ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Enhancing Security of Wireless Sensor Network

Anil M. Hingmire

Abstract*— This paper shows how we can enhance security of the wireless sensor networks. In order to send confidential data from sensor node to sink node and also physical threat is possible to sensor node. Security mechanism can be applied at sink node to protect various threats in OSI layers and also achieve the security goals. This paper suggests architecture to deal with various types of attacks based on Encryption and hardware processor for Wireless Sensor Network (WSN).

***Index Terms*— Encryption, Decryption, WSN, Wireless Sensor Network Architecture, sink node, threats, OSI layers etc.**

I. INTRODUCTION

One of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical environment. A sensor network1 is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The environment can be the physical world, a biological system, or an information technology (IT) framework. [1] Sensing, processing and communication are three key elements whose combination in one tiny device gives rise to a vast number of applications. [2] Although a number of proposals have been reported concerning security in WSNs, provisioning security remains critical and challenging task. WSNs have attracted much attention due to its great potential to be used in various applications. Possible applications of sensor networks are of interest to the most diverse fields. Environmental monitoring, warfare, child education, surveillance, micro-surgery, and agriculture are few examples of WSN. Basically sensor networked applications is divided into four classes viz: Environmental Data Collection, Security Monitoring, Node tracking scenarios and Hybrid networks. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a difference form [2].

Although one can intercept the transmitting data but it is useless because of its unintelligible form. Only the desired receiver can retransform the data into intelligible information. As a result, sensitive communication, electronic fund transfer, electronic commerce can be realized in the Internet [1]. Key-based algorithms use an Encryption key to encrypt the message. There are two general categories for key-based Encryption: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys – a public key to encrypt the message, and a private key to decrypt it. Currently, there are several types of key based Encryption algorithms such as: DES, RSA, PGP, Elliptic curve, and others but all of these algorithms depend on high mathematical manipulations [3, 4].

II. SENSOR NETWORKS COMMUNICATION ARCHITECTURE

The sensor nodes are usually scattered in a sensor field as shown in Fig. 1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and the end users. Data are routed back to the end user by a multi hop infrastructure less architecture through the sink. The sink may communicate with the task manager node via Internet or Satellite. A sensor node is made up of four basic components as shown in Fig. 2: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units may be supported by a power scavenging unit such as solar cells. [6]

