A Comprehensive Review paper on Security Issues in Wireless Sensor Network

Hafiz Tanveer Ahmed[†], Muhammad Sheraz Arshad Malik[††], Kiran Shahzadi[†], Nida Arshad[†], Gulnaz Sabar[†], Ali Akbar[†]

[†]Department of computer science Riphah international university Faisalabad campus Pakistan
[††] Department of information and technology government college university Faisalabad

Abstract
Wireless sensor network (WSN) is one of the maximum developing technology for sensing and performing the diverse obligations. Such networks are useful in many fields, inclusive of emergencies, fitness monitoring, environmental manage, martial, businesses and those networks liable to malicious users and physical attacks due to wireless assortment of community. The extraordinarily touchy nature of collected facts makes security in these special networks a crucial concern. Wireless sensor network (WSN) are normally implemented for gathering statistics from insecure surroundings. Almost all protection protocols for wireless sensor network (WSN) consider that the intruder can obtain entirely manipulate over a sensor node by means of way of direct get physical entrance. Certainly, the improvement of powerful and proficient protection mechanisms to the ones attacks need to be addressed at every degree of the system layout and security is an essential requirement for these networks. The presence of wireless communication technology also suffers diverse forms of security threats because of without appeared installation of sensor nodes as sensor networks may also interact with sensitive information and perform in adverse without appeared surroundings. The problematic of security is because of the wireless environment of the sensor networks and restricted nature of sources at the wireless sensor nodes, which means that safety architectures used for traditional wireless networks are not feasible. Regular safety treats, intrusion detection gadget, key distribution schemes and goal localization is supplied. The determined of this paper is to research the security issues in wireless sensor networks (WSN). We perceive the security threats, overview proposed security instruments for wireless sensor networks (WSN). We also deliberate the entire view of security for certifying layered and strong security in wireless sensor networks (WSN).

Key words:
Wireless Sensor Network, Security Issues in Wireless Sensor Network, Attacks on Wireless Sensor Networks, Security Constraints & Counter Measures in Wireless Sensor Network, Holistic Security in Wireless Sensor Network

1. Introduction

Wireless sensors networks (WSNs) have developed as latest technology under the impulsion of latest technological advances in (MEMS), wireless communications and digital electronics. Sensor node is an insolent, miniature, self-organizing low cost multi useful device, prepared with battery, wireless communication, microcontroller and sensors. Sensor network is mentioned an assorted system that combines minute sensors, their actuators with some different computing elements. The assortment of application that a wireless Sensor network (WSN) may be applied to is enormous as the low strength verbal exchange devices and micro sensors are so without difficulty and with ease accessible. And wireless sensor network (WSN) includes loads to heaps of low-power multi-functioning sensor nodes, running in and without attended or antagonistic environment, with limited computational and sensing abilities. Awareness of sensor network submissions wireless ad hoc networking procedures. So, multiple spatially distributed sensors nodes collaborate and network method gathered information. They may be related to each other through quick collection wireless links, used as an infrastructure to ahead the accrued document to a licensed consumer stop over base position.

Wireless sensor network (WSN) is mostly used for accumulating software precise records from the encompassing environment, its miles highly important to protect the sensitive statistics from unauthorized get right of entry to. Wireless sensor networks (WSNs) are liable to security attacks because of the printed nature of wireless transmission. Sensor nodes will also be substantially captured or devastated through the adversaries. The usages of sensor network in several programs prominence on protected routing. Several protocols are proposed for routing and statistics amassing them are designed with protection as a goal. The source dilemma of sensor networks positions fantastic contests for protection. And sensor nodes are with very limited computing strength, it is hard to provide security in wireless sensor network (WSN) the usage of public key cryptography. Many different favoring elements of wireless sensor networks (WSNs) use are self-organizing and self-healing, having dynamic community topology to cope with node malfunctioning and disasters, mobility of organized nodes, without attended operation, potential to resist evil

