

Wireless Sensor Network and Its Security Concerns

¹Rohit Tiwari, ²Dr. Ashok Jetawat

¹Mewar University, Gangrar, Chittorgarh, India

²IICE Group of Institutions, Udaipur, India

Abstract

Wireless Sensor Networks (WSNs) are used as one of the greatest vital part to collect information. The WSNs, which have speed and are simple to install and maintain, are going to survive in the real world scenario. Although in the earlier WSNs the security concerns are overlooked, but sensor networks are always used to deal with extremely sensitive content and such networks do not have much interaction with external environment while operating. In this paper first we are discussing the WSN architecture and its core element that is, Wireless sensors. Then we are emphasizing on the need for Wireless Sensors and what are the factors of consideration while selecting a wireless sensor. We also focus on discovering some major security concerns for WSN and proposed a few solutions for the same.

Keywords

Wireless Sensors, Wireless Sensor Network, Wireless Sensor Network Security

Abbreviation

WSN (Wireless Sensor Network)

I. Introduction

We all know the great worth and popularity of wireless networks in the real world scenario because of easy installation, not much further expenses and having many ways to save time and money. There is a form of networking, emerging very fast, in the field of wireless networking known as Wireless Sensor Network. The term wireless sensor can be defined as a measurement tool armed with transmitters to translate signals from process control instruments into a radio signal, which is translated by a receiver who is responsible for the conversion of the wireless signal to a precise, anticipated output through PC software.

The term wireless sensor network can be defined as a blend of actuators and small sensors with general purpose computing elements. WSN holds numerous sensor nodes in a big region. It is an amalgamation of scattered sensing, computing and communication. Hence the Wireless Sensor Network can be best described as Wireless Sensing with Data Networking. In a WSN, there are numerous sensors working together, but all are autonomous and dispersed. All of these sensors, having sensing capability, can monitor, track and detect physical and environmental status at several places.

But many kind of security concerns are there, we have recognized, for a Wireless Sensor Network employment. In this paper, we first discuss the wireless sensor anatomy with wireless sensor architecture with the applications of WSN, and then we emphasis on some major security concerns for Wireless Sensor Networks, as well as, some remedies for such security concerns.

II. Applications of Wireless Sensor Networks

There are hundreds, even thousands of possible applications of Sensor Networks in real life, which pull attention from various miscellaneous fields. Sensor Networks can be quite appropriate in environmental monitoring, warfare, kid's education, surveillance, micro-surgical treatment, and cultivation [11].

Sensor networks also suitable for monitoring and to study natural phenomena which essentially do not encourage human being there, such as storms, forest fires and hurricanes.

There is a big project being worked upon in a renowned university, where environmental data, e.g. air temperature, light, wind, relative humidity, rainfall etc., all are gathered by a network of climate sensors implanted in the communication units installed at the South-West Rift Zone in Volcanoes National Park on the Big Island of Hawaii. This project is being worked upon quite successfully, although there is a quite important issue in front of the researchers that how to make the sensors imperceptible to inquisitive tourists.

The sensor networks can provide huge benefits to Medical Research and Healthcare, as with sensor networks most of the natural applications like vital sign monitoring and accident recognition can be successfully deployed.

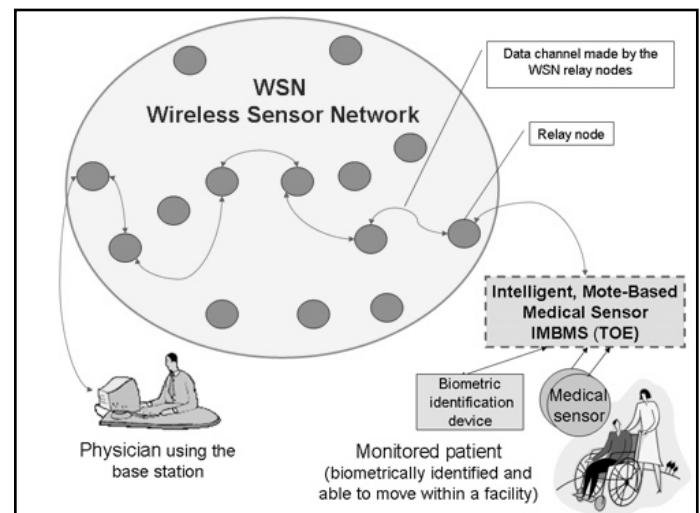


Fig. 1: Wireless Sensor Network Applications in Medical Research and Healthcare

In such applications, the sensors can be used to capture vital signs from patients in real-time and communicate the statistics to handheld computers carried by medical personnel, and there can be wearable sensor nodes, with which patient statistics such as ID, disease history, and treatments can be stored.

