*International Journal of Latest Trends in Engineering and Technology*
*Vol.(9)Issue(1), pp.274-277*
*DOI: http://dx.doi.org/10.21172/1.91.42*
*e-ISSN:2278-621X*

# SECURITY ASPECTS IN WIRELESS SENSOR NETWORKS

Prabha Rani[1]

**Abstract: - WSNs are mostly deployed unguarded in hostile environment which attracts an intruder for capturing a node or at least compromise it physically by shifting its code or extracting private sensitive information like cryptographic keys. By nature, wireless medium is intrinsically broadcast for communication amid nodes which makes them more prone to attacks like sniffing and spoofing, thereby totally altering operation of WSN. The main purpose is to collect environment related values which may be defeated due to existence of the attacks means to provide security to data as well as nodes. The focus is on the all security aspects issues, aims, objectives characteristics and provisions.**

**Keywords: - WSN, Sensor Nodes, Characteristics, Security Aspects, Issues, Aims, Objectives, Attacks and Security Provisions.**

## 1. INTRODUCTION

A Wireless Sensor Network (WSN) is an assemblage of sensory nodes which are distributed, autonomous, small-sized and cheap sensor nodes usually densely located in the target area with general purpose computing elements. These sensors have ability of sense data, process data and communicating with each other [1] [2]. Each node in WSN contains sub components as its processing unit (computational power and memory is limited), varied actuators or sensors (specific circuitry), a communication device (radio transceiver) and energy or power origin (battery or solar cell) to monitor the physical or environmental conditions. The sensing capability can be pressure, temperature etc. and passes data in cooperative manner through network to target point [8][14][20]. These micro-sensors can be positioned over bodies, under water, in air, in vehicles, on ground, and inside buildings etc. These sensors collect information according to their capabilities in their surroundings, and reports simultaneous to the target or remote sinks [5][9][12][15][26].

In WSNs, each sensor node has abilities of recognizing, processing as well as advancing data to the requisite target. The vital units in sensor nodes include “Sensing unit, Power unit, processing unit, Communication unit and Memory unit” for performing needed operations. Since, a sensor node operates on limited battery power resources at its disposal which ultimately affects uptime of network [2][4].

## 2. SECURITY IN WSN

Simplicity in WSN having resources controlled nodes makes them enormously susceptible to range of attacks. On-going radio transmissions can be eaves-dropped by intruders thereby injecting bits in transmission link as well as might retransmit earlier sent packets etc. Hence, a secured WSN must make provision of security properties such as “Confidentiality”, “Integrity”, “Authenticity” and “Availability” [6][7][10] [11] [16]. Intruders might position few “Malicious nodes” with alike hardware abilities similar to genuine nodes which may conspire cooperatively in attacking security of a system either by buying them discretely or by capturing few genuine nodes and "turning" them as malicious node thereby tangibly overwriting their storage memory [17] [18] [19] [20]. Similarly, in few cases, intruder may collude with nodes which are supported by superior communications links for directing their attacks. Though fiddle resilience might be a feasible defense mechanism for physically compromised nodes in few networks, still it can’t be seen as overall security solution. Enormously operative fiddle resilience has a tendency to augment per-unit cost significantly whereas sensor nodes are wished-for to be very low-cost [25] [13] [22] [27] [30].

### *2.1 Security Aims*

WSN must have following exact security aims [25] [23]:

- Front ward confidentiality: It is for thwarting a node from decryption of any forthcoming clandestine messages after it left network.
- Retrograde confidentiality: It is for thwarting an already participating node from decrypting any earlier broadcasted clandestine message.
- Persistence: It is desired for delivering a specified “Level of service” in existence of node failures and/or node attacks.
- Newness: It is to ensure that data is fresh and no intruder can replay older messages.
- Expandability: It is to support large count of nodes.

[1] Haryana Education Department, Rohtak

- Proficiency: It is to support efficiency even in presence of limitations related to processing, storage as well as communication capabilities of sensor nodes.

### *2.2 Security Issues*

It is nearly impossible to outline objectives of security services in broad-spectrum, but following facts try to give an overview of basic as well as most common issues in computer and network security [4][24]. The first part provides a definition of computer security, network security and privacy:

• Computer Security is defined as follows: “Measures that implement and assure security services in a computer system, particularly those that assure access control service.”

