ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (27-33), Month: January - March 2015, Available at: www.researchpublish.com

A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks

Munish Dhar[1], Rajeshwar Singh[2]

[1]Dept. of ECE, DIET Kharar, Punjab, India.
[2]Dept. of ECE, Doaba Khalsa Trust Group of Institution Nawanshahar, Punjab, India.

***Abstract*: In recent years wireless sensor networks has gained a lot of attention and is used in number of commercial and military applications including home automation, building structure monitoring, battlefield monitoring and surveillance. In WSN each sensor node is prone to a plenty of possible malicious attacks launched by the invader and there's a need of making the WSN immune to those attacks. The denial of service is most severe attack. Acknowledging the severity of such attacks, this paper first presents the review of security goals followed by types of denial of service attacks at different layers of transmission control protocol (TCP) model. At last various defense strategies against denial of service attacks have been discussed.**

***Keywords*: Wireless sensor networks (WSN), security issues, transmission control protocol (TCP), active attacks, denial of service (DOS) attacks.**

1. INTRODUCTION

Earlier development in semiconductor devices, material science and networking are motivating the ubiquitous use of large-scale wireless sensor networks (WSNs). These technologies have combined together to permit a new invention of WSNs that greatly differs from wireless networks developed nearly 10 years ago. Wireless Sensor Networks (WSNs) basically consists of a large number of spatially distributed nodes including sensors, embedded processor and low power radio for wireless communication with each other and base station. Sensor nodes perform specific task at the intended location. The base station has longer life time, large power and higher data rates on the communication channel as compared to a standard sensor node. The base station performs operations such as network initialization, information gathering, node activation and revocation tasks, and for interfacing with other sensor networks. Sensor nodes are deployed in harsh and remote environments for monitoring and reporting of real-world events to the base station. The advantages of using WSN technologies are undeniable which includes simple and inexpensive deployment due to the use of wireless interface, the ability to be left unattended and longer surviving time [1]. WSN offers a large range of applications that covers basic temperature measurement to more complex applications. These applications include military, personal sensing, camera and video surveillance, body area network, smart building as well as robotics [2]. It is generally believed that, technology advancement in sensors, wireless communication and the network technology has greatly contributed to the worldwide adoption of WSNs applications in today's and future way of life.

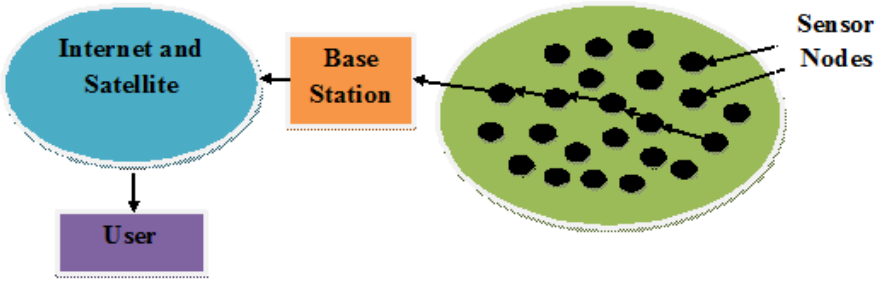

Fig 1: WSN architecture

2. REVIEW SECTION

This section charts out the overview on a plethora of existing ddos defense schemes. We begin our discussion with the Akash Mittal [3], describes different techniques of ddos attacks and the countermeasures which includes different methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP flow analysis. The paper also discusses different tools and software's used to perform DOS attacks in sensor networks.

In [4] author presents ConnectionScore scheme to overcome the ddos attacks occurred at the application layer of TCP model. When attack occurs, any connection is scored which is based on history and statistical analysis is done. From those connections the resources are retaken which take lower scores and considered as adversary or malicious attacks.

In [5] Hao Chen proposes real-time PSD converter based on FGPA to prevent shrew ddos attacks which are low rate TCP targeted attacks. The system uses component-reusable auto-correlation (AC) algorithm and adapted 2N-point real-valued Discrete Fourier Transform (DFT) algorithm.