Keeping applicability of Sensor Network in Medical research and healthcare, one major university is developing an infrastructure in cooperation with another university's School of Medicine. This infrastructure is intended to provide a support for wireless medical sensors, PDAs, PCs, and other such devices that can be used to observe and cure patients in a number of medical circumstances [6].

III. Why Wireless Sensors

There are many advantages of using wireless sensors in different real world scenarios. Some major advantages are listed as below:

A. Safety

The wireless devices can be used at the locations which are

not easy to access because of life-threatening conditions such as high temperature, high pH, high pressure, etc. Operator can uninterruptedly supervise practices in life-threatening atmospheres and report the statistics back to another operator in an observing facility situated at a harmless distance away. In the locations which are quite difficult to access, the wireless measurement can be brilliantly convenient for obtaining data.

B. Convenience

A network can be formed with the help of wireless sensors and the same provides an engineer to monitor a quantity of diverse sites from one base station. This all provides a centralized control of an organization. Apart from this, many wireless sensors as a group are able to create an exclusive web page which provides minute-to-minute up-to-date data and it can be accessed from everywhere in the world.

C. Less Cost

Wireless process control helps in reducing the monitoring and running cost for an organization just by eradicating the requirement for conduit, extension wire, and many other expensive accessories [16].

IV. Wireless Sensors

The sensors are essentially the core of any security inspection system. The sensors, which give great response at relatively low frequency, are very significant for the development of a low price sensing system. There are basically three types of electromagnetic sensors used here, which are: (a) meander, (b) mesh and (c) inter-digital [1]. All of them are appropriate for inspection and assessment of system characteristics in a way, which is non-destructive and non-invasive.

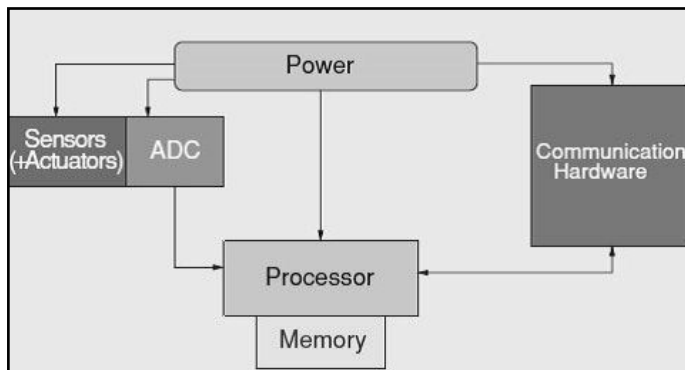


Fig. 2: Structure of a Wireless Sensor Node

V. Wireless Sensors Types

There are following types of wireless sensors available as per the applications in real world:

A. Transmitters

Transmitter type of category uses scientific sensors to measure a specific property in a process, e.g. thermocouples, pressure transducers, flow meters, etc., and then communicate the data through radio signals to a receiver.

B. Receivers

Receiver type of category receives and interprets the wireless data. The receiver 'reads' a radio signal and translates the same into the anticipated output e.g. contact closure, analog output, or digital display. Some receivers can even export the data to advanced software.

C. Transceivers

Transceivers type of category contains a transmitter and receiver in a sole unit. The transceivers have ability to rebroadcast signals, which makes wireless transceivers able to extend the scope of your wireless measurement network.

D. Controllers

Controllers type of category have functions same as of a receiver in the sense that such controllers receive and analyze data from wireless transmitters. However, the wireless controllers are also able to manipulate a process based on the data being measured. For example, if a furnace becomes too hot, a controller can identify the increased temperature and send a signal to switch off some heating elements.

