming, where the technique of acknowledgement (ACK) corruption jamming, was termed as intelligent jamming.

In [15], two defense strategies - channel surfing and spatial retreats were used to evade jamming attack. However, in channel surfing, changing channels at the data link layer was more expensive because of synchronization between the parties. In spatial retreat, there was evasion overhead in terms of energy and time, which boosted the impact of jamming.

In [16], a mobile jamming attack was represented by multi-dataflow topologies in which, the base station (BS) could receive messages from the affected area continuously and the affected sensor nodes need not to re-route messages under the mobile jamming attack. Channel-selective jamming attacks were considered in [17, 18], where it was shown that targeting the control channel reduces the required power for performing a DoS attack to a great extent. Further, to protect control channel traffic, control information was replicated in multiple channels and the locations were cryptographically protected.

III. SYSTEM DESCRIPTION

In order to investigate the impact of the physical layer jamming on the WSN performance, we resort to a QualNet® Developer Platform simulator of the Scalable Network Technology. More precisely, we considered scenarios that implement physical and MAC layers defined in IEEE 802.15.4 standard for developing ZigBee specifications based WSN environment. The IEEE 802.15.4 standard defines the specifications as the wireless communication standard for low-power consumption, low-rate Wireless Personal Area Network (WPAN). ZigBee is a specification of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard [19-21].

The physical layer provides an interface between the MAC layer and the radio communication channel and supports multiple frequency bands, modulation schemes, spread spectrum functionalities, Bit Error Rate (BER) based reception quality estimation, energy detection, link quality indication and clear channel assessment. The MAC layer supports beacon management, channel access, Guaranteed Time Slot (GTS) management, frame validation, acknowledged frame delivery, and device security. At the physical layer, wireless links can operate in three license free industrial scientific medical (ISM) frequency bands, which accommodate data rates of 250 *kbps* in the 2.4 *GHz* band, 40 *kbps* in the 915 *MHz* band, and 20 *kbps* in the 868 *MHz* [21].

Scenario layout consists of both full function devices (FFDs) and reduced function devices (RFDs). FFDs can initiate a Personal Area Network (PAN) and act as the PAN coordinator, or can forward data and act as the routers, whereas, RFDs collect and transmit the sensed data to the PAN coordinators or sink-nodes by employing shadowing (constant and log normal) and multicasting routing. Scenarios with constant shadowing use a path loss model which predicts the mean received power $P_r(d)$ at distance d [22]. It uses a close-in distance d_0 as a reference point. $P_r(d)$is calculated as shown in equation 1(a),

$$\frac{P_r(d_0)}{P_r(d)} = \left[\frac{d}{d_0}\right]^{\beta} \qquad 1(a)$$

where, $P_r(d_0)$ is obtained by following the free space model. β is called the path loss exponent, which, is usually empirically determined by field measurements. High values of β correspond to more obstruction and hence faster decrease in average received power with increase in communication distance. In addition to the path loss $PL(d_0)$ of non-shadowing models, the new path loss is calculated as shown in equation 1(b),

$$PL(d) = -10log_{10}\left\{\left[\frac{d_0}{d}\right]^{\beta} . \frac{P_r(d_0)}{P_t}\right\}$$

$$PL(d) = -10\beta log_{10}\left[\frac{d_0}{d}\right] + PL(d_0) \qquad 1(b)$$

Scenarios with log normal shadowing follow a log-normal distribution with a user-specified standard deviation. This model takes into account the variation of the received power at a certain distance [22]. The path loss is described as per equation 2,

$$PL(d) = -10\beta log_{10}\left[\frac{d_0}{d}\right] + PL(d_0) + X_\sigma \qquad (2)$$

where, X_σ is a Gaussian random variable with zero mean and a standard deviation σ. Scenarios also used Protocol independent multicasting (PIM) routing, which builds a shared distribution tree centered at a rendezvous point and then builds source-specific trees for those sources whose data rate warrants it [23].