Muhammad Amir in [6] 2014 analyze various methods to prevent ddos attacks based on traffic anomaly parameters, botnet flux identifications, neural networks, entropy variations, application layer ddos defense and device level defense. The paper also discussed some traditional methods such as trace back and packet filtering techniques.

In [7] author examines the intrusion prevention system for ddos detection and management. The paper also analyses the role of network management systems to detect ddos attacks with minimum losses.

In [8] Monowar H. Bhuyan explains various information metrics which describes characteristics of network traffic data for the detection of both low-rate and high-rate ddos attacks. These matrices include Shannon entropy, Generalized entropy, Renyi's entropy, Hartley entropy and Kullback leibler divergence. To check the effectiveness of each metric different technique such as MIT Lincoln Laboratory, CAIDA and TUIDS ddos datasets are used.

In [9] author discusses Game-theoretic defense framework which describes interaction between an attacker and a defender during a one-shot, non-cooperative, zero-sum game ddos attack.

In [10] author proposed a new method to detect ddos attacks at application layer who considers detection of AL-DDoS attack in high traffic. The method involves a Real-time Frequency Vector (RFV) and attacks can be recognized by investigating the entropy of application layer -DDoS attacks and flash crowds.

3. SECURITY CONCERNS

With the development of wireless and micro-electronics technologies, low-cost and better performance sensor nodes can be easily deployed in wireless sensor networks and have been efficiently used in various kinds of commercial and security applications as discussed in previous section. Once these sensor nodes are deployed in an unsecure environment, it may arise many critical security issues. Due to those issues and difficulties, the security of WSNs is much more complicated. The WSN security challenges and various types of threats are categorized by many researchers. The main issues related with the security of WSNs are Key management, attack detection & prevention, secure routing and secure location [11, 12]. Security services include the following parameters:

Authentication: ensures that the originator of packet or the destination is that node which is claimed.

Access control: prevents unauthorized access to a resource.

Confidentiality: protects the message content as well as avert an intruder from undertaking traffic analysis.

Privacy: prevents adversaries or unauthorized users from accessing private information by analyzing various traffic patterns, i.e. source node, routes, frequency, etc.

Integrity: ensures that the packet received at destination is same as transmitted by source i.e. packet is not modified during transmission.

Authorization: authorizes another node to update or to receive information. Generally services such as authentication and integrity are used for authorization.

Anonymity: hide the basis of a packet or a particular frame. Already discussed data confidentiality and privacy uses basis of anonymity.

Non repudiation: related to authentication. In later case the source proves its identity and former prevents the source node from denying that it transfers the packet.

Freshness: ensures that a malicious or unauthorized node does not send previously captured packets again in the network.

Availability: mainly targets denial of service attacks and is the ability to carry out the various functions of sensor network with no disruption due to security concerns.

Resilience to attacks: required to continue the various functions of sensor network when some nodes are destroyed or compromised [13].

4. TYPES OF ATTACKS

Passive versus active: Based on the mode of operation, attacks are categorized as passive or active. In a passive attack, the goal of intruder is to obtain critical information without being detected. Usually, the attacker remains quiet to eavesdrop on the traffic. Once attacker knows the communication protocols, it can follow those like normal sensor nodes. In this case the invader collects a large volume of traffic data and carries out analysis to obtain secret information. Normally these attackers are very difficult to detect because they do not leave much evidence. In an active attack, the attacker utilize the security holes in the network protocol stack in order to launch numerous attacks such as replaying of packets, packet modification or injection. The impact of these attacks is more powerful than passive attacks. However, abnormalities in the network will show presence of malicious attacks because the attacker is active [14].