Manuscript received August 5, 2018
Manuscript revised August 20, 2018

environmental circumstances. Disparate to a traditional sensor network, the deployment is done in a dense manner in the remote sensor networks, and thus a large number of sensors are used. The sensors are assigned the task of processing substantial signals, compute and self-configure the network for achieving long enduring, vigorous and accessible. The elementary idea of sensor network is to dissolve miniature sensing strategies, which are capable of sensing a few modifications of incidents/parameters and communicating with different gadgets, over a selected geographic area for some precise functions like board tracking, observation, environmental monitoring. These day's sensors can reveal temperature, strain, humidity, soil maquillage, vehicular motion, noise tiers, lighting fixtures situations, the presence or absence of certain forms of items & substances, mechanical pressure stages on attached objects, and different possessions. Conventional security issues in Wireless sensor networks (WSNs) have to contain collaborations a few of the nodes because of the decentralized nature of the networks and the absence of any infrastructure. So, researchers have centered on building a sensor trust version to clear up the problems which can be past the abilities of traditional cryptographic mechanisms. In furthermost instances, an alternate off has to be made among security and overall routine. The quantity of secure and well-organized routing protocols, secure facts aggregation protocols have been proposed by means of several researchers in wireless sensor protection (WSN). Conventional security issue in wireless sensor networks (WSNs) security ought to involve collaborations among the nodes due to the reorganized environment of the networks and the absence of any organization.

2. Related Work

The WSN is primarily based on the dense deployment of throwaway low energy, low value tiny nodes for amassing real time facts. Common capabilities of wireless sensor network (WSN) are broadcasting, multicasting and routing. These nodes consist of three primary additives recognizing, processing and communication. Numerous kinds of sensor network play a massive role in the one of a kind subject. In terrestrial wireless sensor network (WSN) nodes are dispersed and randomly or pre deliberate manner located into the goal region. The battery electricity is confined in those networks. Some other kind is secretive wireless sensor networks (WSNs), on this kind the nodes are buried underground like cave or mine for monitoring the situations. The nodes are costly on this kind evaluate to native type. The multimedia sensor network has low charge nodes and prepared with microphones and cameras. This type of network desires extra bandwidth and excessive strength and high-quality of carrier for processing the records. The underwater sensor networks are positioned underwater for accumulating the statistics and network nature is sparse. The sign fading, put off and lengthy propagation are principal issues proceeding this networks.

2.1 Security Issue in Wireless Sensor Network

An attack may be described as an attempt to advantage unauthorized get right of entry to a provider, an aid or data, or the try to compromise integrity, availability, confidentiality of a machine. Attackers, intruders or the adversaries are the originator of an assault. The weak spot in a system security design, implementation, configuration, obstacles that might be exploited by using attackers is referred to as susceptibility or defect. Any condition, together with the being of an attacker and susceptibilities with the ability to adversely affect a system through a security breach is known as threat and the prospect that an attacker will exploit a particular susceptibility, inflicting damage to a device asset is referred to as risk.

Frequently, sensor nodes are densely deployed and they have interaction with their contiguous environments very closely. They're operated without attended and additionally without the absence of any faraway monitoring machine. This is, the nodes are uncovered to the adverse environment in addition to the attackers and at a hazard of substantially being interfered. Consequently, there may be always the opportunity of taking pictures nodes substantially through the attackers to assault the wireless sensor network (WSN). Additionally, there are abundantly of security problems in wireless Sensor community that may be logically exploited via the challengers to assault the networks. Sensor nodes are factors of attack for the wireless Sensor Networks (WSNs). Adversaries can compromise or subvert sensor nodes to benefit complete manage of them and utilize them for disrupting the community. If sensor nodes are compromised, the attackers are able to recognize all of the confidential statistics saved on them and can release a ramification of malicious movements in opposition to the network through those negotiated nodes, Like, the compromised nodes may discard critical records or report with incorrect or modified records to misinform any decision that's taken based totally on this records. The overthrown nodes may also monitor the cryptographic key facts and as a result allow the attackers to compromise the entire network. Fake malicious nodes may be delivered to exhaust other sensor nodes, attract them to ship statistics simplest to it preventing the route of actual records besides the sensor nodes, attackers can goal the routing information that is used to preserve the communication among sensor nodes and the bottom station the routing mechanisms used for wireless sensor network (WSN) calls for complete agree with among all of the participating nodes. The right shipping of data within the network relies

upon at the integrity of the routing facts given via other nodes. Attacks also can be categorized into outside and inside attacks. an out of entrances attacker has no get admission to most cryptographic materials in sensor networks, whilst an interior attacker may additionally have partial key substances and the accept as true with of other sensor nodes. Interior attacks are a great deal harder to hit upon and protect against.

2.2 Few More Security Issues In Wireless Sensor Network Is

Authenticity: Is imperative in wireless sensor community (WSN), because an adversary can easily inject messages. The receiver node want to guarantee that records utilized in any decision making manner originate with relied on supply. The statistics authenticity is to ensure of identities of communique nodes. Its miles required in various administration responsibilities.