Our experimental wireless sensor network is constituted by 200 Mica-Z nodes, 10 PAN Coordinators and a sink-node deployed randomly in a terrain size of 500 *m* x 500 *m*, employing 2.4 *GHz* transmission channel and two-ray path-loss model. All the experiments have been performed with nodes configured to execute the Ad hoc On-Demand Distance Vector (AODV) routing protocol with simulation run-time set as 1800 *s* and, the mobile nodes (jammers) were configured with defined path trajectories for mobility in space with pause time intervals as 5 *s* and the speed of 12 *m/s*. Three network

configurations have been considered for the experimental tests, with RFDs connected to the coordinator/sink-nodes (i) without using jammer node, (ii) with static jammer, (iii) with mobile jammer. Scenario configurations also employed varying strength of shadowing means (constant and log normal shadowing) and PIM sparse mode routing technique.

In the following, Table I shows WSN simulation general setup parameters, Table II shows the AODV routing protocol parameters used by RFD and FFD nodes, Table III shows the multicasting parameters, Table IV shows jammer node parameters.

TABLE I. WSN SIMULATION GENERAL SETUP PARAMETERS

Simulation Parameter	Value/Option
Terrain size	500 *m* x500 *m*
Simulation time	1800 *s*
Propagation channel frequency	2.4 *GHz*
Path loss model	Two Ray
Shadowing model	Constant/Log Normal
Shadowing mean	0-11 *dB*
Weather mobility interval	100 *m/s*
Antenna model	Omni directional
Antenna height	1.5 *m*
Energy nodes	Mica-Z
Noise factor	10 *dB*
Temperature	290 *K*
Mode	Carrier Sense
Modulation	O-QPSK

TABLE II. AODV ROUTING PROTOCOL PARAMETERS

Routing Parameter	Value/Option
Routing protocol	AODV
Node traversal time	40 *m/s*
Active route timeout interval	3 *s*
Max rreq. retries	2
TTL start	1
TTL increment	2
TTL threshold	7

TABLE III. MULTICASTING PARAMETERS

Multicasting parameter	Value/Option
Multicast protocol	PIM
PIM routing mode	Sparse
PIM-SM triggered delay	5 *s*
PIM-SM bootstrap timeout	10 *s*
PIM-SM candidate RP timeout interval	10 *s*

TABLE IV. JAMMER NODE PARAMETERS

Jammer node parameter	Value/Option
Type	Static/ Mobile
Transmission power (802.15.4)	30 *dBm*
Transmission power (802.11a/g)	150 *dBm*
Jammer mobility model	Random Waypoint
Jammer pause time	5 *s*
Jammer minimum speed	12 *m/s*
Jammer maximum speed	12 *m/s*
Noise factor	200 *dB*
Temperature	350 *K*

IV. RESULTS AND DISCUSSIONS

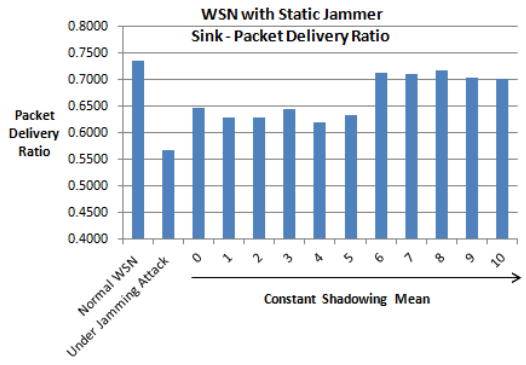
In this section, the results of the study are presented and discussed both for static and mobile jammer WSN environments in sub-sections A and B respectively.