E. Data Loggers

Data Loggers belong to an extraordinary kind of wireless measurement network as they give a new dimension of elasticity to the end user. Such wireless data loggers are able to remotely monitor temperature anywhere and then transmit the data back to an engineer once the component is brought to a receiver. These miniature wireless sensors are quite advantageous for applications that comprise of a roaming component e.g. food being shipped. In this example, by packaging a wireless data logger within a shipping container, a vendor or transporter will be able to make sure and certify that products were refrigerated all the way to a distributor or grocery store [16].

VI. Factors of Consideration for Selection of a Wireless Sensor

Following are some of the major factors of consideration for selection of a wireless sensor [16]:

1. Type of Measurement
2. Accuracy and Response Time
3. Range
4. Frequency

VII. Architecture for Wireless Sensor Network

Wireless Sensor Network architecture is a composition of following components as discussed under-

A. Sensor Nodes

The sensor nodes are at the base of the WSN architecture as we can see in fig. 3. These Nodes are actually tiny devices generating a computable response to a deviation in a physical or environmental condition. All of these sensors can be used independently to compute and to convert a physical or environmental amount into a signal which is read by a device or by an observer. Sensor Nodes are used for routing of packets for additional devices must be done by them only. The process or process apparatus is mostly characterized or controlled by them. There is a special type of field device, called as router, which does not have control apparatus or process sensor. Router has interface with the process itself. As it is shown in the Fig. 3, there are basically three groups of sensor nodes. At the very bottom, there is a group of thousands of special-purpose sensor nodes e.g. Asset Tags. At the top of these, there is a group of hundreds of generic sensor nodes e.g. Door/Window Motion Sensors, and at the top of the sensor nodes hierarchy, there are dozens of high-bandwidth sensors e.g. Cameras and/or Microphones.

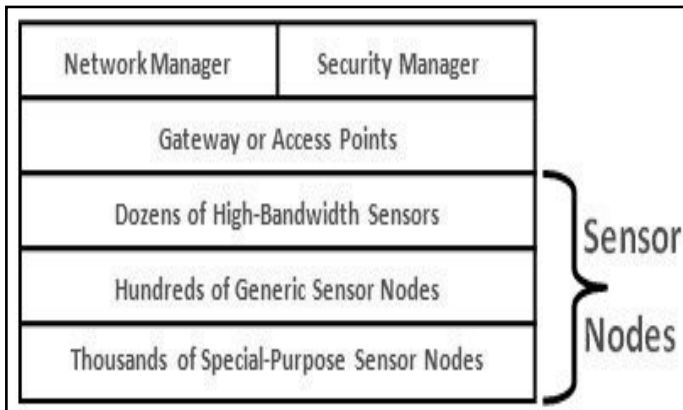


Fig. 3: Wireless Sensor Network Architecture

B. Gateway or Access Points

These instruments provide communication between field devices and host application. It handles web interfaces and databases.

C. Network Manager

Network Manager is accountable for setting up communication among devices, management of routing table, observation of the network and reporting the status for the same. It handles configuration of the whole network too.

D. Security Manager

Security Manager is accountable for key creation, stocking and management.

VIII. Types of Wireless Sensor Network

There are basically two types of wireless sensor networks on the basis of organization, as discussed below-

A. Unstructured WSN

Unstructured WSN is having a dense collection of nodes, follows ad-hoc deployment, and it is difficult to maintain.

B. Structured WSN

Structured WSN is having a few and scarcely distributed nodes, follows pre-planned deployment, and it is comparatively easy to maintain, due to less maintenance concerns.

IX. Security Concerns for Wireless Sensor Networks

Security Concerns for Wireless Sensor Networks can be broadly categorized two different phases, (a) the attack over the elementary mechanism (e.g. routing), and (b) the attack over the security mechanism. We will present some of the major security concerns for WSN. The four basic attributes, which are required for a secure wireless sensor network, are –

- Authenticity
- Availability
- Integrity
- Confidentiality.

The major security concerns for WSN are discussed in brief as under:

A. Denial of Service

Denial of Service attack is encompassing by failure of unpremeditated of nodes. DOS attacks are destroyed the resources at destination node by the sending of unwanted extreme packets, so that it can prevent the network to access amenities. Many DOS attacks are performed in various wireless sensor network

layers [7].