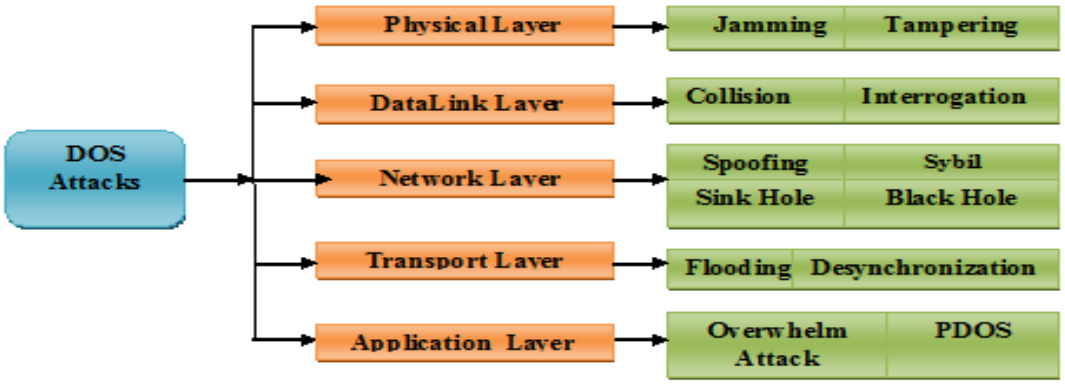

Fig 2: DOS attacks at different layers of TCP model

5. DOS ATTACKS

Each sensor node is prone to a plenty of possible malicious attacks that may be launched by the intruder from either within or outside the sensor network. Due to deployment of sensor nodes over a large area they are, more vulnerable to any of these attacks [1]. Denial of service (DOS) attacks is the most common attack to WSN security. As all the communication between nodes in a WSN is done using wireless link i.e. radio, intruders can perform a number of different denial of service attacks. Since communication is usually done by broadcast intercepting and sending bogus messages is very easy [15].

A Denial of Service (DOS) attack can be described in many forms. In [16], author defined DOS attack as an incident in which a user is deprived of the services of a resource he would normally expect to have, whereas in [17] it was defined as "any event that diminishes or eliminates a network's capacity to perform its expected function". Generally DOS not only means adversary's attempt to subvert, disrupt, or destroy whole network, but also event that decreases a network's capability so that it was not able to provide a service. In wireless sensor networks, several DOS attacks are performed at different layers. These DOS attacks at different layers are discussed in Wood and Stankovic [17]. They consider any type of intentional activity that can disrupt, subvert or even destroy the network as a Denial of Service (DOS) attack. Basically, DOS attacks can be categorized into three types:

• Utilization of limited, partial or non-renewable resources.

• Devastation or variation of configuration data or material.

• Physical damage or amendment of network resources [18].

The adversaries can compromise some sensors and launch the DOS attack by replaying redundant messages or making overdose of fake or bogus messages. Under this situation, DOS attack breaks off the wireless communication channel and results in interference, noise or collision between the senders and the receivers, which leads to a high transmission power signal in a certain area and then overwhelm sensors by flooding bogus or replayed packets. The DOS attack can quickly exhaust the limited energy and block the communication bandwidth, which makes the network, not work well even fail down [19].

6. ATTACKS ON LAYERS OF TCP MODEL

Physical Layer:

1. Jamming: With any radio based medium there always exists the problem of jamming, same is with WSNs. Jamming is a type of attack which interferes with the radio frequencies that network's nodes are using [20]. A jamming source may either only be able to disrupt a very small portion of the network or it may be powerful enough to disrupt the whole network. An intruder has the potential to disrupt the whole network if the jamming sources are randomly distributed in the entire network. Typical defense strategies involve variations in spread-spectrum communication such as frequency hopping and code spreading.

2. Tampering: This is another physical layer attack. By providing physical access to a node, an intruder can remove responsive data e.g. cryptographic keys or related information from the node. The node may also be altered or converted into malicious node from the legitimate one to create a compromised node which is controlled by the attacker. Defense strategy involves tamper-proofing the node's physical package.