A. Case I: Using Static Jammer

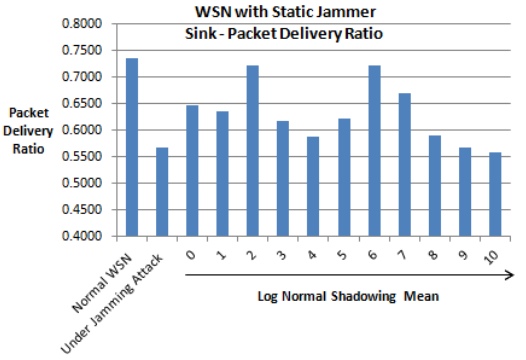
In Fig. 1(a) and 1(b), experimental results relative to the impact of the static jammer on WSN performance, employing constant and log normal shadowing respectively, are presented. Table V, shows the total number of bytes received at the sink-node of a WSN for different shadowing means.

Fig. 1(a) shows that the scenario employing constant shadowing gives high Packet Delivery Ratio (PDR) of 0.7175 with shadowing mean 8.0 and low PDR of 0.6196 with shadowing mean 4.0. An improvement in PDR by 15.02 % is observed by employing constant shadowing with shadowing mean 8.0 and PIM sparse mode routing. Fig. 1(b) shows that the scenarios employing log normal shadowing gives high PDR 0.7224 with shadowing mean 2.0 and low PDR of 0.5584 with shadowing mean 10.0.

Simulation runs revealed that the constant shadowing technique is more suitable in case of static WSN environment, as, average sink-node PDR with constant shadowing is 0.6700 while that with the log normal shadowing is 0.6286, which shows an improvement of 4.15 %.



(a)



(b)

Figure 1. Sink-node PDR using static jammer and multicasting (a) With constant shadowing. (b) With log normal shadowing

TABLE V. SIMULATION RESULTS OF DIFFERENT SCENARIOS OF WSN WITH STATIC JAMMER.

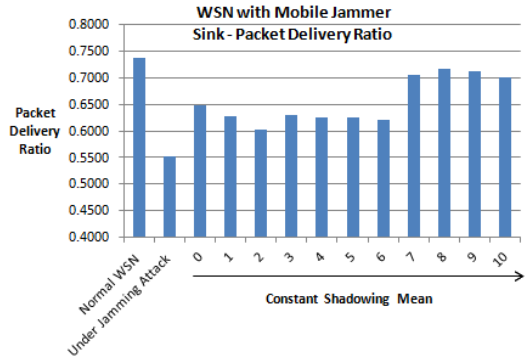
Shadowing Mean (dB)	Under Jamming Attack (Total number of bytes received at Sink-node)	
	With constant shadowing and multicasting	With log normal shadowing and multicasting
10.0	350000	278950
9.0	351680	282940
8.0	358470	294000
7.0	355320	334110
6.0	355880	360080
5.0	316330	309960
4.0	309540	293230
3.0	321510	308560
2.0	314300	360920
1.0	314300	317450
0.0	322560	322560

B. Case II: Using Mobile Jammer

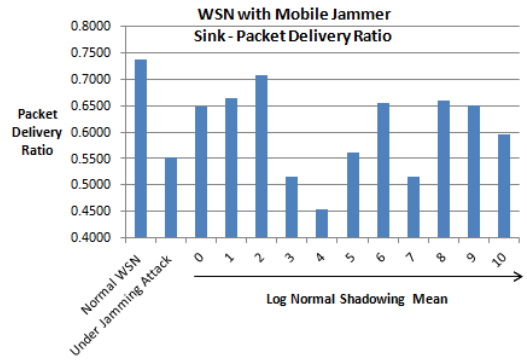
In Fig. 2(a) and 2(b), experimental results relative to the impact of the mobile jammer on WSN performance, employing constant and log normal shadowing respectively, are presented. Table VI, shows the total number of bytes received at the sink-node of a WSN for different shadowing means.

