ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Security Issues and Challenges in Wireless Sensor Networks: A Survey

Rudramurthy V C[1], Dr. R Aparna[2]

[1] Assistant Professor, Dept. of Computer Science and Engineering, Global Academy of Technology, Karnataka, India

[2] Professor, Dept. of Information Science and Engineering, Siddaganga Institute of Technology, Karnataka, India

ABSTRACT: Wireless Sensor Network is a recent advanced technology of computer networks and electronics. Wireless sensor networks are used in many applications in military, ecological and health-related areas. These networks are likely to be composed of hundreds and potentially thousands of tiny sensor nodes, functioning autonomously and in many cases, without access to renewable energy resource. As wireless sensor networks edge closer towards wide-spread deployment, security issues become a central concern. Confidentiality, integrity and authentication are the most important data security concerns. When considering the network itself, need to protect fair access to communication channels and often need to conceal the physical location of our nodes. This paper describes some security issues, goals and attacks in wireless sensor networks as wireless sensor networks are more vulnerable. Several techniques are being developed by many researchers to handle these security issues are discussed.

KEYWORDS: Wireless Sensor Networks, Security, Issues, Challenges.

I. INTRODUCTION

Wireless Sensor Networks (WSN) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental condition, such as temperature, sound, vibration, pressure, motion or pollutants and to co-operatively pass their data through the network to a main location or sink where the data can be observed and analyzed. The application domains of wireless sensor networks are diverse due to the availability of micro-sensor and low-power wireless communication. These sensors are densely deployed. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust. Today's sensors are tiny, inexpensive to manufacture and don't need lot of power—an essential characteristic, since many sensors are expected to operate for long-term without access to line power. Most wireless objects get their power from batteries, but interesting new classes of devices are emerging that scavenge electricity directly from the environment. The more modern networks are bi-directional, also enabling control of sensor activity. These sensor nodes can communicate among themselves using radio signals. They will do local processing to reduce communication and consequently energy costs. The typical multi-hop wireless sensor is shown in Figure 1.

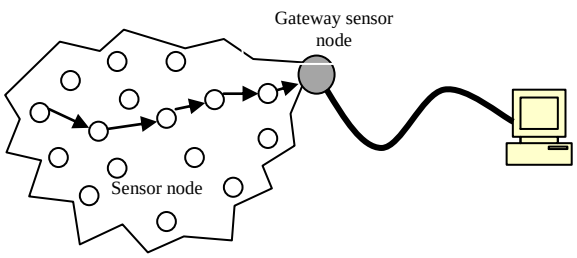

Fig 1: Typical multi-hop wireless sensor network

II. WSN ARCHITECTURE

WSN form a particular class of ad-hoc networks that operate with little or no-infrastructure. In a typical WSN we see following network components (Figure 2) [4].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

- *Sensor motes (Field devices)* – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.
- *Gateway or Access points* – A Gateway enables communication between Host application and field devices.
- *Network manager* – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames),management of the routing tables and monitoring and reporting the health of the network.
- *Security manager* – The Security Manager is responsible for the generation, storage, and management of keys.

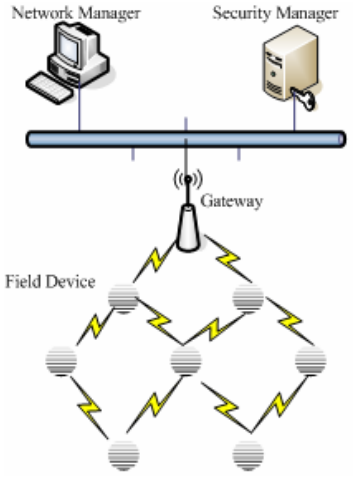

Fig 2: WSN architecture

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc.

Structure of a wireless sensor node: A sensor node is made up of four basic components [as in 8] such as sensing unit, processing unit, transceiver unit and a power unit which is shown in Figure 3. It also has additional components such as a location finding system, a power generator and a mobilizer.

Sensing units are usually composed of two subunits: sensors and Analogue to Digital Converters (ADCs). The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage 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. Power units can be supported by a power scavenging unit such as solar cells. The other subunits, of the node are application dependent.

WSN Characteristics

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting.
- Ability to cope with node failures.
- Mobility of nodes.
- Heterogeneity of nodes.
- Scalability to large scale of deployment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

- Ability to withstand harsh environmental conditions.
- Ease of use.
- Cross-layer design.