Link Layer:

1. Collisions: A collision generally takes place when two nodes try to transmit on the equal frequency concurrently [17]. When packets collides with each other, this results in change in the data portion cause difference in the checksum at the other end. Thus packet will be treated as invalid and discarded. An adversary may continually transmit messages in an attempt to generate large collisions in entire network. This requires retransmission of packets affected by the collision such as ACK or NACK control messages. With help of error correcting codes collisions can be avoided [17].

2. **Interrogation:** This attack makes use of the interaction between nodes before data transmission. For example, WLANs (IEEE 802.11) use Request to Send (RTS) and Clear to Send (CTS) messages. An attacker can consume a node's resources by frequently transmitting RTS requests to obtain CTS responses from a under attack node [17]. Anti replay protection and strong link-layer authentication are some defense strategies against such type of attacks.[21].

Network Layer:

1. Spoofed, altered or replayed routing information: The main attack against a routing protocol in a wireless sensor network is to access the routing information exchanged between the nodes. An attacker may burlesqueor or changes the routing information in order to disturb traffic in the network [22]. This type of disruption includes attract traffic from particular nodes, increasing or decreasing the routes, generate bogus wrong messages, partitioning of network, and increasing end-to-end delay .

2. Black hole: A general guess made in multi-hop networks is that all nodes in the network will truthfully forward receive messages. A specific form of this attack is the black hole attack in which a node drops all messages it receives as if the node doesn't exist at all. An attacker may perform another form of attack by selectively forwarding only certain messages and simply dropping others which is denoted by grey holes [23].

3. Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to nearby nodes by forging routing information [17]. The end effect is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network will flow through the adversary's node.

4. Sybil: In this attack, a single node presents a variety of identities to all other nodes in the WSN. It may deceive other nodes, and hence routes made between valid nodes may possibly be between a valid node and compromised node.

Transport Layer:

1. Flooding: Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [24]. It can be possible that attacker frequently requests for a new connection until all the resources are finished. A very common form of DOS attacks involves sending a large number of common packets aimed at a single destination. The most common packets used are: TCP, ICMP, and UDP. The huge traffic deluge caused by these packets leads the network to no longer be able to distinguish between legitimate and malicious traffic. Basically all available resources such as bandwidth are used up and nothing is left for legitimate use causing the users to be denied the service of the network.

2. De-synchronization: De-synchronization refers to the disruption of an existing connection [23]. An attacker may, for example, repeatedly spoof messages to an end host causing that host to request the retransmission of missed frames. And if the adversary maintains a proper timing, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data to instead waste energy attempting to recover from errors which never really existed. This will cause a considerable drainage of energy of legitimate nodes in the network in an endless synchronization-recovery protocol.

Application Layer:

1. Overwhelm attack: An attacker may forward large volumes of traffic towards a base station to overwhelm the entire network. This results in consumption of whole bandwidth and energy. Its effect can be reduced using Rate-limiting and efficient data aggregation algorithms. [25].

2. Path-based DOS attack: It involves transferring bogus or replayed packets into the network at external or farthest nodes. As it consumes resources on the path to the base station, this will waste away the network of legal traffic. Hence prevents valid nodes to transfer data to the base station. Anti replay protection and packet authentication can prevents these attacks [23]

7. DEFENCE STRATEGIES

Watchdog scheme: It is an important operation for identification of misbehaving nodes. [27]. This is achieved by using concepts such as path-rater and watchdog .Each node uses a watchdog that continuously monitors activities of its neighbors such as the packet forwarding and a path-rater rates the transmission reliability of all alternative routes to a particular destination node.

Rating scheme: It strikes a resonant chord on the significance of making selfishness pay. Selfishness greatly differs from maliciousness as former aims only to save resources for the node itself by refusing to execute any request by the other nodes, such as packet forwarding and not at disturbing the information flow in the sensor network by intension.

