www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19466-19470

Safety in Wireless Sensor Network: Types of Attacks and Solutions

Kanika Sharma[1], Dr. Nischay Bahl[2]

[1]Assistant Professor, P.G Department of Computer Science
D.A.V College, Jalandhar, India

[2]Associate Professor and Head, P.G Department of Computer Science
D.A.V College, Jalandhar, India

Abstract: ***Wireless Sensor networks (WSNs) have become the most interesting regions of exploring in the 21st century. WSNs include a large number of sensor nodes, actuator nodes, gateways, and clients. Recent progress in wireless technologies has facilitated the vast variety of uses of WSNs in the military, traffic observation, target tracking, environment monitoring, healthcare monitoring, and so on. The designers of WSNs have been faced many new challenges, like sensed quantities, the size of nodes, and nodes' autonomy. As a result, improved solutions to these confront and perfections in the modern technologies are required. The prospect expansions in sensor nodes must construct very influential and expenditure effective devices so that they may be used in applications. This paper also describes the modern research challenges for WSNs. And finally it reviews a number of security methods presently planned or implemented in WSNs.***

Key words: wireless sensor networks, Future trends, recent advances, research challenges etc.

1. Introduction

Currently, WSNs have been analyzed as one of the most significant technologies for the 21st century [1]. For Example, China has integrated WSNs in their national tactical research agendas [2]. WSNs can, in general, be described as a network of nodes that considerately sense and may direct the environment, enabling dealings between users or computers and the adjoining environment [3]. As a result, the commercialization of WSNs is increasing up and many latest technology companies are rising such as Crossbow Technology (connecting the physical world to the digital world) and Dust networks. Today, industrial computerization is one of the most imperative areas of WSN applications. WSN are being used in many engineering and civilian application areas, including industrial process monitoring and control described by Gang Zhao (2011), machine health monitoring described by Pooja Rai, Sourav Dhar, Depanjan Bhattacharjee (2015), environment and habitat monitoring, healthcare applications, home automation, and traffic control presented well by Dr. Deepti Gupta (2015) and Hadim (2006) [4]-[7].

2. Latest Trends in WSNs

Latest trends in wireless sensor technologies have facilitated a wide choice of applications of WSNs in military sensing, target tracking, environment monitoring, traffic observation (Management and Monitoring), healthcare monitoring, security and privacy concern and so on. At this point, such type of Latest Trends in WSNs and their applications in different grounds are presented by I.F. Akyildiz et al. (2002). Some of the latest trends are discussed in Table-1.

Table 1: Latest Trends in WSNs

Current Trends	Description
Smart Electricity Consumption Services	Smart electricity consumption services depend on a physically powerful power network and the concept of present organization, based on highly developed metering, high-efficiency control, high-speed communication, and fast power storage tools, real-time communication between power networks. Presently, some regional power companies of SGCC have begun to use the automatic meter reading system based on WSN technology. For example, Liaoning Province Electric Power Limited Company has approved WSN-based electric energy data acquirement system for more than 25000 households. WSNs can join the workstation tools of the sender side and the receiver side with sensors to build a complete interactive network for electric energy consumption information and understand electricity information acquirement in a difficult environment [8].
Smart Water Networks	Conventional technology systems are not typically created to monitor possible pollutants, as a result to track and manage the most difficult pollutants and also to monitor air born pollutants new sensors system need to be used. The information collected can not only be used as a key performance indicator (KPI) dashboard but

	also be used to forecast water superiority based on instant monitoring of associated events, such as artificial (manmade pollution) or environmental (climate) events [9].
Sensing of Traffic Flows	Wireless technology can be valuable in reducing consumption costs of traditional wired sensors; it does not have a direct effect on the accuracy or usefulness of the measurement results [10].
Environmental Monitoring	Environment pollution, sudden natural and ecological disasters and man-made damages are still the major environmental problems that need to be resolved at present. Early detection, alarming and initiation of emergency measures are key steps to avoid great environment disasters. Great sensing skill and large exposure of detecting area can make an instant and on all sides monitoring the environment. In WSNs, a data fusion and intelligent detection technology can increase the alarming efficiency. As a result, it is reasonable to predict that WSNs will play a vital role in the warning and forecast of the flood, forest fire and water pollution, etc.[11]
Defense	The quick use of, self-organization and fault tolerance characteristics of sensor networks construct it a very hopeful sensing technique for military C4ISRT. Critical territories, approach routes, paths and channels can be quickly sheltered with sensor networks and strongly observed for the activities of the divergent military [12].