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

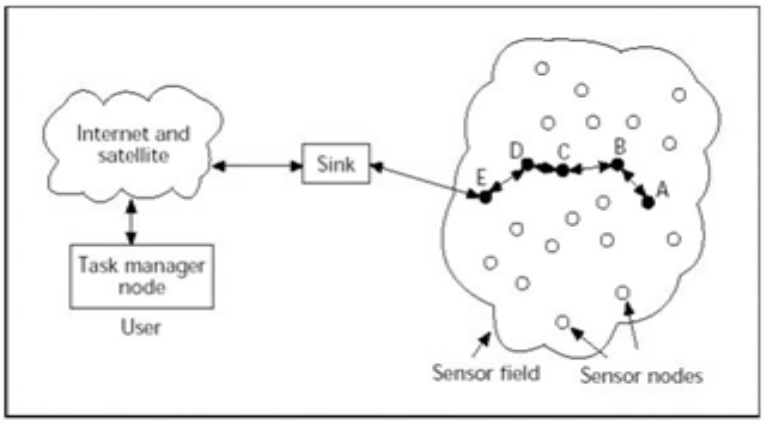


Figure 1. *Sensor nodes scattered in a sensor field.*

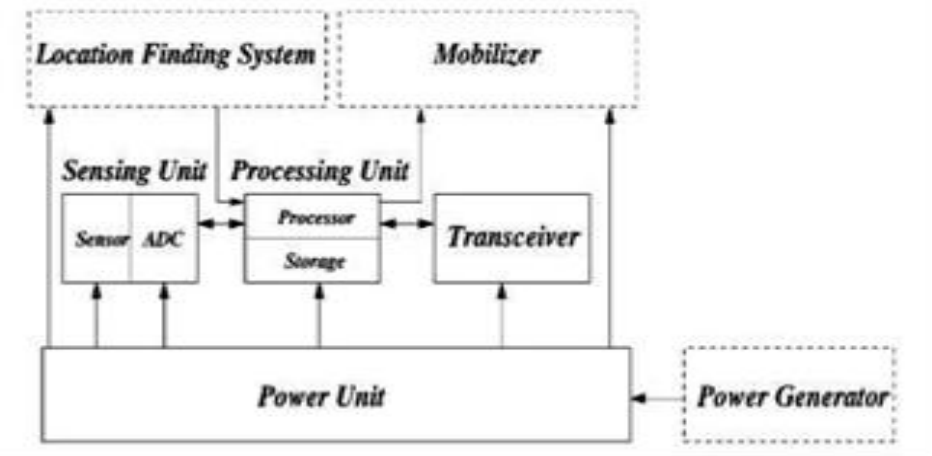


Fig 2. Components of Sensor node

III. EXISTING SENSOR NETWORK ARCHITECTURE

Most common architecture for WSN follows the OSI Model. Basically in sensor network we need five layers: application layer, transport layer, network layer, data link layer and physical layer. Added to the five layers are the three cross layers planes as shown in Fig. 3 [6]. The three cross planes or layers are; power management plane, mobility management plane and task management plane. These layers are used to manage the network and make the sensors work together in order to increase the overall efficiency of the network [6].

- Mobility management plane: detect sensor nodes movement. Node can keep track of neighbors and power levels (for power balancing).
- Task management plane: schedule the sensing tasks to a given area. Determine which nodes are off and which ones are on.

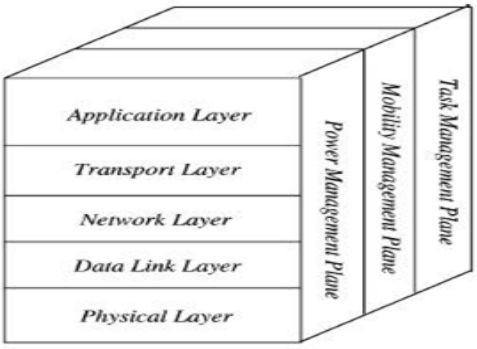


Fig 3. WSN OSI Layers

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

IV. WSN OSI LAYER AND ATTACKS

As shown in Figure 3. Of WSN OSI layers, there are five layers: Physical, Data link layer, Network layer, Transport layer and Application layer. The threats in each layer are discussed below.

A. Physical Layer

Can provide an interface to transmit a stream of bits over physical medium. Responsible for frequency selection, carrier frequency generation, signal detection, and Modulation. IEEE 802.15.4: proposed as standard for low rate personal area and WSN with low: cost, complexity, power consumption, range of communication to maximize battery life. Use CSMA/CA, support star and peer to peer topology. There are many versions of IEEE 802.15.4.

PHYSICAL LAYER THREATS:

Comparing WSNs with traditional networks, there are more threats to WSNs in the physical layer, due to the non-tamper-resistant WSN nodes and the broadcasting nature of wireless transmission. Typical types of attacks in the physical layer include physical layer jamming and the subversion of a node.

Physical layer jamming: It is a type of attack which interferes with the radio frequencies that network's nodes are using. A jamming source may randomly disturb a part of or the whole network.

Subversion of a node: If a sensor node is captured, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls.

B. Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access, and error control.

LINK LAYER THREATS

The following attacks can happen in the link layer of WSNs.

Link layer jamming: The link layer jamming attacks focus on disturbing the communication between sensor nodes around the jammer. This kind of jamming attack utilizes the weaknesses of some link layer protocols [3].

Eavesdropping: An adversary can gain access to private information by monitoring transmissions between nodes.

Collisions: An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off in certain media access control protocols.

Resource exhaustion: Denial-of-service (DoS) attack because of resource exhaustion can be caused by purposely introduced repeated collisions. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets.

Traffic analysis: The basic idea of traffic analysis attack [4] is that the nodes near to the sink forward a significantly greater volume of packets than nodes further away from the sink. By listening to the network traffic at various locations in a sensor network, an adversary is able to locate the important nodes, such as the base station.

Packet-tracing: The packet-tracing attack is a case of that an equipped adversary can tell the location of the immediate transmitter of an overheard packet. The adversary is thus able to perform hop-by-hop trace toward the original data source, causing the disclosure of the source privacy.