B. Sybil

Sybil is another major security concern for WSN. In this kind of attack, the attacker creates more than one identity for a single node and successfully manages the same, though many protocols follow the rule that a single node characterizes a unique identity. The fundamental concept behind the Sybil attack is that in such kind of attack the attacker used to present at multiple places, but at the same time. The attacker is also selected as a regular next-hop in topographical advancing by creating fake identities of nodes located at the edge of communication region all around a target object.

C. Wormhole

More than one attackers work in co-operation to provide a low latency side channel for communication, in Wormhole attack [8]. Let's discuss a scenario for better understanding of wormhole attack, suppose we have two attackers who are equipped with a long range link and a separate radio for communicating over a high speed.

With the help of side channel, one attacker will communicate the message received by him. The messages are transferred in side channel assuming that all these messages are only one node far from the original source. in wormhole attack the adjacent nodes provide a favor to the attacker because they presume that the link provided by attacker decreases the distance between two adjacent nodes. It makes the adjacent node to believe that by using this side channel, instead of being denied the services will be improved. Due to all this the network will move into an unpredictable state.

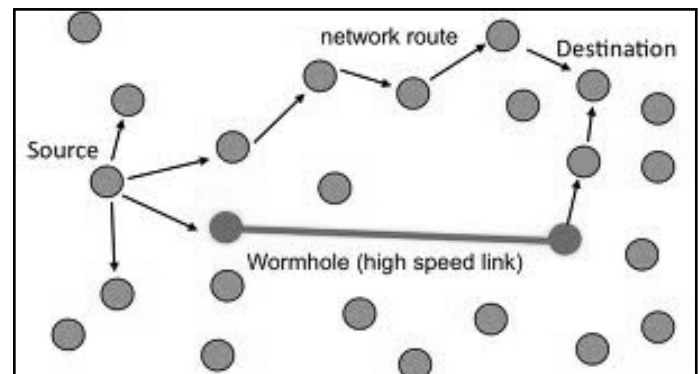


Fig. 4: Wormhole Attack

D. Sinkhole (Black Hole)

In the case of Sinkhole attacks a compromised node is prepared to appear entirely appealing to its neighboring nodes as per the routing algorithm. And then this compromised node is used to get almost all of the network traffic diverted to itself from a precise region. A symbolic sinkhole with the adversary at the center is being created by this process [5]. Such kind of attacks might support other security concerns for example selective forwarding, to WSN, because it provides so many opportunities to destruct the application data to the nodes close or on the route of packet.

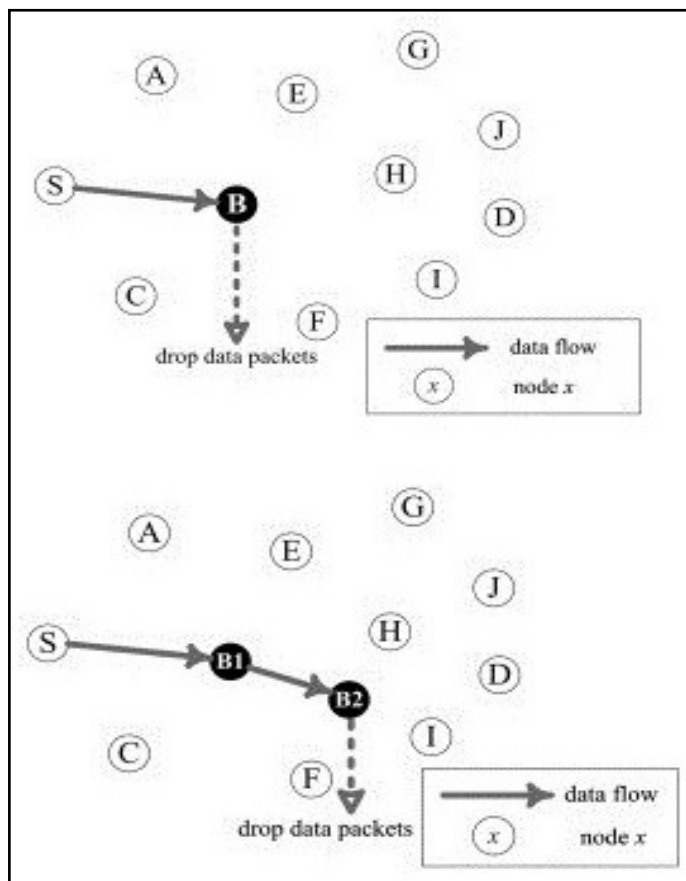


Fig. 5: Sinkhole Attack

E. Selective Forwarding

If the Wireless Sensor Networks need to provide a preferred forwarding route, then they depend upon each and every node in the network to participate in routing for the nodes which are adjacent.