Fig. 2(a) shows that the scenario employing constant shadowing scenario gives high PDR of 0.7173 with shadowing mean 8.0 and low PDR of 0.6031 with shadowing mean 2.0. An improvement in PDR by 16.58 % is observed by employing constant shadowing with shadowing mean 8.0 and PIM sparse mode routing. Fig. 2(b) shows that the scenarios employing log normal shadowing gives high PDR 0.7072 with shadowing mean 2.0 and low PDR of 0.4529 with shadowing mean 4.0.

Simulation runs revealed that the constant shadowing is more suitable in case of static WSN even in the presence of mobile jammer, as, average PDR of constant shadowing is 0.6567 while that of the log normal is 0.5973, which reflects an improvement of 5.94 %.



(a)



(b)

Figure 2: Sink-node PDR using mobile jammer and multicasting (a) With constant shadowing. (b) With log normal shadowing

TABLE VI. SIMULATION RESULTS OF DIFFERENT SCENARIOS OF WSN WITH MOBILE JAMMER.

Shadowing Mean (dB)	Under Jamming Attack (Total number of bytes received at Sink-node)	
	With constant shadowing and multicasting	With log normal shadowing and multicasting
10.0	349650	297080
9.0	355600	324380
8.0	358330	329770
7.0	352730	256970
6.0	309890	326760
5.0	312200	280420
4.0	312690	226240

3.0	314720	256900
2.0	301280	353290
1.0	313460	332150
0.0	323750	323750

V. CONCLUSIONS & RECOMMENDATIONS

In this paper, we have analyzed the impact of physical layer jamming on the performance of WSNs. In particular, we have presented simulation and experimental results, using Qualnet simulator by employing Mica-Z nodes, building various scenarios including normal WSN, with static jammer and with mobile jammer. In all these scenarios, the system performance has been evaluated, considering the impact of constant shadowing, log normal shadowing, and multicasting.

This study shows that there is significant impact of physical layer jamming on performance degradation of WSNs. From the simulation runs of static WSN scenarios, we conclude that hybrid use of the constant shadowing and multicasting technique is a good fit both in case of static and mobile jammers environments, as; average sink-node PDR shows an improvement of 4.15% and 5.94 % respectively for the two environments. However, log normal shadowing is not suitable for static WSNs scenarios, as low sink-node PDRs were observed.

It is further concluded that, PIM sparse multicasting is usefully suitable to counter the effects of jamming by providing additional communication paths in jammed network.

Future work may extend these studies to analyze the impact of other physical layer parameters on WSN energy related policies, mobility and techniques to optimize these parameters to make WSNs better secure, energy-efficient and more adaptable in commercial applications.

REFERENCES

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

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

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

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

[5] Eitan Altman, Konstantin Avrachenkov and Andrey Garnaev. "Jamming in Wireless Networks under Uncertainty", Mobile Networks and Applications, Volume 16, No. 2, pp. 246-254 (2011).

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

[7] M. Simon, J. Omura, R. Scholtz, and B. Levitt. "Spread spectrum communications handbook", McGraw-Hill Companies, 1994.

[8] G. Noubir and G. Lin. "Low-power DoS attacks in data wireless LANs and countermeasures", ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, 2003.

[9] C. Popper, M. Strasser, and S. Capkun. "Jamming-resistant broadcast communication without shared keys" Proceedings of the USENIX Security Symposium, 2009.

[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks", Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 46–57, 2005.

[11] Nischay Bahl, Ajay K Sharma and Harsh K Verma. "On Denial of Service Attacks for Wireless Sensor Networks", International Journal of Computer Applications 43 (6): 43-47, April 2012. Published by Foundation of Computer Science, New York, USA.

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

[13] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. "Energy-efficient link-layer jamming attacks against WSN MAC protocols", ACM Transactions on Sensor Networks, 5(1):1–38, 2009.

[14] D. Thuente and M. Acharya. "Intelligent jamming in wireless networks with applications to 802.11b and other networks", Proceedings of the IEEE MILCOM, 2006.

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

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

[17] Chan, X. Liu, G. Noubir, and B. Thapa. "Control channel jamming: Resilience and identification of traitors", Proceedings of the IEEE ISIT, 2007.