C. Network Layer

The major function of this layer is routing. Threats in the network layer mostly aim at disturbing data-centric and energy efficient multi-hop routing, which is the main design principle in WSNs.

Network Layer Threats

Spoofed, altered, or replayed routing information: The most direct attack against a routing protocol in any network is to target the routing information itself although it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network.

Sybil: The Sybil attack is the forging of multiple identities of a compromised node. This attack can affect fault-tolerant schemes, distributed storage, and network-topology maintenance.

Selective forwarding: A significant assumption made in multi hop networks is that all nodes in the network will accurately forward / received messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others.

Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information, creating a metaphorical sinkhole with the adversary at the center.

Wormholes: A wormhole is an attack that tunnels messages received in one part of the network over a low-latency link and replays them in a different part.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Hello flood attacks: Many protocols which use HELLO packets to announce new nodes to their neighbors, and a node receiving such a packet may assume that it is within (normal) the radio range of the sender and is therefore a neighbor.

Acknowledgment spoofing: Routing algorithms used in sensor networks sometimes rely on implicit or explicit link layer acknowledgements. An attacking node can spoof the acknowledgments of overheard packets destined for neighboring nodes to provide false information to those neighboring nodes.

Flooding: Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit.

Desynchronization: It is a case of disruption of an existing connection. An attacker may cause an end host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them instead to waste energy by attempting to recover from errors which never really existed.

D: Transport Layer

The function of this layer is to provide reliability and congestion avoidance where a lot of protocols designed to provide this function are either applied on the upstream (user to sink, ex: ESRT, STCP and DSTN), or downstream (sink to user, ex: PSFQ and GARUDA). These protocols use different mechanisms for loss detection ((ACK, NACK, and Sequence number)) and loss recovery ((End to End or Hop by Hop)) . This layer is specifically needed when a system is organized to access other networks.

TRANSPORT LAYER THREATS

SYN flooding attack: The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a –receiver or victim node, but never completes the handshake to fully open up the connection. During the attack, a malicious node sends a large amount of SYN packets to a victim/receiver node, spoofing the return addresses of the SYN packets. The victim after receiving the SYN packets from the attacker, sends them and awaits ACK packet response.. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way handshake, all the pending connections would result in overflow.

E. Application Layer Threats

Many WSNs' applications heavily rely on coordinated services such as localization, time synchronization, and in-network data processing to collaboratively process data. Unfortunately, these services represent unique vulnerabilities such as false data filtering, clock unsynchronization, and false data injections.

False data filtering:

The energy limited WSN usually use in-network data aggregation. The need for aggregation makes end-to-end cryptography infeasible. An attack on an aggregation point allows an adversary to corrupt not only all the data from the downstream nodes but also the overall data aggregation result observed at the base station. Thus, an attack can seriously hamper sensing applications by manipulating data even without having to disrupt other fundamental components in an in-network data aggregation WSN.

Clock unsynchronization:

Time synchronization is a critical building block in distributed WSN. Time unsynchronization can disrupt sleep scheduling. An attacker node can send a falsified synchronization message to its neighbor during this time exchange period. This will make other nodes calculate an incorrect phase offset and skew.

False data injections

The nature of in-network aggregation is vulnerable to false data injection. Attackers can launch an outsider attack by sending their own packets to inject data. An insider attack can also be launched by compromising several sensor nodes, and then use the compromised nodes to inject false data into the network. The Table 1, summarize the above OSI layers, it's threats and general techniques of defense.

Table 1: Typical treats in WSNs [8]

Threat	OSI Layer	Defense Technique
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Exhausting	Link	Rate limitation
Collision		Error correcting code
Route informs. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hello flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

V. PROPOSED SENSOR NODE ARCHITECTURE

As shown in Fig.4, the proposed sensor node architectures, having components such as Physical attack detector, cryptography engine, processor, data store, and transiver. The new components added in the existing sensor node architecture are Physical attack detector and the Cryptography Engine. Sensor node mostly having limited computing capability and also power. So that adding only crypt engine is feasible. For each sensor node the new components are added to enhance the security.