3. Current Issues on WSNs

The key issues that change the blueprint and action of a wireless sensor network discussed in Table 2:

Table 2: Current Issues on WSNs

Current Issues	Description
Hardware and Operating System	A Sensor is a device which senses the information and transmits the same on to a mote. Sensors are used to measure the changes to pressure; humidity, sound, vibration, blood pressure, stress and heartbeat [13]. A Mote is a collection of processor, battery, Audio Digital converter, memory for connecting to a sensor and a radio transmitter for forming an ad hoc network. A Sensor and Mote collectively form a Sensor Node.
Wireless Radio Communication Features	Working of wireless sensor networks depends on the quality of wireless communication and the wireless communication in sensor networks is known for its irregular temperament. Main challenges for communication in WSNs are Low power consumption, Multi-hop networking, and Error control subsystems to detect errors [14].
Deployment	Setting up an operational sensor network in an actual world environment [14]. Sensor nodes can be deployed through placing one after another in a sensor field or through dropping it from a flat surface.
Localization	Sensor localization is a primary and critical matter for network management and process. Setting the physical location of the sensors after deployment is known as the problem of localization.
Synchronization	Time synchronization is an important service in sensor networks. In a sensor system it will help to process and analyze the data correctly and predict future system behavior [15].
Network Layer Issues	At the network layer, different techniques are founded for discovering energy efficient routes and for relaying the data from the sensor nodes to the BS so that the lifetime of a network can be optimized [16].
Security	In WSN, security is not only being positioned in front line purposes but also for inspection, building monitoring, and intruder alarms and in grim systems (airports and hospitals).

4. Security Attacks on WSNs

Many types of security attacks cause to be broadcast in Wireless sensor networks due to its very weak and susceptible signals. The security threats and attacks in wireless sensor networks are discussed in Table-3.

Table 3: Main Security Attacks on WSNs

Name	Description
Traffic analysis	Traffic analysis is the process of catching and investigating communication posts in order to presume information from patterns in communication [17].
Denial-of-service attack (DoS attack)	It is an effort to make a computer sources unavailable to its anticipated users [18]. Builders of DoS attacks normally corrupt sites or high-profile web servers such as banks, credit card payment gateways, and domain name.
Replay attack	A replay attack is a violation of protection system in which relevant data is stored without approval and then present to scam the recipient into illegal procedures such as false recognition or authentication or a replicate operations [19].
Interference and Jamming	Radio signals can be jammed or interfered with, which causes the message to be corrupted or lost. If the intruder has an influential transmitter, then it will be generated a strong signal to overpower the targeted signals and disturb communications [20]. These types of signal jamming are known as random noise and pulse.
Data forwarding phase	In the network layer, some attacks hit data packet forwarding phase. In this phase, malicious nodes do not send the data packets constantly according to the routing table. Malicious nodes simply drop data packets without any acknowledgment, change data material, hold-up forwarding real-time data packets selectively or insert garbage packets [21].
Rushing attack	Two schemed attackers use the tunnel process to make a wormhole. The tunneled packets can propagate faster if a fast transmission path and dedicated channel shared by attackers, exists between the two finishes of the wormhole, rather than a normal multi-hop route. This causes the rushing attack. These attacks can act as a valuable denial of service attack beside all currently proposed on-demand WSN routing protocols [22].
Resource Consumption Attack	In Resource consumption attack a compromised node can try to use battery life by forwarding needless packets to the fatality node [23].
Session hijacking	In the TCP session hijacking attack, the attacker take-offs the sufferer's IP address determines the correct sequence number (expected by the target) and then performs a DoS attack on the sufferer. A session hijacking over UDP is the same as over TCP, apart from that UDP attackers do not have to worry about the transparency of managing sequence numbers because it is a connectionless protocol [24].
Malicious code attacks	Malicious code (viruses, worms, spyware, and Trojan Horses) can attack both operating systems and user applications. Typically these malicious programs can spread itself through the network and cause to slow down or even damage the computer system and networks [25].
Location disclosure attack	An attacker discloses information about the position of nodes or the composition of the network such as a route map and then plans further attack scenarios [26].

