A Complete Survey on Facts and Attacks in Wireless Sensor Networks

Rashidha Begam .K[1], Savitha Devi .M[2]

[1]Research Scholar, Don Bosco College, Dharmapuri, Tamilnadu, India

[2]Assistant Professor in Department of Computer Science, PG and Research Department of Computer Science, Don Bosco College, Dharmapuri, Tamilnadu, India

Abstract: ***Wireless Sensor Networks (WSN) is an emerging technology that shows great promise for various futuristic applications. As wireless sensor networks continue to grow, for the needs of effective security mechanisms. A wireless sensor network may comprise thousands of sensor nodes. Each sensor node has a sensing capability as well as limited energy supply, compute power, memory and communication ability. Sensor nodes can be used for continuous sensing, event detection, event ID, location sensing and local control of actuators. However, realizing the full potential of wireless sensor networks poses myriad research challenges ranging from hardware and architectural issues. In this paper we analyze the security attacks in wireless sensor networks.***

Keywords: Security, attacks, distributed detection, wireless sensor networks, detection.

1. Introduction

Wireless sensor devices are employed for security applications which have several functionalities. The **first task** is the distributed detection of the presence of a target, and the estimation of parameters of interest. The target may be tracked for various purposes. The detection, estimation and tracking efforts may or may not be collaborative. The **second task** involves wireless networking to organize and carry information and the issues related to distributed detection and estimation have analyzed. Moreover, the wireless network cannot perform individual, where the wired is the basic bond to transfer the data or information through the network. Access point is the mode to transfer the data from wired to wireless and wise verse. Advances in wireless communication and electronics have enabled the development of low cost, low power, multifunctional sensor nodes. These tiny sensor nodes, consisting of sensing, data processing and communication components make it possible to deploy wireless sensor network which represent a significant improvement over traditional wired sensor network. Wireless sensor network are expected to be the solutions to many applications such as detecting and tracking the passage of troops and tanks on a battlefield, monitoring environmental pollutants, measuring traffic flows on roads and tracking the location of personnel in a building. Wireless sensor networking is addressed to a certain extent in the context of ad hoc networking. Difference between sensor network and adhoc network are the number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in adhoc network. Sensor nodes are densely deployed. Sensor nodes are prone to failures and the topology of a sensor network changes very frequently. Wireless sensor network is the lower speed compared to wired network, less secure because hacker's laptop can act as access point, if you connected to their laptop all information is retrieved.

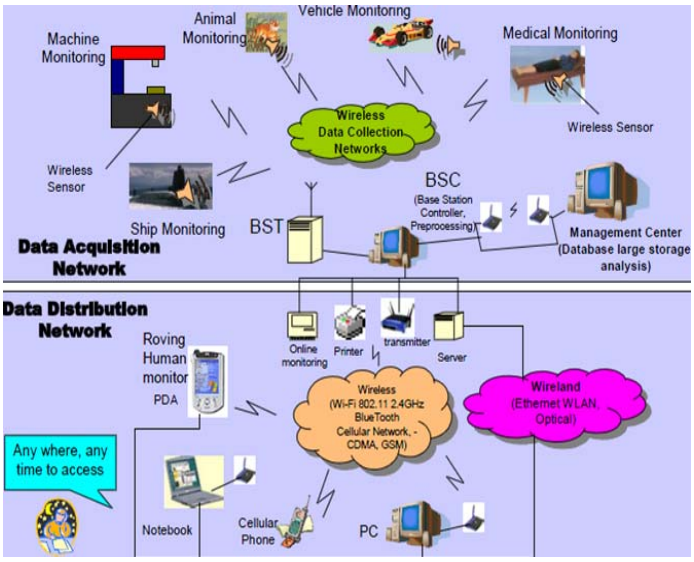

Figure 1: Architecture of WSN

2. Distributed Detection

Distributed detection of certain events or targets in the environment is an important application of sensor networks. Distributed detection suffers a performance loss caused by the local processing at sensors (mapping, quantization, etc.) as well as the noise in the communication channel. As the advances in hardware technology enabled the dense deployment of low cost sensors, the trend of the detection performance as the number of sensors goes to infinity, as measured by the error exponent, has gained much research interest. The error exponent gives an estimate of the number of sensors required to reach a certain error probability, and is therefore a useful performance index in the large sample regime.