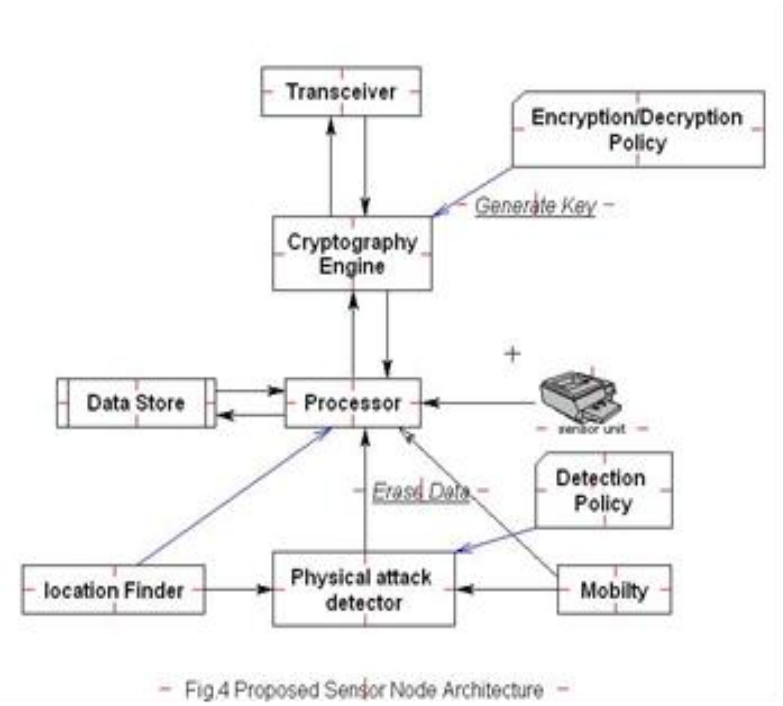


Fig.4 Proposed Sensor Node Architecture

Cryptography Engine: It is responsible to encrypt the message/data before transmit through the transceiver to the. The symmetric key algorithm can be used to encrypt or decrypt the data. Sink node having the mapping table of sensors and its encryption/decryption key.

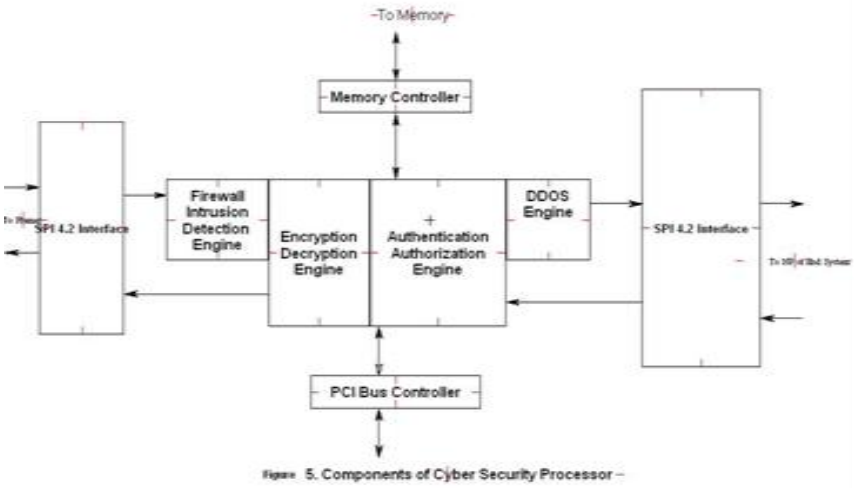
ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Physical attack detector:

This is responsible to detect the physical replacement of any device or tamper or theft of device. In such a case it will send command to processor to erase the secret data from the data store. The IEEE 1149.1 JTAG standard is designed to assist electronics engineers in testing their equipment during the development phase. Among other things, it can be used in current equipment for on-chip debugging, including single-stepping through code, and for reading and writing memory. Mostly sensor node having JTAG Test Access Port (TAP). If JTAG access is left enabled, an attacker equipped with an appropriate adapter cable and a portable computer is capable of taking complete control over the sensor node. Even if there is no JTAG connector provided on the circuit board, attackers can still get access to the JTAG ports by directly connecting to the right pins on the microcontroller which can be looked up in the datasheet.