Availability: The provision in wireless sensor network (WSN) ensures the network offerings are viable even within the subsistence of denial of service attacks. The securities protocols carry out the availability of facts in the community with fixate low strength and storage with reuse of code in network. In availability, some approaches choose to regulate the code to reuse as lots code as feasible and make use of greater conversation to attain the identical intention.

Flexibility: The sensor community scenarios are extraordinary and depending on environmental situations, risks and task because they may be converting regularly. The changing undertaking desires regularly want sensors to be reduced from settle nodes within the network.

Time Synchronization: The wireless sensor network (WSN) applications depend on a few kind of synchronization. The nodes have two states inside the network on and sleep and radio may be switch on or in sleep mode for historical of time. The sensor calculates the end-to-give up postpone of a packet.

Self-organization: The wireless sensor network (WSN) has many nodes for operations & deployed in extraordinary places and fields. In self-enterprise, the nodes are flexible to be self-organizing and self-restoration in community. The wireless sensor network (WSN) is an advert hoc community and all nodes are unbiased in community & without infrastructure. This intrinsic function brings a super task for wireless network and protection.

Attacks on Wireless Sensor Networks:

Wireless sensor networks (WSNs) are susceptible to diverse styles of assaults. According to the security necessities in Wireless sensor networks (WSNs), these attacks may be categorized as:

1. **Attacks on Network Accessibility:** Attacks on availability are regularly referred to as denial-of-service (DoS) attacks. The denial-of-service (DoS) assaults can also goal any layer of a sensor community.
2. **Attacks on Secrecy and Authentication:** Popular cryptographic techniques can shield the secrecy and authenticity of communication channels from outsider attacks along with eavesdropping, packet replay attacks, and amendment or spoofing of packets.
3. **Stealthy Attacks in Opposition to Provider Integrity:** In a stealthy attack, the aim of the attacker is to make the network accept a false information value. Like, an attacker compromises a sensor node and injects a fake records value through that sensor node.
4. **Passive Attacks:** Those attacks are mainly in opposition to information confidentiality. An attacker video display unit's unencrypted traffic and looks for sensitive records that may be used in different types of attacks. Passive attacks encompass traffic analysis, tracking communications, decrypting weakly encrypted visitors, and taking authentication facts. Passive interception of network operations allows challengers to perceive imminent changes.
5. **Active Attacks:** In energetic assaults, the attacker is now not passive however takes active measures to attain manage over the community. Some examples of lively attacks are DoS, change of records, black hole, sinkhole, replay, and flooding, spoofing, jamming, weigh down, wormhole.
6. **Denial of Service attacks:** The transmission of a radio sign that interferes with the radio frequencies being utilized by the sensor network is called jamming. Jamming may come in forms, constant jamming, and intermittent jamming. Regular jamming implies the jamming of the complete community. While in the case of intermittent jamming, the sensor nodes are capable of exchange messages periodically.
7. **Outsider vs. Insider Attacks:** Outsider attacks are attacks from nodes which do now not belong to a wireless sensor network (WSN). Insider attacks occur while valid nodes of a wireless sensor network (WSN) behave in unintended or unauthorized methods.
8. **Sinkhole Attacks:** In sinkhole attacks, challenger attracts the site visitors to a negotiated node. The humblest way of creating sinkhole is to place a malicious node wherein it can attract most of the traffic, in all likelihood in the direction of the bottom station or malicious node itself deceiving as a base position.