3. Different Facts in Security

Network security system typically relies on layers of protection and consists of multiple components including networking, monitoring and security software in addition to

hardware and appliances. All components work together to increase the overall security of the computer network. The sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. To be considered sufficiently advanced along the spectrum of security, a system must adequately address identification, authentication, access control or authorization, availability, confidentiality, integrity, accountability, and non-repudiation, each of which is defined in the following sections. In network security, it is necessary to define some fundamental terms relating to that. These terms are the foundation for any discussion of network security and are the elements used to measure the security of a network.

A. Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. It is used to Identity verify and validate authentic identity of the senders and receivers. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

B. Authorization refers to the ability to control the level of access that individuals or entities can access network or system and how much information they can receive. Your level of authorization basically determines what you're allowed to do once you are authenticated and allowed access to a network, system, or some other resource such as data or information. Access control is the determination of the level of authorization to a system, network, or information (i.e., classified, secret, or top-secret).

C. Data Integrity in the context of networking refers to the overall completeness, accuracy and consistency of data. Data integrity must be imposed when sending data through a network. This can be achieved by using error checking and correction protocols. Data is exchanged without malicious alteration and it gives protection from unauthorized change. It refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network.

D. Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. To keep information private such that only authorized users can understand it.

E. Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on. The outsider cannot block legitimate access and the service has to be always available.

F. Non-repudiation The data can always be linked to its true owner to supply undeniable evidence to prove the message transmission and network access. The ability to prevent individuals or entities from denying (repudiating) that information, data, or files were sent or received or that information or files were accessed or altered, when in fact they were.

G. Data Freshness Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

H. Time Synchronization Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. In [24], the authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

I. Self-Organization A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

J. Secure Localization Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.

4. Security attacks

An attack is a specific technique used to exploit vulnerability. For example, a threat could be a denial of service. Vulnerability is in the design of the operating system, and an attack could be a "ping of death." There are two general categories of attacks, **passive and active**.

4.1 Passive Attacks

An attacker's goal in a passive attack is to obtain information about the wireless sensor network and the sensor data. It is collecting, without being discovered, and it may be internal or external in origin. They are easier to carry out in the

wireless communication than in wired because of the inherent shared nature of the wireless communication medium.