[18] P. Tague, M. Li, and R. Poovendran. "Probabilistic mitigation of control channel jamming via random key distribution", Proceedings of the PIMRC, 2007.

[19] Yu-Kai Huang, Ai-Chun Pang and Hui-Nien Hung. "A comprehensive analysis of low-power operation for beacon-enabled IEEE 802.15.4 wireless

networks", IEEE Transactions on Wireless Communications, Vol. 8 Issue 11, pp. 5601-5611 (2009).
[20] Shigeru Fukunaga et al. "Development of Ubiquitous Sensor Network", Oki Technical Review, Issue 200, Vol. 71, No. 4, pp. 24-29 (2004).
[21] Qualnet 5.0.2 Sensor Network Model Library. Scalable Network Technologies, Inc., Los Angeles, CA (2010).
[22] T.K. Sarkar et al. "A survey of various propagation models for Mobile Communications", IEEE Antennas and Propagation Magazine, Vol. 45, Issue 3, pp. 51 – 82 (2003).
[23] R. Mukherjee and J. William Atwood. "Rendezvous point relocation in protocol independent multicast – sparse mode", Telecommunication Systems, Vol. 24, No. 1, pp. 207-220 (2003).

Nischay Bahl completed his B. Tech. (Computer Science & Engineering) from Kerala University and M. S. (Software Systems) from Birla Institute of Technology, Pilani, Rajasthan (Deemed University). Currently he is pursuing a Ph.D. in the Department of Computer Science and Engineering at Dr. B.R. Ambedkar National Institute of Technology, Jalandhar. He has numerous national and international research publications to his credit. His areas of interest are wireless sensor networks, wireless networks, security aspects, energy related aspects etc.

Ajay K Sharma received his BE in Electronics and Electrical Communication Engineering from Punjab University Chandigarh, India in 1986, MS in Electronics and Control from Birla Institute of Technology (BITS), Pilani in the year 1994 and PhD in Electronics Communication and Computer Engineering in the year 1999. His PhD thesis was on "Studies on Broadband Optical Communication Systems and Networks". From 1986 to 1995 he worked with TTTI, DTE Chandigarh, Indian Railways New Delhi, SLIET Longowal and National Institute of technology, Hamirpur HP. He has joined National Institute of Technology (Erstwhile Regional Engineering College) Jalandhar as Assistant Professor in the Department of Electronics and Communication Engineering in the year 1996. From November 2001, he has worked as Professor in the ECE department and presently he working as Professor in Computer Science & Engineering in the same institute. His major areas of interest are broadband optical wireless communication systems and networks, WDM systems and networks, Radio-over-Fiber (Roof) and wireless sensor networks and computer communication. He has published 237 research papers in the International / National Journals Conferences and 12 books. He has supervised 12 Ph.D. and 36 M.Tech theses. He has completed two R&D projects funded by Government of India and one project is ongoing. Presently he is associated to implement the World Bank project of 209 Million for Technical Education Quality Improvement programme of the institute. He is the technical reviewer of reputed international journals like: Optical Engineering, Optics letters, Optics Communication, Digital Signal Processing. He has been appointed as member of the technical Committee on Telecom under International Association of Science and Technology Development (IASTD) Canada for the term 2004-2007 and he is Life member of Indian Society for Technical Education (I.S.T.E.), New Delhi.

Dr Harsh Kumar Verma is currently working as Head of the Department of Computer Science and Engineering at Dr B R Ambedkar National Institute of Technology Jalandhar. He has done his Bachelor's degree in Computer Science and Engineering in May 1993. He did a Master's degree in Software Systems from Birla Institute of Technology Pilani in Feb 1998 and Ph.D. from Punjab Technical University Jalandhar India in May 2006. He is presently working in the area of Information Security, Computer Networks and Scientific Computing. He has many publications of international national level to his credit.