9. **Sybil Attack:** In Sybil attack, illegal node is a part of the community we cannot save you it from taking element inside the sports of the network, but for allowing any communications the identities of the nodes it has negotiated are required. With the help of a key shared globally the attacker can pose as any node within the community, whilst nodes that don't exists. Accordingly we must have a verification of identities. Generally its miles accomplished thru the use of the public cryptographic keys, but a sensor node cannot generate and affirm digital signature.
10. **Wormhole Attack:** Is a large attack in wireless sensor network (WSN). This assault occurs on the preliminary phase when the sensors begin to find out the neighboring records. In this attack there's no need compromising a sensor inside the network. In wormhole attack, the attacker information the packets at one vicinity within the community and tunnels the ones to every other location. The tunneling or re transmitting of bits could be finished selectively. The most effective case of this attack is to have a malicious node forwarding facts among legitimate nodes. Wormholes convince distance nodes that they are acquaintances, leading to quick exhaustion in their electricity assets. An adversary located close to a base station may be capable of disrupt routing by way of developing a glowing located wormhole.
11. **Physical Attack:** A wireless sensor network (WSN) is designed in layers form and those layers shield the sensor with various attacks. The sensor networks are power constraint with a confined computational electricity, due to these traits uncovered the network for attackers. The physical attacks primarily based on altered approaches and effects.
12. **Eavesdropping Attack:** The eavesdropping is a detection of contents of communique through overhearing attempt to records and observe via wireless sensor network (WSN) transmission intermediate. The eavesdropping is likewise referred to as confidentiality and lead to wormhole or black hole assaults in network. The consequences of this assault are extracting touchy WSN data and delete the privacy and confidentiality of nodes.
13. **Signal Jamming Attack:** The signal or radio jamming attack is transmit the radio alerts emitted with the aid of the receiving antenna at the equal transmitter. The attack strategies are constant, misleading, random and reactive jamming in this attack. These attacks results on radio intervention and useful resource exhaustion. The attack is primarily based on amendment class and always the supply integrity is a major danger for wireless sensor network (WSN) in this attack.
14. **Traffic Analysis Attack:** Wireless sensor networks (WSNs) consist of many insufficient-power sensors communicating with some effective and sturdy base stations. Facts amassed with the aid of the individual nodes routed to the base station. Frequently, for an adversary to effectively render the network vain, the attacker can clearly disable the base station. Even when encrypted messages are transferred, it nonetheless leaves an excessive opportunity analysis of the communication patterns. Sensor accomplishments can potentially screen sufficient statistics to enable an adversary to purpose malicious damage to the sensor network.

In those attacks, preserving the sensor network available for its supposed use is crucial. Denial-of-provider (DoS) attacks against wireless sensor networks (WSNs) may additionally permit actual-international damage to the fitness and protection of humans. In this segment, we focus most effective on denial-of-provider (DoS) attacks and their countermeasures in sensor networks. We talk attacks on secrecy and authentication in the segment “comfy Routing Protocols,” and speak stealthy assaults and countermeasures in the segment “Intrusion Detection” below. The denial-of-carrier (DoS) attack normally refers to a challenger’s try to interrupt, subvert, or damage a community. However, a denial-of-provider (DoS) assault may be any event that diminishes or gets rid of a network’s capacity to perform its anticipated feature. Sensor networks are typically divided into layers, and this layered architecture makes wireless sensor networks (WSNs) disposed to denial-of-service (DoS) assaults, as denial-of-provider (DoS) assaults may additionally occur in any layer of a sensor network. Preceding discussions on denial-of-carrier (DoS) attacks in WSNs may be observed in. The rest of this section summarizes the feasible denial-of-provider (DoS) attacks and countermeasures in every layer of a sensor network.

Review of Security Constraints in Wireless Sensor Network (WSN):

A Wireless Sensor Network (WSN) is a special community which has many constraints as compared to a traditional laptop community. Consequently, to increase beneficial protection mechanisms whilst borrowing the ideas from the present day security techniques, it's far essential to know and recognize these constraints first.

1. **Memory and power limitations:** A sensor is a tiny device with most effective a small quantity of reminiscence and garage area for the code. Its

miles important to restriction the code length of the safety algorithm to construct a powerful security mechanism. Power is the largest constraint to wireless sensor skills. We anticipate that when sensor nodes are deployed in a sensor network, they can't be without difficulty changed or recharged due to excessive operative price.

2. **Unreliable communication:** It is one of the predominant threats to sensor security. The security of the community relies closely on a described protocol, which in turn depends on communication. The main parameters are unreliable switch, latency and conflicts.
3. **Unreliable Transfer:** Typically the packet based routing of the sensor network is connectionless and consequently inherently unreliable. Packets may additionally get damaged because of channel faults or delivered to fantastically congested nodes. The end result is lost or lacking packets. Moreover, the unreliable wireless communication channel also effects in broken packets. Better channel error fee also forces the software developer to dedicate sources to errors managing.
4. **Conflicts Even:** If the channel is consistent, the communication might also nevertheless be unreliable. This is due to the printed nature of the wireless sensor network (WSN). If packets meet in the center of transfer, conflicts will arise and the transfer itself will reject.
5. **Authentication:** In any choice making manner, the receiving nodes want to make sure that the data originates from the reliable supply. Similarly, authentication is necessary during a change of manipulate records in the network. Information authenticity is an assurance of the identities of speaking nodes.
6. **Integrity:** Data in transit may be modified via the challengers. Facts loss or damage may even occur without the presence of a malicious node due to the cruel surroundings. Information integrity guarantees that the facts is not changed in transit, either because of malicious reason or with the aid of twist of fate. Use of message integrity code is a general technique for ensuring statistics integrity.
7. **Secure Localization:** The sensor community often wishes vicinity facts appropriately and automatically. But, an attacker can without difficulty manipulate non secured region facts with the aid of reporting fake signal strengths and replaying alerts.
8. **Data confidentiality:** Programs like surveillance of facts, industrial secrets and key distribution want to depend on confidentiality. The usual method for keeping confidentiality is thru using encryption. The main hassle is that radio spectrum is an open aid and may be used by everyone geared up with right radio transceivers. An attacker can snoop on the packets transmitted within the air as long as he is able to keep path of the radio channels used inside the communication.