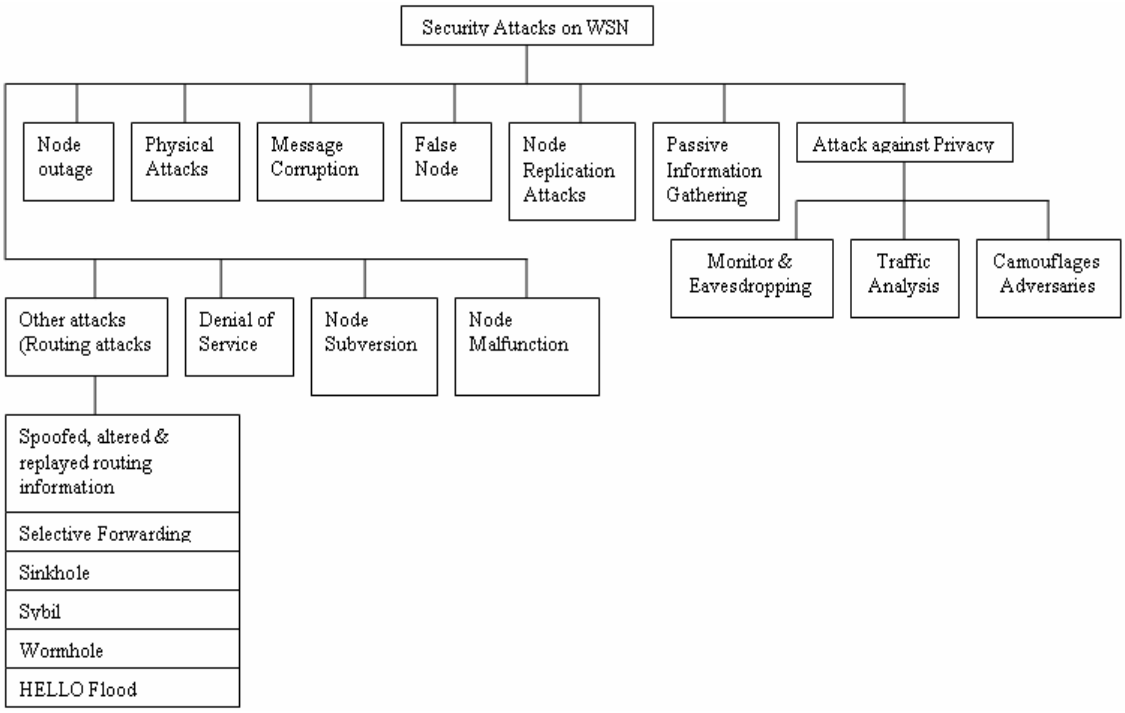

Figure 2: Security Attacks in WSN

If the attacker knows the network protocol, it can parse the messages it overhears in the same manner as an authenticated node, and can glean information from them. By continually collecting information from one or more target nodes, the attackers may obtain knowledge that can be utilized at a later time to launch an active attack. Passive attacks are very difficult to detect, because there is no overt activity that can be monitored or detected. Examples of passive attacks would be packet sniffing or traffic analysis. These types of attacks are designed to monitor and record traffic on the network. They are usually employed for gathering information that can be used later in active attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. In **a**. **Monitor and eavesdropping on transmission** is the most common attack in private. By snooping to the data, the adversary could easily discover the communication contents. Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, video conference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside. **b.** In **Traffic analysis,** when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network. And also in **c**. **Camouflage Adversaries,** one can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to strikes the packets, then misroute the packets, conducting the privacy analysis.

4.2 Active attacks

As the name implies, employ more overt actions on the network or system. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The analyzed attacks are active in nature. As a result, they can be easier to detect, but at the same time they can be much more devastating to a network. In some situations, this type of attack would be a denial-of-service attack or active probing of systems and networks.

4.2.1 Routing Attacks in Sensor Networks: The attacks which acts on the network layer are called routing attack. We have analyzed some of the attacks that happen while routing the messages.

a. Spoofed, altered and replayed routing information When a malicious node miss-present his identity, so this way it can alter the vision of sender and sender change the topology. It will create routing loops, extend or shorten service routes, and generate false error messages. And also increase end-to-end latency.
b. Selective Forwarding In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.
c. Sinkhole Attack typically work by making a compromised node look especially attractive to surrounding nodes. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node.
d. Sybil Attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number

of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased.

e. Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that he found the shortest path in the network. This tunnel between two colluding attackers is called the wormhole.

f. HELLO flood attacks an attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN.

4.2.2 Denial of Service Attacks is a type of attack is common and tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

4.2.3 Node Subversion is a capture of node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.

4.2.4 Node Malfunction will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.

4.2.5 Node Outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route.

4.2.6 Physical Attacks Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

4.2.7 Message Corruption is of any modification of the content of a message by an attacker compromises its integrity.

4.2.8 False Node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.

4.2.9 Node Replication Attacks is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

4.2.10 Passive Information Gathering An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them.

5. General Security Attacks

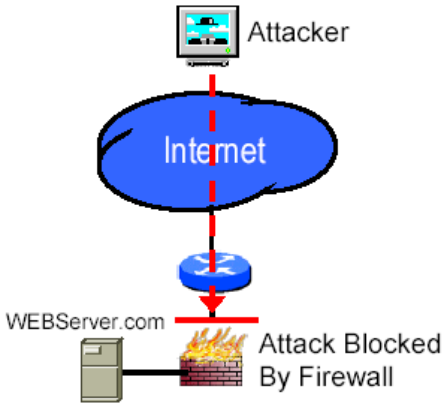

Figure 3: Firewall

Security is a fundamental component of every network design. When planning, building, and operating a network, you should understand the importance of a strong security policy. A security policy defines what people can and can't do with network components and resources.

5.1 Denial-of-service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer,

neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

5.2 Masquerade attacks may happen in a number of ways. In case of an insider attack, a masquerade attacker gains access to the account of a legitimate user either by stealing the victim's account ID and password, or by using a key logger. Another common method is by exploiting a legitimate user's laziness and trust. For example, if a legitimate user leaves the terminal or session open and logged in, a co-worker may act as a masquerade attacker.