5. Security Methods for the Wireless Sensor Networks

In the current era, WSN security has concerned with the interest of a number of researchers all over the world. In the matter of security, the main idea followed by the Wireless Sensor Networks is to have a fundamental approach, so as to expand the performance of the networks with respect to protection, durability, and interconnectivity under the varying ecological circumstances. Table 4 shows an amendment of various projected or implemented security methods based on the type of WSN attack [27], and their key features.

Table 4: Different Security Methods applied to Wireless Sensor Networks

Security methods	Attacks	Main features
JAM [28]	DoS attack	Point to point nodes used to stop avoidance of the jammed region.
Based on Wormhole [29]	DoS attack	Utilizes Wormholes to avoid jamming.
Random key pre-distribution, radio resource testing, etc. [30]	Sybil attack	By using radio resources, random key pre-distribution, registration procedure, verification of position, and code testing Sybil entity attacks are detecting.
Two-directional verification,	Hello flood	Two-directional verification and multiple base station routing and multi-

multi-base station routing, Multi-routing [31]	attack	routing are used. And also adopts a secret, probabilistic, sharing compartment.
Based on communication security [32]	Information or data spoofing.	Efficient use of the resources. Protects the network even if part of the network is compromised.
Pre-distribution of random key [33]	Data and Information spoofing. Attacks Information in transit.	Provides flexibility in the network protects the network, even if part of the network is compromised, provides authentication measures for sensor nodes.
REWARD [34]	Black-hole attacks	Uses geographic routing and takes advantage of being the sender to see the nearer transmission and detects black-hole attacks.
TinySec [35]	Data and Information spoofing, the messages repeat the attacks.	Centered on providing message authenticity, integrity and confidentiality messages works in the link layer.
SNEP y μTESLA [36]	Data and Information spoofing, the messages repeat the attacks.	Semantic security, Replay protection, data authentication, low communication overhead.

5. Conclusion

Wireless Sensor Network is the major field in recent trends. Major issues of WSNs are discussed in this paper, and various types of attacks are also discussed. Major attacks in network layer are Wormhole attack, Denial of Service. The attack which interrupts the routing, communication facility, and network's functioning. The choices of eligible sensor nodes are depending on their power levels and association with a number of nodes in the transmission area. Most security attacks in WSNs are caused by the insertion of false data by the compromised nodes within the network. This paper presents the requirements, the different types of security attacks.

References

[1] NI, L.M. China's national research project on wireless sensor networks. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08),

[2] BRORING, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

[3] COY, P. and GROSS, N. et al. 21 Ideas for the 21st Century. Business Week Online, 1999, pp. 78-167. http://www.businessweek.com/1999/99_35/2121_content.htm

[4] Gang Zhao, "Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey" Network Protocols and Algorithms ISSN 1943-3581 2011, Vol. 3, No. 1.

[5] Pooja Rai, Sourav Dhar, Depanjan Bhattacharjee, International Journal of Scientific & Engineering Research, Volume 6, Issue 3, March-2015 ISSN 2229-5518.

[6] Dr. Deepti Gupta, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p-ISSN: 22788735.Volume10, Issue 2, Ver.II (Mar - Apr.2015), PP 41-46.