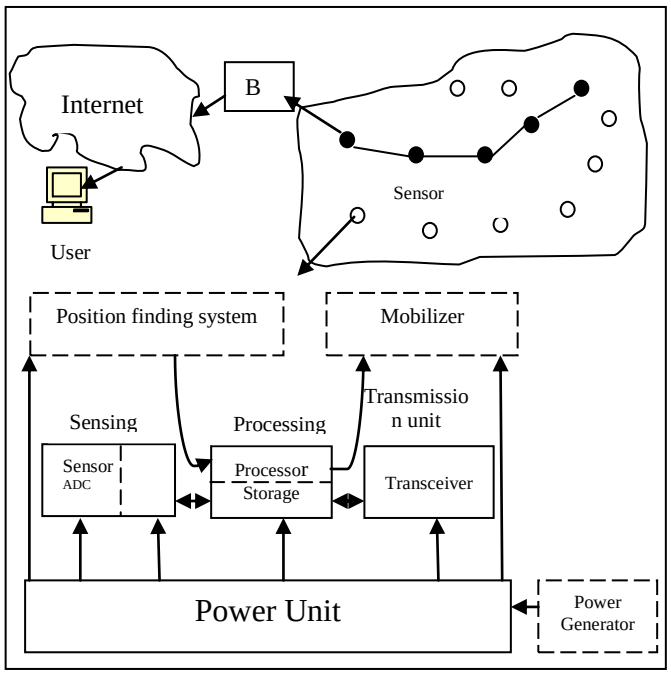

Fig 3: The components of a sensor node

III. WSN APPLICATIONS

WSN has many varied applications. Some of the applications strictly used in WSN are as follows [6]:

- Nuclear reactor control.
- Traffic monitoring.
- Fire detection.
- Contaminant Transport.
- Environmental/Habitat monitoring.
- Acoustic detection.
- Military surveillance.
- Medical monitoring.

IV. OBSTACLES IN WIRELESS SENSOR SECURITY

A wireless sensor network has many constraints compared to other networks, because of these constraints it is more difficult to directly deploy the traditional security approaches in WSNs. Individual sensor nodes in a WSN are inherently resource constrained. They have limited processing capability, storage capacity and communication bandwidth. Each of these limitations is due in part to the two greatest constraints — limited energy and physical size [7, 8, 9].

Wireless Medium: The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Very Limited Resources: All security techniques require a specific amount of resources for the implementation, including code space, data memory, and energy to power the sensor devices. However, these resources are very limited in a wireless sensor device.

The two major limitations are storage space and battery power:
1) *Limited Storage Space and Memory*: A tiny sensor device has a small amount of memory and storage space for the code. Indeed, to construct effective security techniques, it is necessary to limit the size of the security algorithm code.
2) *Power Limitation*: Once sensor nodes are deployed in a sensor network, the energy must be conserved for prolonging the life of the individual sensor node and the entire sensor network.

Exposure to Physical Attacks: The sensor may be deployed in an environment open to adversaries, bad weather and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

Managed Remotely: Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

No Central Management Point: A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient and fragile.

V. SECURITY ISSUES AND REQUIREMENTS IN WSN

When dealing with security in WSNs, we mainly focus on the problem of achieving some or all of the following security contributes or services. There are various security issues in WSN as follows [6, 8, 9, and 10].
Data Integrity: Integrity refers to the ability to confirm the message has not been tampered or changed while it was on the network.
*Data Freshness***:** Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. Line space
Data Availability: Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network.
Data Confidentiality: This ensures that a given message cannot be understood by anyone other than the desired Recipients. It is the ability to hide message from a passive attacker.
Self Organization: A wireless sensor network is 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 infra-structure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security.
Authentication: ensures that the communication from one node to another node is genuine (a malicious node cannot masquerade as a trusted network node).

VI. WSN ATTACKS

WSNs are particularly vulnerable to several types of attacks because of wireless and infrastructure-less architecture, so we can have many different types of attacks in WSN shown in figure 4[11].

Sybil Attack: the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

node using the identities of other legitimate nodes and is shown in figure 5. This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve [11].