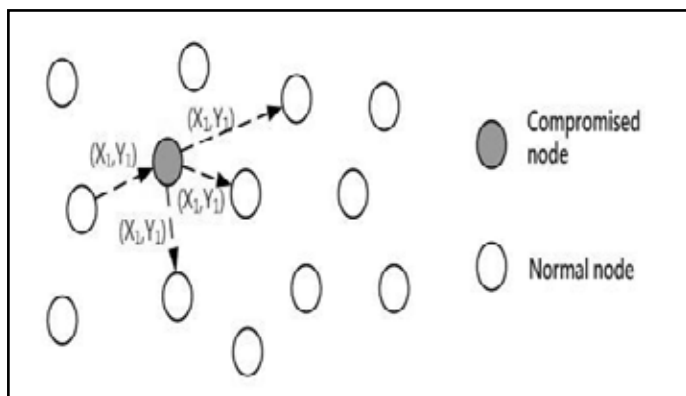


Fig. 6: Selective Forwarding Attack

Most of the selective forwarding security concerns might put an end to this dependency which results in Denial of Service using routing. An undermined sensor device will simply refuse to transmit certain messages. In return the local loss rate is increased by the random dropping policy, which prompts expensive end-to-end recovery practices. The attacker might also utilize base stations or rest of the servers as victims and then might drop messages to or from.

F. Hello Flood

In such attacks, the attacker uses hello packets as a weapon to influence the sensor nodes. The attackers send hello packets to

multiple sensor nodes in which are widely spread in a huge area in Wireless Sensor Network. The victim node puts all of its efforts to go through the attacks consequently while communicating the message to the sink. All adjacent nodes keep believing of the fact that it is their neighbor and eventually betrayed by the attacks.

X. Proposed Solution Mechanisms

The proposed protection techniques, for some of the above discussed attacks, are described as under-

A. Denial of Service Attack Protection

There are a number of mechanisms to achieve protection from the denial of service attacks. To name a few we have payment for network resources, pushback and strong authentication and identification of traffic [15]. One of the security technique, which uses the authentication streams to secure the reprogramming procedure. In this approach a program binary is divided into a series of messages, in which each has a hash of a next message. This technique offers assurance that an intruder cannot take over a currently running program transmission, even if he or she is aware of the hashing technique. The concept behind the working of this technique is that it will be nearly impossible to generate a message that matches the hash present in the earlier message [4]. With the help of present encryption and authentication mechanisms, users can get fortification against several attacks, and there are some other mechanisms which can be utilized to alert network managers regarding present attacks or trigger mechanisms to preserve energy on affected devices.

B. Wormhole Attack Protection

For the protection of wormhole attack, user can utilize a proactive routing protocol known as DAWWSEN [9]. In this protocol a hierarchical tree is constructed in which base node acts as base station and the sensor nodes are denoted as the leaf (internal) nodes of the tree. With the help of DAWWSEN provides, the user can be benefited as it does not require any kind of physical information of the sensor nodes and does not take the time stamp of the packet as a process to detect a wormhole attack, but it is very important for the resource controlled nature of the sensor nodes [9].