• Network Security is a more general term which is really complex to define. Although the definition has to be general enough to cover the large field network security is dealing with, it also has to be very detailed to fulfill the requirements of a good definition. Within this thesis, Network Security is defined as: A process to improve the properties (confidentiality, integrity, access control, availability and authentication) of a distributed IT-system as much as possible and furthermore make every operation against the security policy as hard as possible [25] [23].

• Privacy in terms of computing means that every user is the owner of his/her private data and must have the privilege to know what is stored and where it is stored and he/she should almost always be able to delete this private data. The term “private data” means data which was created by the user and also data which contains information about the user, which was sometimes even collected without its accordance (e.g. communication protocols at Internet or telephone providers) [21].

Implementing security into WSNs is a hard work by itself and it is definitely impossible to implement perfect and total security [24]. There are a lot of other issues one has to think about when designing, developing or implementing security in a network. Some of the most important security issues are stated here:

• Password Security is a basic security method in IT-systems, is simple and freely implementable. There are lot of varied easy-to-understand rules, one should respect when choosing a password, e.g. not to use your name, birth date, name of friend or family. Secure passwords should have a length of at least 8 characters and should consist of upper, lowercase and special characters; furthermore, it is recommended to change the password frequently.

• Social Engineering is the process of informing your employee and respectively every user of a single part of the whole network about the security policy and to provide methods for maintaining the policy. It should always be easier for the user to do the right thing, as it is demanded in the security policy, than to do the wrong thing, which might compromise the computer and network security.

• Data Security is depending on the value of data which is stored. The more important the stored data is, the better and more advanced data security mechanisms have to be designed, which might comprise mirroring them with the use of a RAID system, regularly backups on long time storage medias like magnet bands or strict access control and management of privileges on file layer.

• Access Security regulates the access to resources of a network from “outside”, which means that only those resources that are really needed by external users are available from outside network. All other resources have to be protected from unauthorized access, whereas this must not interfere with the availability of the system. Also bandwidth management and load sharing can be realized by the access security. Load sharing in this case means to manage the Internet access via two or more providers on the one hand and to distribute the requests to (redundant) servers equally. Computer or network security is a complex area and there have already been a lot of studies carried out in this field, but there is still no checklist-based guideline how to secure a (distributed) system.

### *2.3 Security Objectives*

The security objectives are described as follows:

• Authentication: The security mechanisms have to ensure that the parties initiating a communication are really the parties they claim to be, which means that their identities are proofed. Furthermore, it is needed to ensure that an already established connection is not interfered by a third (not authorized) party within communication. Peer entity authentication provides the confidence that no one is masquerading and/or claims to be someone else, whereas data origin authentication provides the confidence that the origin of a data is really the origin it should be or one believes it to be. Access Control should provide the availability to regulate and control the access from its own interfaces or from network to data, applications and resources on a system. Every entity that wants to get access has to be identified first and afterwards be restricted to its user-based-privileges defined in the general security policy [30].

• Data Confidentiality: It means the protection of data against a passive attack like traffic analysis. Data must not be read by someone else, except the sender and the recipient (or the group of recipients) and it should also be impossible to identify the origin or the destination of data stream.

• Data Integrity: Data sent via communication links must not be modified unnoticed in any way, regardless if the modification was done by a third (not authorized) party or even happened accidently. Data integrity should at least provide the possibility to recognize modifications of data and furthermore provide mechanisms to recover this data. A message has to be marked as “modified” irrespective if data was inserted, reordered, modified, deleted or duplicated.

• Non-Repudiation: In general, repudiation has two varied meanings: Either the recipient claims that data has never been received, although it was received correctly, or the sender claims that data has never been sent, even if message was indeed initiated by that and correctly delivered from the sender to the recipient. Security systems must prohibit repudiation for improving “Traceability of messages” in network which is especially vital in any kind of e-commerce.
• Availability: It refers to the property of a system to be accessible by an authorized entity within the specified parameters. Availability is not provided if the system is not able to fulfill authorized requests because it is overloaded with denying unauthorized request.