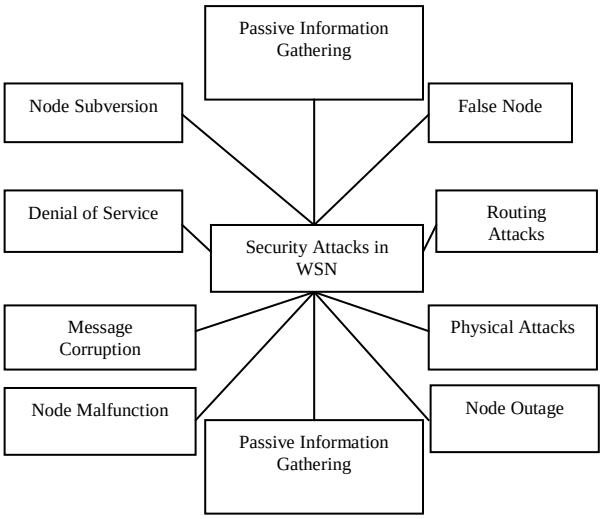

Fig 4: Types of Attacks in WSN

Worm Hole Attack: Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. This is shown in figure 6. [4].

When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighbourhood. Each neighbouring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole

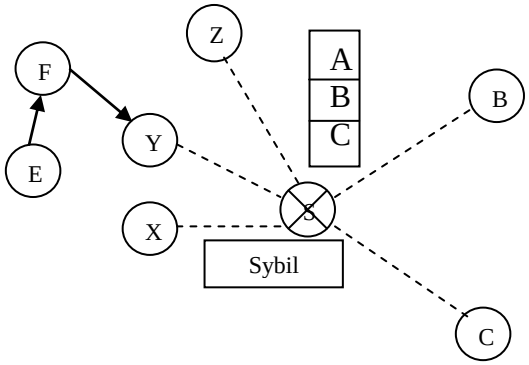

Fig 5: Sybil Attack

Node Replication Attack: Node replication attack [11] 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.

Denial of Service: The simplest Denial of Service (DoS) attack [11] 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

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, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer, this attack could be performed by malicious flooding and resynchronization.

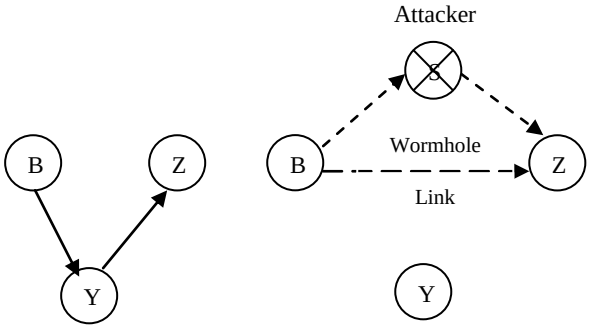

Fig 6: Worm Hole Attack

Traffic Analysis Attacks: Traffic analysis attacks [3] are forged where the base station is determinable by observation that the majority of packets are being routed to one particular node. If an adversary can compromise the base station then it can render the network useless.

Black Hole Attack: In this attack [4], a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 7 shows the conceptual view of a black hole/sinkhole attack.

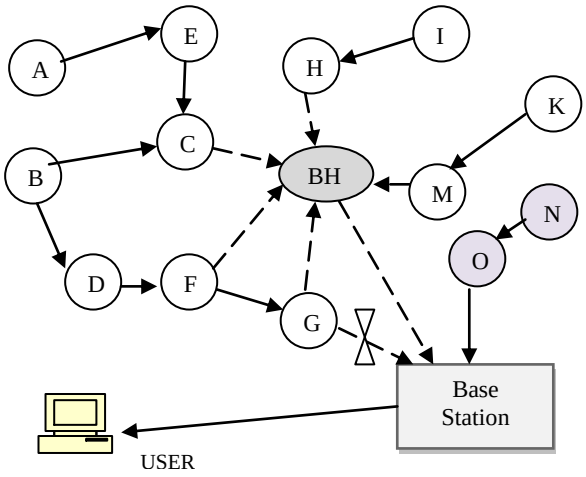

Fig 7: Black Hole Attack

Physical Attacks: Unlike many other attacks mentioned above, physical attacks [4] 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.

HELLO Flood Attack: This attack [11, 13] uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

VII. COUNTERMEASURES FOR SOME OF WSN ATTACKS

Now days, the researchers are attracted by security concepts of wireless sensor networks. Many researchers have proposed some security mechanisms in wireless sensor networks. In this section, we are dealing several security mechanisms.

HELLO Flood Attack: The simplest defense against HELLO flood attacks [3] is to verify the bi directionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol is sufficient to prevent HELLO flood attacks. Not only does it verify the bidirectional link between two nodes, but even if a well-funded adversary had a highly sensitive receiver or had wormholes to a multiple locations in the network, a trusted base station that limits the number of verified neighbors for each node will still prevent HELLO flood attacks on large segments of the network when a small number of nodes have been compromised.