VI. DESIGNING SINK NODE USING CYBER SECURITY PROCESSOR

Figure 5 shows the architecture of a Cyber-Security Processor (CYSEP) which can serve as a key module for enhancing security for high-speed networks/systems. The CYSEP supports, at wire-speed, four major functions, namely, firewall/ intrusion detection, encryption/decryption, message authentication, and distributed denial of service (DDoS) attack protection at the speed of 10 Gbps or higher. [9] The sink is the node that is routed to the entire network. Is responsible for receiving messages from the other nodes, storing information, and perform periodically (every 10 minutes) sending all the information to the server, where it is treated and inserted into the database. For enhancing security of Sink node, we can use the concept of CYSP. CYSP having to capabilities to protect from various threats.



5. Components of Cyber Security Processor

Figure 6 shows the proposed architecture of sink node, where the CYSP is used with the processor and memory components.

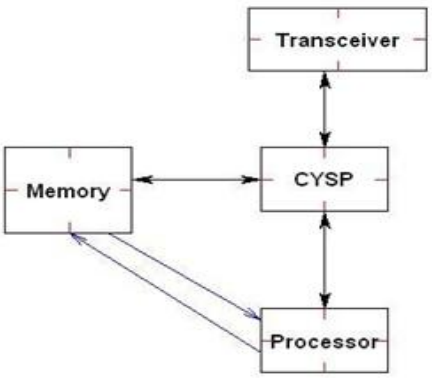


Figure 6. Block diagram of Sink Node

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

VII. CONCLUSION

This paper basically shows that we can enhance the security of WSN from the Physical threats and other threats in OSI layer using the concepts of cryptography. The concept can be used in various applications where security demand high such as military, banking, navigation etc.

REFERENCES

[1] Wireless sensor networks: Technology, protocols and applications by KAZEM SOHRABY, DANIEL MINOLI, TAIEB ZNATI, Wily publication.

[2] "Wireless sensor networks: Applications and Challenges in ubiquitous sensing" by Daniele Puccinelli and Martin Haenggi IEEE Circuits and system (1531-636X/05/©2005 (IEEE).

[3] "Security Issues in Wireless Sensor Networks" by Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz IJCS Issue 1, Volume 2, 2008.

[4] "The Data Encryption Standard (DES) and its strength against attacks". IBM Journal of Research and Development, Vol. 38, PP. 243-250. 1994.

[5] "System Architecture for Wireless Sensor" Networks by Jason Lester Hill UNIVERISY OF CALIFORNIA, BERKELEY Spring 2003.

[6] "Wireless sensor networks: a survey" by I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci I.F. Akyildiz et al. / Computer Networks 38 (2002) 393–422.

[7] "A survey on security in wireless sensor networks" by Zhang & Kitsos , Security in RFID and Sensor Networks AU6839_C014.

[8] Security Issues in Wireless Sensor Networks" by Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 1, Volume 2, 2008.

[9] CYSEP -- A CYBER-SECURITY PROCESSOR FOR 1O GBPS NETWORKS AND BEYOND" by H. Jonathan Chao, Ramesh Karri, Wing Cheong Lau MILCOM 2004 – 2004 lEEE Military Communications Conference.

[10] "Wireless Sensor Network Architecture" by Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher (CNCS 2012) IPCSIT vol.35 (2012) © (2012) IACSIT Press, Singapore.

[11] "Defense against outside attacks in wireless sensor networks" by Somanath Tripathy a, Sukumar Nandi www.sciencedirect.com, Computer Communications 31 (2008) 818–826.

[12] "Study of Security Issues in WSN" by MANJU.V.C IJEST, ISSN: 0975-5462, Vol. 3 No.10 October 2011.

[13] " A secure scheme based on three-dimension location for wireless sensor networks" by Zhang, Yu-quan ; Wei, Lei , IET International Conference on WSN- Publication Year: 2010 , Page(s): 138 – 143.

[14] " Design of WSN nodes and network performance analysis in a tea plantation" by Sun, Daozong ; Wang, Weixing ; Lu, Jianqiang ; Lin, Zuanhui , IET-WSN., Publication Year: 2010 , Page(s): 144 – 147.

AUTHOR BIOGRAPHY

Mr. Anil Hingmire. (M.E. Computer)
Designation: Assistant Professor
Vidhyavardhini's College of Engineering & Technology
Vasai (w), 401202 India
Email: anilhingmire@yahoo.com
Research Area: Artificial Intelligence, Computer Security, Database, Neural Network. Etc.