## 3. SECURITY PROVISIONS

In WSNs, data accuracy is indispensable as WSN are generally utilized in trust worthy situations [16] [19]. There are three prime security considerations in a WSN namely “Data integrity and data confidentiality”, “Origin validation and endorsement” and “System integrity and availability”. Provisions of security in a WSN include the following [28]:

- Precision of functionality in network
- Inoperative classic network protocols
- Restricted resources
- Un-reliable nodes
- Necessitating reliable center for managing key
- Validation of nodes
- Deterrence to attacks
- Key Institution, Confidentiality and Secrecy
- Toughness to DoS attacks
- Secured routing
- Resilient to node capturing

## 4. CONCLUSION

This paper covers the working of Wireless Sensor Networks and related aspects. WSNs are also vulnerable to countless sorts of attacks primarily owing to insecure as well as undefended nature of message link, unreliable broadcast medium, positioning in unfriendly surroundings, mechanized nature and narrow availability of resources. There is a necessity of security for sensing nodes and data transmitted by nodes and until data used by the user application. These aims, objectives and issues related to security in WSNs are focused. In the last security provisions are also discussed. Security is the one of the most important aspect of WSNs, without security all application of WSN are useless.

## 5. REFERENCES

[1]. Akyildiz I. F., W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey", Computer Networks, Vol.38, pp. 393-422 (2002).

[2]. Zheng Jun, Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, John Wiley & Sons (2009).

[3]. Neeraj Sharma, B.L. Raina, Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Attack Prevention Methods for DDoS Attacks in MANETs”, Asian Journal Of Computer Science And Information Technology, ISSN – 2249-5126,Vol 1, Issue 1, pp. 18 – 21 (2011).

[4]. Parveen Kumari, Yudhvir Singh, “Delaunay Triangulation Coverage Strategy for Wireless Sensor Networks”, Proc. of IEEE sponsored Second International Conference on Computer Communication and Informatics (2012).

[5]. Du (2008) X. Du, H., “Security in Wireless Sensor Networks”, IEEE Transactions on Wireless Communications, vol 7, issue 2.

[6]. Pooja, Manisha, Yudhvir Singh, “Security Issues and Sybil Attack in Wireless Sensor Networks”, International Journal of P2P Network Trends and Technology, ISSN: 2249-2615, Volume3, Issue1, pp7-13, 2013.

[7]. Preeti, Yogesh Chaba, Yudhvir Singh, “Review of Detection and Prevention of DDOS attack in MANET”, Proc. National Conference on Challenges & Opportunities in Information Technology (COIT –2008), India, pp. 56-59 (March 29,2008).

[8]. Krishnamachari B., D. Estrin, S. Wicker, "Impact of Data Aggregation in Wireless Sensor Networks", Proc. 22nd IEEE International Conference Distributed Computing Systems, Jul. 2002, pp. 575-578 (2002).

[9]. Du (2008), Xiang-dang, Yi-yang Li, Xiu-hua Shi, "Improved Arithmetic in Choice of Head-Note Based on Clustering of WSN," Chinese Journal of Sensors and Actuators, Volume 7, pp 1-25.

[10]. Prabha Rani, Yogesh Chaba, Yudhvir Singh, “Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Adhoc Network”, International Journal of Wireless Communication, ISSN 0974-9640, pp 885-890, August, 2011.

[11]. Walters (2007) J.P., Z. Liang, W. Shi, V. Chaudhary, “Wireless sensor network security - a survey”, Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, Vol 1, pp 367-372.

[12]. Miodrag Živković, "A Survey and Classification of Wireless Sensor Networks Simulators Based on the Domain of Use," Adhoc & Sensor Wireless Networks, Vol 20, issue 4-3, pp 245-287 (2014).

[13]. Rahul Rishi, Dheer Dhwaj Barak,Yudhvir Singh, Prabha Rani, “Mobility Analysis of Blackhole Node Attacks in Mobile Adhoc Networks”, International Conference on Recent Trends in Computing, Mechatronics and Communication, India,pp 93-97, February 25-26, 2012.