Wormhole and Sinkhole attacks: Wormhole and sinkhole attacks [3, 25] are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology, because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole. When routes are established simply based on the reception of a packet as in TinyOS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify. A technique for detecting wormhole attacks is presented in [25], but it requires extremely tight time synchronization and is thus infeasible for most sensor networks. Because it is extremely difficult to retrofit existing protocols with defenses against these attacks, the best solution is to carefully design routing protocols in which wormholes and sinkholes are meaningless.

Key Establishment: One security aspect that receives a great deal of attention in wireless sensor networks is the area of key management [7]. Wireless sensor networks are unique (among other embedded wireless networks) in this aspect due to their size, mobility and computational/power constraints. Researchers envision wireless sensor networks to be orders of magnitude larger than their traditional embedded counterparts. This, coupled with the operational constraints described previously, makes secure key management an absolute necessity in most wireless sensor network designs. Because encryption and key management/establishment are so crucial to the defense of a wireless sensor network, with nearly all aspects of wireless sensor network defenses relying on solid encryption.
Defending against DoS Attacks: Since Denial of Service attacks is so common, effective defenses must be available to combat them. One strategy in defending against the classic jamming attack [7] is to identify the jammed part of the sensor network and effectively route around the unavailable portion.

Wood and Stankovic describe a two phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it. To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not fool-proof as the network must be able to handle any legitimately large traffic volumes. Overcoming rogue sensors that intentionally misroute messages can be done at the cost of redundancy. In this case, a sending node can send the message along multiple paths in an effort to increase the likelihood that the message will ultimately arrive at its destination. This has the advantage of effectively dealing with nodes that may not be malicious, but rather may have simply failed as it does not rely on a single node to route its messages.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Selective forwarding: Even in protocols completely resistant to sinkholes, wormholes and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a base station. Multipath routing can be used to counter these types of selective forwarding attacks [3, 26]. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised nodes and still offer some probabilistic protection whenever nodes are compromised. However, completely disjoint paths may be difficult to create. Braided paths [26] may have nodes in common, but have no links in common (i.e., no two consecutive nodes in common). The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

Secure Broadcasting and Multicasting: The major communication pattern of wireless sensor networks is broadcasting and multicasting [9], e.g., 1-to-Y, Y-to-1 and X-to-Y, in contrast to the traditional point-to-point communication on the Internet network. In the following subsections we describe secure multicasting and broadcasting patterns:

1) Secure Multicasting Pattern: Reference [27] proposes a directed diffusion based multicast technique for wireless sensor networks considering also the advantage of a logical key hierarchy. The key distribution center is the root of the key hierarchy while individual sensor nodes make up the leaves. By utilizing this technique, they modify the logical key hierarchy to build a directed diffusion based logical key hierarchy. This technique provides mechanisms for sensor nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node's hierarchy.

2) Secure Broadcasting Pattern: Reference [28] suggests a routing-aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. This technique takes advantage of routing information and is more energy efficient than mechanisms that arbitrarily arrange sensor nodes into the routing tree. Authors in [29] describe mechanism which takes advantage of geographic location information GPS instead of routing information. Sensor nodes are grouped into clusters with the observation that nodes within a cluster will be able to reach one another within a single hop. Indeed, by using the cluster information, a key hierarchy is constructed as in [28].

The Table I shows the some of the Security attacks and countermeasures in WSN as layered approach [1].

Table I: Security Map of Sensor Networks

Secure Data Aggregation	Attacks	Security Issues	Application Layer
Secure Localization	Denial of Services Sybil Attacks Wormhole Attacks Traffic Analysis Node Replication Physical Attacks Privacy	Data Freshness Data Integrity Data Confidentiality Self Organization Secure Localization Authorization Availability Privacy	Middleware Layer
Secure Routing			OS Layer
Crypto Algo/Analysis			Hardware Layer

VIII. CONCLUSIONS

Wireless Sensor Networks (WSN) are becoming promising future for many applications. Security in WSN is vital to the acceptance use of sensor network. Security in WSN is quite different from the traditional (wired) network security, because of the WSN characteristics, low-cost deployment and real environment orientation. So we can't able to use security methods similar to wired networks. This paper summarizes the general concepts of WSN architecture, security issues, challenges and countermeasures in WSN security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