Counter Measures in Wireless Sensor Network:

This segment describes the countermeasures for fulfilling the security requirements and defensive the sensor network from attacks.

Defending Towards Attacks on Routing Protocols:

There is an exquisite need for both secure and energy efficient routing protocols in wireless sensor networks (WSNs) towards attacks consisting of the sinkhole, wormhole and Sybil attacks. It's discussed an intrusion tolerant routing protocol, which is designed to restriction the scope of an interloper ruining and rout facts within network intrusion. They posit using the bottom station to compute routing tables on behalf of the man or woman sensor nodes. This is achieved in 3 levels. The forwarding tables will encompass the redundancy data used for the redundant message transmission.

Attacks that can be made at the routing protocol during each of the 3 stages above are:

- Sensor node might fool the base station with the aid of sending a bogus request message.
- Compromised node may additionally encompass a bogus paths while forwarding the asked message to its mates.
- Finally, it is able to not even ahead the requested message in any respect.

Secure Multi-casting Pattern:

Proposes a directed diffusion primarily based multicast method for wireless sensor networks (WSNs) thinking about also the advantage of a logical key hierarchy. The key distribution middle is the foundation of the important thing hierarchy while person sensor nodes make up the leaves. Via utilizing this approach, they alter the logical key hierarchy to build a directed diffusion based totally logical key hierarchy. This method affords mechanisms for sensor nodes joining and leaving groups where the key hierarchy is used to effectively key all nodes in the leaving node's hierarchy.

Secure Broadcasting pattern:

Proposes a routing-aware based tree where the leaf nodes are assigned keys primarily based on all relay nodes above them. This approach takes benefit of routing records and is greater vigor efficient than mechanisms that randomly organize sensor nodes into the routing tree.

Defending in Opposition to Denial-of-Carrier Attacks:

One method in defending in opposition to the jamming assault is to perceive the wedged a part of the sensor network and effectively direction around the unavailable element. To handle jamming on the MAC layer, nodes

would possibly make use of a MAC admission manage this is price limiting. This would allow the network to disregard those requests designed to exhaust the power reserves of a node. But, it's not foolproof because the network ought to be able to deal with any legitimately huge traffic measurements.

Key Management and Protocols:

Sensor nodes may be deployed in a hostile environment; but, security will become extraordinarily vital, as they're vulnerable to variant types of malicious attacks. The open problem is the way to set up pair-sensible secret key among communicating nodes. In one of the recently offered schemes, the protection as critical as overall performance and power efficiency for many applications. Key pre dissemination is a superb concept to remedy the important thing settlement problems in wireless sensor network (WSN), but in this instance, the attacker may prominent it after conceding the node.

Secure Routing:

The primary capability of wireless sensor networks (WSNs) is to sense the surroundings and transmit the obtained statistics to base stations for further processing. For that reason, routing is an important operation in sensor networks. Some of routing protocols had been proposed for sensor networks. Conversely, preceding studies on sensor network routing become targeted very lots on efficiency and effectiveness of facts dissemination, and only a few studies taken into consideration security issues in the layout of the routing protocol.

Holistic Security in Wireless Sensor Networks:

A holistic technique aims at improving the performance of wireless sensor networks (WSNs) with respect to security, sturdiness and connectivity beneath converting environmental conditions. The holistic technique of security worries approximately involving all the layers for making sure average security in a security. Aimed at such a network, a distinct security explanation for a single layer may not be a well-organized solution instead using a holistic approach will be the best choice. Holistic security in wireless sensor network is a major research issue. Several of today's proposed security arrangements are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security appliances become well-established.