[14]. Renu Dalal, Manju Khari, Yudhvir Singh, “Survey of Trust Schemes on Ad-hoc Network”, Springer - Lecture Notes of the Institute for Computer Sciences, Social Informatics & Telecommunications Engineering (LNICST), Series 84, Springer, NETCOM-3, CCSIT-2012, pp 170-180,(2012).

[15]. Vikash Siwach, Yudhvir Singh, Seema, Dheer Dhwaj Barak, “An approach to optimize QoS routing protocol using genetic algorithm in MANET”, IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 149-53, (Sept 2012).

[16]. Su (2006) Zhong, Chuang Lin, FengYuan Ren, XiaoSu Zhan, “Security mechanisms Analysis of Wireless Sensor Networks specific Routing Attacks”, Proc. of 1st IEEE International Symposium on Pervasive Computing and Applications, pp 579-584.

[17]. Yogesh Chaba, Yudhvir Singh, Prabha Rani, “Comparison of Various Passive Distributed Denial of Service Attack in Mobile Adhoc Networks” Proc. WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication (EHAC10), Cambridge, UK (ISBN: 978-960-474-155- 7), pp 49-53 (2010)

[18]. Yogesh Chaba, Yudhvir Singh, KP Singh, Prabha Rani, “Performance Modeling of MANET Routing Protocols with Multiple Mode Wormhole Attacks”, Communications in Computer and Information Sciences, Springer [Online : Springer Digital Library] (2010) Volume 101, Part 3, pp 518-527, (2010).

[19]. Roman (2005) R., J. Zhou, and J. Lopez, “On the security of wireless sensor networks,” Proc of International Conference on Computational Science and Its Applications, vol. 3482, Lecture Notes in Computer Science, Springer Verlag, Heidelberg, Germany, pp. 681–690, D-69121.

[20]. Yogesh Chaba, Yudhvir Singh, Aarti, “Performance Analysis of Scalability and Mobility on Routing Protocols in MANETs” International Journal of IT & Knowledge Management (ISSN: 0973-4414), Vol. 1, No. 2, pp. 327-336 (July-Dec, 2008).

[21]. Acquisti (2004) A., Jens Grossklags, “Privacy attitudes and privacy behavior”, Economics of Information Security, Springer, USA, vol. 12, pp 165–178.

[22]. Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, “Wormhole Attack Avoidance Technique in Mobile Adhoc Networks”, Third IEEE International Conference on Advanced Computing & Communication Technologies, 2012.

[23]. Avancha (2005) A., "A Holistic Approach to Secure Sensor Networks," Ph. D. Thesis, University of Maryland at Baltimore County, August 2005.

[24]. Yudhvir Singh, Yogesh Chaba, Prabha Rani, “Integrating – VPN and IDS – An approach to Networks Security”, International Journal of Computer Science & Security (ISSN:1985-1533), Vol. 1, Issue 3, pp. 1-13(2007)

[25]. Wu Di, Gang Hu, Gang Ni, “Research and Improve on Secure Routing Protocols in Wireless Sensor Networks”, Proc. of 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC), pp: 853-856 (2008).

[26]. Yudhvir Singh, Amit Kumar, Prabha Rani, and Sunil Kumar Kaushik, “Impact of CBR Traffic on Routing Protocols in MANETs”, IEEE UKSim-AMSS 16th International Conference on Computer Modeling and Simulation, [Online: IEEE Xplore Digital Library], University of Cambridge, United Kingdom, 26-28, March 2014.

[27]. Yudhvir Singh, Dheer Dhwaj Barak, Vikash Siwach, Prabha Rani, “Attacks on wireless sensor networks: a survey”, IJCSMS, ISSN: 2231-5268, Vol 12, Issue 3, pp 143-148, (Sept 2012).

[28]. Zia (2008) A. T., “A Security Framework for Wireless Sensor Networks”, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.

[29]. Kizza (2008) Joseph Migga, “Implementing Security in Wireless Sensor Networks”, Data Communication and Computer Networks, pp 296-310.

[30]. Chaba (2011) Yogesh, Yudhvir Singh, Ritu Sharma, “Performance Analysis of Individual Pair-wise Cluster Key Management Scheme for Wireless Sensor Network”, International Journal of Networking and Communication Engineering, Vol 3, issue 3, pp 193-197.