C. Sybil Protection

The protection technique for Sybil attack protection relies over the utilization of ID certificates. In this process, it follows a very basic approach, where even before deployment the setup server allocates every sensor node certain unique information. After that it creates an ID certificate which joins this ID of node to the assigned unique information, and transfers this information into the node. To display its ID in a secure manner, a node needs to present its ID certificate first, and then proves that it possesses or matches the related unique information. This whole process comprises of receiving and transferring of frequent messages. A hash tree is being proposed by Merkle which is utilized pretty often as an elementary resource for ID certificates computation [4]. This proposed hash tree is a vertex-labeled binary tree, where each non-leaf vertex label is a hash of the combination of the labels of its two child vertexes. The set of vertexes on the path from the leaf to the root of the tree is the primary path of a leaf vertex. The authentication path has the siblings of the vertexes on this primary path. One can compute the primary path up to and including the root of the tree, if provided with a vertex, its authentication path, and the hash function. And at the last, to verify the legitimacy of the label of the leaf vertex this computed value of the root can be

compared with a stored value.

D. Selective Forwarding Attack Protection

For the protection of selective forwarding attacks, one mechanism is specified which called multipath is routing. Whether the message are communicated along with the route which has completely fragmented to the sensor nodes, so these messages are entirely secure from selective forwarding attacks [3].

E. Sinkhole Attacks Protection

It is very difficult to protect against sinkhole attacks, however there is a one protocol class which is helpful for protection of sinkhole attacks that is known as geographic routing protocols. This protocol is capable to construct a network structure as per the requirement of limited interaction and particular information [2], and any initial point it is not required.

F. Hello Flood Attacks Protection

We can get protection from hello flood attack to the use of proper examine the link's in both directions so that the nodes get assure that they have to reach at their parent node inside the single hop.

XI. Related Works

The present research in wireless sensor network emphasis on application driven systems so that, it can address more solid concerns. Introductory outcomes acquired from these deployments are inspiring and extensive use is extremely expected.

IBM is also doing research over Wireless Sensor Network. In its research IBM is using its proficiency in wireless networking, advanced middleware perceptions and embedded platform design to craft state-of-the-art concepts, proficient architectures and reference designs for end-to-end enterprise solutions. IBM built a reference testbed, which can be utilized to verify IBM's end-to-end concept, assess performance and scalability, and which serves as a demo platform for client engagements [10].

WSNs are capable of enhancing system performance significantly so they hold considerable promise to Industry. WSN technology is slowly graduating from the researcher "market" to the early adopters in industry. Several start-up companies are offering products in the sensor networking domain: Sentilla, Sensicast, Point8, ArchRock, SynapSense, Crossbow, sensorial, and others. Industrial research labs have also funded sensor networking research. In some cases, the technology is showing up in vertical niche markets, e.g., in process control, where it is not even advertised as WSN. The military continues to fund research in this area, now more so in the context of aiding mobile dismounts/units, but is yet to seriously adopt the technology in its operation.

A recent issue of IEEE Spectrum classified WSNs as one of the top 10 emerging technologies. Eventually, it is felt by most of the research community that it will pervade into daily life like the cell phone technology. WSNs may either connect to the rest of the world through the cellular network or through the wired internet. In any case WSN impact on the traditional networks is likely to be transformative, simply by taking into account the amount of data that will enter/leave as machines talk to enterprises and other machines. WSNs have a major role to play in cyber-physical systems, pervasive computing, Body Networks and Internet of Things.

According to Freedonia Group report on sensors, 2002, Sensor market in 2001 was approximately \$11 Billion while the Wiring installation costs were more than \$100 Billion. With recent

advances and availability of wireless sensor device that can be battery powered the cost of wiring would be the major saving. Further over-the-air programming and solar power sensor devices, helps in reducing the deployment and maintenance cost to a large extent.

XII. Conclusion

The area of WSN is thriving and every day new ideas are emerging. The wireless sensor networks have an unexpected growth presently because of its enormous number of sensor network applications in numerous fields. But to transmit and receive sensitive data in the wireless sensor networks without compromising its security is a critical job. In other words, the industry will only adopt a WSN based application, when it provides assurances on full security in all aspects. Although there are potentials that upcoming research over confidentiality and authenticity in WSN will make it a smart choice in innumerable new fields. Recently presented security techniques are focused on specific network structures, hence it is less efficient to deliver a comprehensive solution for the security in wireless sensor networks. In this paper, we analyzed the basic structure of a wireless sensor network, with its core ingredient Wireless Sensors. We also analyzed few major security attacks for wireless sensor networks & proposed solutions for the same.