5.3 Man-in-the-middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.

5.4 Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

5.5 Tempering and Capturing Attack is another physical attack is device-tempering attack on network; the attacker captured the sensor node physically and replaces the node with their malicious node. The effects of this attack are stopping the services or disturb the network and may control over the captured node [7]. This attack belongs to intersection, modification and fabrication security class. The availability, integrity and confidentiality are the attack threat in this class. The detection of this type of attack is through sensor node disconnection node destruction and notice misbehavior of the node in network. The defensive mechanism is optimizing and using crypto-processors and applying standard precautions in network. Further the physical protection of node and malicious node detection techniques are protect the network from these attacks.

5.6 Path Based DOS Attack is **t**he path based DOS attack is another category of physical attaches and typically combination of jamming attack. In this attack, the attacker sends a large number of packets to the base station. The effects of this physical attack are disturbing the network availability and node batteries exhaustion. The path based DOS attack is belonged to modification and fabrication class and availability and authenticity are main threats for WSN network. The nodes affected by path based DOS attack. Initially the nodes along the path will rapidly become exhausted and after this the second nodes downstream from nodes along the main path and unable to communicate with base station. This is because of tree-structured topology and in last; the path based DOS attacks can disable a much wider region than simply a single path.

6. Conclusion

Provision of security in network is a vital requirement for sufficient and stable network in communication technologies. It is a complex feature to deploy in wireless sensor network because due to the nature of network. The most physical security attacks disturb the WSN security dimensions like confidentiality, integrity, authenticity and availability. In this short review, the security issues and physical attacks analyzed. We try to focus more specific knowledge on the prevention systems to prevent the data from the attackers in our further study. The approach is to classify and compare the wireless sensor network attacks and their properties such as their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them independently and comprehensively. In future we propose to design the enhanced prevention system for wireless sensor networks.

7. Acknowledgement

The present work is benefited from the input of my research guide Mrs. M. Savitha Devi, Assistant Professor in PG and Research Department of Computer Science, Don Bosco College, Dharmapuri. I would like to thank her, for her valuable assistance to the undertaking of the study report summarized here. And also I would like to thank my management Don Bosco College, Dharmapuri, for giving me this opportunity to present the article.

References

[1] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299-302, year 2003
[2] Zia, T.; Zomaya, A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006
[3] Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
[4] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” *IEEE Commun. Surveys Tutorials*, vol. 8, pp. 2–23, year 2006.
[5] C.P. Fleeger, Security in computing, 3rd edition, *Prentice-Hall Inc*. NJ. 2003.
[6] Perrig, J Stankovic, D. Wagner, Security in wireless sensor network, *Communication of the ACM*, Vol.47, No. 6, 2004.
[7] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, year 2002.
[8] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[9] Deng, J., Han, R., & Mishra, S. (2002). Intrusion-tolerant routing in wireless sensor networks (Tech. Rep. No. CU-CS-939-02). University of Colorado, Department of Computer Science.
[10] Paolo B, Prashant P, and Vince W C, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 ZigBee standards. Computer Communications", 30(7): PP 1655-1695, 2007.
[11] C. J. C. Burges, "A tutorial on support vector machine for pattern recognition,"in Data Mining and Knowledge Discovery, vol. 2, pp. 121–167, 1998.
[12] A survey on intrusion detection approaches,Murali..A Rao.M Computer centre University of Hydrabad-India,2005-IEEE.org
[13] Network intrusion detection-Mukhergy.B,California Univrsity,Devis.CA,USAHeberlein LT;:Levitt,K.N iEEE1994-ieexplore.ieee.org
[14] www.southwestmicrowave.com
[15] csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Author Profile

Mrs. K. Rashidha Begam has completed Master of Computer Applications in Allagappa University, Karaikudi. She is doing her M.Phil Research in Network Security in Don Bosco College, Dharmapuri, Tamilnadu, India.

Mrs. M. Savitha Devi has completed M. Sc (CS)., M. Phil, MCA. She is working as Assistant Professor in Computer Science, PG and Research Department of Computer Science, Don Bosco College, Dharmapuri, Tamilnadu, India. Now she is doing her research in Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks in Mother Theresa Women's University, KodaiKanal, Tamilnadu, India.