Virtual currency: This scheme introduces a type of selfish node that is called nuglets [28]. To insulate a node's nuglets from illegal manipulation, a tamper resistant security module storing all the relevant IDs, nuglet counter and cryptographic materials, is compulsory. In Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out nuglets for its forwarding services.

Route DOS Prevention: This technique takes place at the routing layer to prevent DOS attacks with cooperation of multiple nodes. It incorporates a method to assure robustness, security and fairness targeted to mobile ad hoc networks.

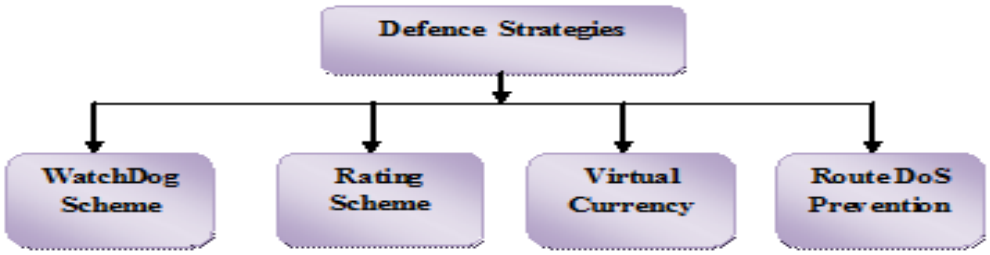

Fig 3: Defence Strategies in WSN

8. CONCLUSION

The wireless sensor networks continue to grow and become widely used in many applications. Thus, the need for security becomes vital. Among all types of DOS attacks in WSN, physical layer attacks are the most difficult to handle because the sensors are not built with powerful radios or the nature of wireless sensor network needs unattended environment. In this paper the security goals and various types of denial of service attacks at different layers of TCP model has been discussed. In the end various defense strategies against DOS attacks have also been discussed.

REFERENCES

[1] Yusnani Mohd Yussoff, Habibah Hashima, Roszainiza Roslib, Mohd Dani Baba (2012), " A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks", International Symposium on Robotics and Intelligent Sensors, Vol.41, Issue.4, April 2012, pp.580-587.

[2] I.F.Akyildiz, W.Su, Y.Sankara subramaniam and E. Cayirci , "Wireless sensor networks: a survey", School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA,20 December 2001

[3] Akash Mittal, Prof. Ajit Kumar Shrivastava and Dr. Manish Manoria, "A Review of DDOS Attack and its Countermeasures in TCP Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011

[4] Hakem Beitollahi and Geert Deconinck , "Tackling Application-layer DDoS Attacks", The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT-2012)

[5] Hao Chen, Thomas Gaska, Yu Chen and Douglas H. Summerville, "An optimized reconfigurable power spectral density converter for real-time shrew DDoS attacks detection", Computers and Electrical Engineering 39 (2013) 295–308

[6] Muhammad Aamir and Mustafa Ali Zaidi, "DDoS Attack and Defense: Review of Some Traditional and Current Techniques", SZABIST, Karachi, Pakistan

[7] Mohd. Jameel Hashmi, Manish Saxena and Dr. Rajesh Saini, "Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System", International Journal of Computer Science & Communication Networks, Vol 2(5), 607-614

[8] Monowar H. Bhuyan, D.K. Bhattacharyya and J.K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection", Pattern Recognition Letters 51 (2015) 1–7

[9] T. Spyridopoulos, G. Karanikas, T. Tryfonas and G. Oikonomou, "A game theoretic defence framework against DoS/DDoS cyber attacks", Cryptography Group, Faculty of Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Clifton BS8 1UB, UK

[10] Wei Zhoua , Weijia Jia b, Sheng Wenc, Yang Xiang c and Wanlei Zhouc, "Detection and defense of application-layer DDoS attacks in backbone web traffic"

[11] Chen X Q, Makki K and Kang Yen, "Sensor network security: a survey" Communications Surveys & Tutorials, IEEE, Second quarter 2009, 11(2): 52–73