3. Analysis

In this paper represented a security issues in wireless sensor network, Wireless sensor network (WSN) is one of the maximum developing technology for sensing and performing the diverse obligations. Such networks are useful in many fields, inclusive of emergencies, fitness monitoring, environmental manage, martial, businesses and those networks liable to malicious users and physical attacks due to wireless assortment of network. Wireless sensor networks (WSNs) keep growing and end up greater common need for security in wireless sensor network (WSN) applications will develop even more. And also discussed security issues in wireless sensor network in this paper authenticity, availability flexibility, time synchronization, and self-organization. And also discussed attacks on wireless sensor networks (WSNs) are susceptible to diverse styles of attacks. According to the security necessities in Wireless sensor networks (WSNs). Also discussed about security constraints that wireless sensor network (WSN) is a special network which has many constraints as compared to a traditional laptop community. Consequently, to increase beneficial protection mechanisms whilst borrowing the ideas from the existing time security techniques. And also discussed holistic security in wireless sensor networks (WSNs) that holistic technique aims at improving the performance of wireless sensor networks (WSNs) with respect to security, strength and connectivity beneath converting environmental circumstances.

4. Conclusion

This paper discussed about security issues in wireless sensor network (WSN). Wireless sensor network (WSN) are normally implemented for gathering measurements from insecure environments. Almost all protection protocols for wireless sensor network (WSN) consider that the stalker can obtain entirely manipulate over a sensor node by means of way of direct get physical entrance. The weak spot in a system security design, implementation, configuration, obstacles that might be exploited by using attackers is referred to as susceptibility or defect. Endowment of safety in community is an important requirement for enough and stable community in communication technology. It's complicated characteristic to organize in wireless sensor network (WSN) because of the environment of network. The most physical security attacks interrupt the wireless sensor community (WSN) protection dimensions like confidentiality, integrity, the security issues and physical attacks examined. And also discussed attacks on wireless sensor Networks (WSNs) and security constraints in wireless sensor network (WSN) that is a superior network which has many constraints as compared to a traditional laptop network. So, to increase useful protection instruments whilst borrowing the ideas from the security techniques. Also discussed secure routing, the crucial capability of wireless sensor networks (WSNs) is to sense the environments and transmit the obtained statistics to base stations for additional processing. And holistic technique aims at improving the performance of wireless sensor networks (WSNs) with respect to

security, strength and connectivity +under converting environmental conditions. Wireless sensor networks (WSNs) continue to grow and come to be greater commonplace want for safety in wireless sensor network (WSN) programs will grow even in addition. We also count on that the contemporary and future work in privacy and consider will make wireless sensor networks (WSNs) a more appealing alternative in an expansion of new fields.

References

[1] M. K. Jain, "Wireless sensor networks: security issues & challenges", IJCIT, vol. 2, no. 1, (2011), pp. 62-67.

[2] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33, Jun. 2004.

[3] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53–57, Jun. 2004.

[5] Jain, M.K., 2011. Wireless sensor networks: Security issues and challenges. International Journal of Computer and Information Technology, 2(1): 62-67.

[6] Adrian Perrig,John Stankovic, and David Wagner,(2004)" Security in wireless sensor networks",Commun;ACM,4796):53-57.

[7] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002.

[8] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong – Security in Wireless Sensor Networks: Issues and Challenges – pp 1043-1048.

[9] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT, vol. 2, issue 1, pp. 62-67, 2011

[10] Kalpana Sharma. M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on Mobile Ad-hoc Networks 2010.

[11] Singla A, Sachdeva R. Review on Security Issues and Attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X , Vol.3, Issue 4, April 2013.

[12] Chowdhury M, Kader M F, Asaduzzaman. Security Issues in Wireless Sensor Networks: A Survey. International Journal of Future Generation Communication and Netwrking, ISSN: 2233-7857 IJFGCN , Vol.6, No 5 (2013), pp 97-116.

[13] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.

[14] Gilbert E P K, Kaliaperumal B, Rajsingh E B. Research Issues in Wireless Sensor Network Applications: A Survey. International Journal of Information and Electronics Engineering, Vol.2 No. 5, September 2012.

[15] T. A. Zia and A. Y. Zomaya, "Security issues in wireless sensor networks," in Proc. of the International Conference on Systems and Networks (ICSNC 06), Tahiti, French Polynesia, Nov 2- 4, 2006.