XIII. Acknowledgements

This work was supported by and completed under guidance of my guide Dr. Ashok Kumar Jetawat², who is co-author for this research paper too. The authors thank to Mr. B. L. Pal, Head of Department, Department of Computer Science, Mewar University, India, for his kind guidance in the research and as reviewer to this research paper.

References

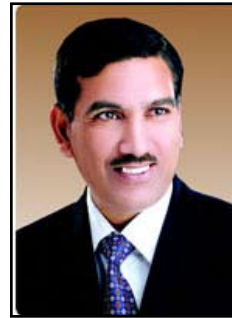
- [1] S. C. Mukhopadhyay, C. P. Gooneratne, G. Sen Gupta S. Yamada, "Characterization and Comparative Evaluation of Novel Planar Electromagnetic Sensors", IEEE Transactions on Magnetics, Vol. 41, No. 10, pp. 3658-3660, Oct. 2005.
- [2] M. Zorzi, R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance", IEEE Transactions on Mobile Computing, Vol. 2, No. 4, pp. 337-348, 2003.
- [3] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, "Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks", Mobile Computing and Communications Review, Vol. 4, No. 5, October 2001.
- [4] David R. Raymond, Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing, Vol. 7, No. 1, 2008, pp. 74-81.
- [5] Hemanta Kumar Kalita, Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.
- [6] T. Fulford-Jones, D. Malan, M. Welsh, S. Moulton, "CodeBlue: An ad hoc sensor network infrastructure for emergency medical care", in International Workshop on Wearable and Implantable Body Sensor Networks, London, UK, 2004.
- [7] Md. Anir Rehman, Mitu Kumar Debnath, "Energy Efficient Data Security System for Wireless Sensor Network", Sixth International Conference on Computer and Information Technology, 2008.
- [8] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet leashes: A Defense against Wormhole Attacks in Wireless

Networks", In Proceedings of IEEE Infocom 2003, April 2003.

- [9] Rouba El Kaissi, Ayman Kayssi, Ali Chehab, Zaher Dawy, "DAWSEN: A Defense Mechanism against Wormhole Attack in Wireless Sensor Network", Proceedings of the Second International Conference on Innovations in Information Technology (IIT, 2005).
- [10] D. Braginsky, D. Estrin, "Rumor routing algorithm for sensor networks", In ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
- [11] M. Haenggi, "Opportunities and Challenges in Wireless Sensor Networks", in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL, pp. 1.1–1.14, CRC Press, 2004.
- [12] John R. Douceur, "The Sybil attack", In IPTPS, pp. 251–260, 2002.
- [13] Anthony D. Wood, John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Department of Computer Science, University of Virginia.
- [14] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.
- [15] A.D. Wood, J.A. Stankovic, "Denial of Service in Sensor Networks", Computer, Vol. 35, No. 10, 2002, pp. 54– 62. J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, Vol. 61.
- [16] "Types of Wireless Sensors and Factors of Consideration for Selection of a Wireless Sensor" [Online] Available : <http://www.omega.com/wirelessensors.html>



Rohit Tiwari received his Bachelor of Engineering degree in Computer Engineering from Rajasthan University, India, in 2006. He had worked as a Software Engineer at Trianz Inc., Bangalore for 3 years. At present he is M. Tech. Scholar at Mewar University, Chittorgarh, India. His research interests include Wireless Sensor, Wireless Sensor Network, Cloud Computing and Pervasive Computing.



Dr. Ashok Kumar Jetawat is a Managing Director of IICE College, Udaipur, Rajasthan (India). After completing M. Tech. (IT) and MBA, he did his PhD from Mohan Lal Sukhadia University on "A Critical Evaluation of e-Governance Implementation in Rajasthan State". He is having more than 30 years of experience in the field of information technology. He is the member of "Special Interest Group on e-Governance" of Computer Society of India. His area of interest is to study and provide consultancy for successful implementation of e-Governance and e-Learning implementation in India. The author received "Rashtriya Ratana Award" in 2002 for individual outstanding performance. He is the research guide and life member of CSI, IE (India), IIIE, IIMM, ISTD and many professional bodies. He is also the active member of Internet Governance Capacity Building Program (IGCBP) whose head office is in MALTA.