[12] TIAN Bin, YANG Yi-xian, LIDong, LI Qi and XIN Yang, "A security framework for wireless sensor networks", The Journal of China Universities of Posts and Telecommunications, Vol.17, Issue.2, February 2010, pp.118–12

[13] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI and Mohammed EL GHAZI, "Wireless Sensor Network: Security challenges" IEEE 2012

[14] T.Thenmozhi and Dr. R.M. Soma, "Towards an approach for improved security in Wireless Sensor Networks", ICCCNT' 12 Coimbtore India, 26 -28 July 2012

[15] Tin Petrović and Mario Žagar ,"Security in distributed wireless sensor networks", University of Zagreb, Faculty of electrical engineering and computing/Department of Control and Computer Engineering, Zagreb, Croatia, MIPRO 2012, May 21-25,2012

[16] Y. Zhou, Y. Fang and Y. Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials", vol.10, issue 3, pp. 6 –28, 2008.

[17] D.Wood and J. A Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, vol. 35, no. 10, October 2002, pp. 54-62.

[18] Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman and Wai Choong Wong , "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" , Ieee Communication Surveys and Tutorials, July 2013. [IF = 6.311]

[19] ZHANG Yi-ying, LI Xiang-zhen and LIU Yuan-an, "The detection and defence of DOS attack for wireless sensor network" jcupt , 2012

[20] D. J. Thuente and M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks", in Proc Military Communications Conf. Atlantic City, USA, (MILCOM) 2006

[21] T. Kavitha and D. Sridharan, "Security vulnerabilities in wireless sensor networks: a survey", Journal of Information Assurance and Security, vol.5, pp.31-44.

[22] Padmavathi and G. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks", International Journal of Computer Science andInformation Security (IJCSIS): vol. 4, no.1 & 2, Dec. 2009.

[23] Karlof.C and Wagner.D, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, May 11, 2003.

[24] EL Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.

[25] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey", Security in distributed, grid, and pervasive computing, Auerbach Publications, CRC Press, ISBN 0-849-37921-0, 2006.

[26] H.Chan and A.Perrig, "Security and Privacy in Sensor Networks", IEEE Computer, vol.36, no. 10, 2003, pp. 103-105.

[27] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. of ACM International Conference on Mobile Computing and Networking , Boston, Massachusetts, USA, (MOBICOM), 2000.

[28] Agah and S. K. Das, "Preventing DOS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach", International Journal of Network Security, vol.5, no.2, pp.145–153, Sept. 2007.

AUTHOR'S BIOGRAPHY:

Er. Munish Dhar is Research Scholar at Doaba Institute of Engineering and Technology, Mohali, Punjab. He has completed his bachelor's degree in Electronics and Communication Engineering (ECE) from BGIET, Sangrur, Punjab, India under Punjab Technical University, Jalandhar. Currently, he is working as research scholar in Electronics and Communication Engineering at Doaba Institute of Engineering and Technology (DIET), Kharar, Punjab, India.

Prof. (Dr.) Rajeshwar Singh is presently working as Director at Doaba Khalsa Trust Group of Institutions, Nawanshahr, Punjab. His area of research are Security, Energy and routing issues in Communication Networks. He received his Ph.D. Engineering degree from Department of Electronics and Communication Engineering, Faculty of Engineering, BIT Sindri, Dhanbad, and Jharkhand. His Master of Engineering degree is in Electronics and Communication Engineering with specialization in Digital Systems from Motilal Nehru Regional Engineering College (currently NIT), Allahabad, U.P. He received his AMIE (India) degree in 1992 from The Institution of Engineers, Calcutta. He has also received Master of Business Administration (MBA) in Information Technology from MD University, Rohtak, Haryana. He has more than 22 years of experience in teaching and industry. He has guided two Ph.D and 12 M.Tech research scholars. Seven Ph.D. and three M.Tech research scholars are working under him. He has published four books and more than 60 papers in national and international journals/conferences of repute.