REFERENCES

1. Kuthadi Venu Madhav, Rajendra.C and Raja Lakshmi Selvaraj, "A Study of Security Challenges In Wireless Sensor Networks," *Journal of Theoretical and Applied Information Technology*, 2005-2010.
2. Luis E. Palafox, J. Antonio Garcia-Macias, "Security In Wireless Sensor Networks," *IGI Global*, 2008.
3. Hemanta Kumar Kalita1 and Avijit Kar, "Wireless Sensor Network Security Analysis," *International Journal of Next-Generation Networks (IJNGN)*, Vol.1, No.1, December 2009.
4. Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges And Solutions," *International Journal Of Information & Computation Technology*, Volume 4, Number 8 (2014), pp. 859-868.
5. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah And Kashif Naseer Qureshi, "Security Issues And Attacks In Wireless Sensor Network," *World Applied Sciences Journal 30 (10)*: 1224-1227, 2014, Idosi Publications, 2014.
6. Divya Singla, Chander Diwaker, "Analysis Of Security Attacks In Wireless Sensor Networks," *International Journal Of Software And Web Sciences (IJSWS)*, 14-233; 2014.
7. Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges," Volume 02, Issue 01, Manuscript Code: 110746, IJCIT, 2011.
8. Yong Wang, Garhan Attebury, and Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, Volume 8, No. 2, 2nd Quarter 2006.
9. Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia, "Threat Models And Security Issues In Wireless Sensor Networks," *International Journal Of Computer Theory And Engineering*, Vol. 5, No. 5, October 2013.
10. Jyoti Shukla, Babli Kumari, "Security Threats and Defense Approaches In Wireless Sensor Networks: An Overview," *International Journal Of Application Or Innovation In Engineering & Management (IJAIEM)*, Volume 2, Issue 3, March 2013.
11. Vishal Rathod, Mrudang Mehta, "Security in Wireless Sensor Network: A Survey," *Ganpat University Journal of Engineering & Technology*, Vol.-1, Issue-1, Jan-Jun-2011.
12. Adrian Perrig, John Stankovic, David Wagner, "Security in WirelessSensor Networks," *Communications of the ACM*, Page53-57, year 2004.
13. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *AdHoc Networks (elsevier)*, Page: 299-302, year 2003.
14. Poonam Khare, Sara Ali, "Survey of Wireless Sensor Network Vulnerabilities and its Solution," *International Journal of Recent Development in Engineering and Technology*, Volume 2, Issue 6, June 2014.
15. Hiren Kumar Deva Sarma and Avijit Kar, "Security Threats in Wireless Sensor Networks," *IEEE A&E SYSTEMS MAGAZINE*, June 2008.
16. Mahfuzulhoq Chowdhury, Md Fazlul Kader and Asaduzzaman, "Security Issues in Wireless Sensor Networks: A Survey," *International Journal of Future Generation Communication and Networking* Vol.6, No.5 (2013), pp.97-116.
17. Vinod Kumar Jatav, Meenakshi Tripathi, M S Gaur and Vijay Laxmi, "Wireless Sensor Networks: Attack Models and Detection," IACSIT Hong Kong Conferences IPCSIT vol. 30, 2012.
18. Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges," Feb. 20-22, 2006 ICACT2006.
19. Xiaojiang Du and Hsiao-Hwa Chen, "Security in Wireless Sensor Networks," IEEE Wireless Communications, August 2008.
20. Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks," *International Journal of Communications*, Issue 1, Volume 2, 2008.
21. Ranjit Panigrahi, Kalpana Sharma, M.K. Ghose, "Wireless Sensor Networks –Architecture, Security Requirements, Security Threats And Itscountermeasures," Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA – 2013, pp. 107–115, 2013. CS & IT-CSCP 2013.
22. David Boyle and Thomas Newe, "Securing Wireless Sensor Networks: Security Architectures," *Journal of Networks*, Vol. 3, No. 1, January 2008.
23. Fei Hu, Jim Ziobro, Jason Tillett and Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions," Systemics, Cybernetics And Informatics Volume 1 - Number 4.
24. Dirk Westhoff, Joao Girao, Amardeo Sarma, "Security Solutions for Wireless Sensor Networks," *NEC Technical Journal*, Volume 3, 2006.
25. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.
26. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.
27. R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga, "LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks," in *First International Workshop on Wireless Security and Privacy* (WiSPr 03), 2003.
28. L. Lazos and R. Poovendran, "Secure broadcast in energy-aware wireless sensor networks," in Proc. *IEEE International Symposium on Advances in Wireless Communications (ISWC 02)*, BC Canada, 2002.
29.] L. Lazos and R. Poovendran, "Energy-Aware secure multicast communication in ad-hoc networks using geographic location information," in Proc. *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP 03)*, China, pp. 201-204, 2003.