[7] S. Hadim, N. Mohamed, "Middleware: middleware challenges and approaches for wireless sensor networks" Distributed Systems Online, IEEE Vol.7.No.3 (2006) pp 11.

[8] E. Andrey and J. Morelli, "Design of a smart meter techno-economic model for electric utilities in Ontario," in Proc. IEEE-Electric Power Energy Conf., 2010, pp. 1–7.

[9] José A. Gutierrez, Marco Naeve, Ed Callaway, Monique Bourgeois, Vinay Mitter, Bob Heile, "IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks"; IEEE Network, pp. 12-19, September/October 2001.

[10] E. Y. Luz and A. Mimbela, "Summary of vehicle detec-tion and surveillance technologies used in intelligent transportation systems," The Vehicle Detector Clearing-house, Southwest Technology Development Institute (SWTDI) at New Mexico State University (NMSU), Fall 2007. http://www.nmsu.edu/traffic/.

[11] García-Hernández, Carlos Felipe; Villanueva-Cruz, José Alonso; "Security in AODV Protocol Routing for Mobile Ad Hoc Networks", IEEE ROC&C'2005, C-03, P-11, Acapulco Gro. México, 29/November-04/December 2005.

[12] Al-Sakib khan Pathan, Hyung-Woo lee, Choong Seon Hong, "Security in Wireless Sensor Network: Issues and Challenges", ICACT,2006.

[13] Hu Lingxuan, Evans D. "Using directional antennas toprevent wormhole attacks". In Network and distributed network security symposium,2004

[14] Connectivity and Coverage in Hybrid Wireless Sensor Networks using Dynamic Random Geometric Graph Model, Author : Jasmine Norman, Vellore Institute of Technology,Vellore – 14, International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.3, September 2011.

[15] A New Graph Theory based Routing Protocol for Wireless Sensor Networks, Author : B.Baranidharan, B.Shanthi, SASTRA University, School of Computing, Thanjavur, India, International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPHHOC) Vol.3, No.4, December 2011.

[16] Chen Avin , "Random Geometric Graphs: An Algorithmic Perspective" , Ph,D dissertation, University of California , Los Angeles , 2006

[17] A.Wood and J. Stankovic. Denial of service in sensor networks. IEEE Computer, 35(10):54ñ6 2,October 2002

[18] J. Diaz D. Mitsche X. Pierez-Gimienez , "On the Connectivity of Dynamic Random GeometricGraphs, Symposium on Discrete Algorithms" , Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms , 2008, pp 601-610

[19] Josep Diaz, Dieter Mitsche, and Xavier Peirez-Gimeinez ,"Large Connectivity for Dynamic Random Geometric Graphs", IEEE Transactions On Mobile Computing, Vol. 8, No. 6, June 2009

[20] Gupta, P.; Kumar, P.R., "Critical Power for Asymptotic Connectivity in Wireless Networks", In Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming; McEneaney, W.M., Yin, G.G., Zhang, Q.,Eds.; Birkhauser Boston: Cambridge, MA, USA, 1998; 1106–1110.

[21] Hemanta Kumar Kalita and Avijit Kar. Wireless sensor network security analysis. In International Journal of Next-Generation Networks, 2009.

[22] Gupta, P., Kumar P.R, "The Capacity of Wireless Networks", IEEE Trans. Inform. Theory 2000, 46, 388 404.

[23] K. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[24] Willem Burgers. Session proxy, a prevention method for session hijacking in black-board. bachelor thesis, Institute for Computing and Information Sciences, RadboudUniversity Nijmegen, The Netherlands. Bachelors Thesis, July 2012.

[25] 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.

[26] Deng J, Han R, Mishra S: Countermeasures against traffic analysis attacks in wireless sensor networks. In Proceedings of IEEE/Create Net International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm). Athens, Greece; 2005:113.

[27] PATHAN, A. S. K. H.-W. LEE, C. S. HONG, Security in Wireless Sensor Networks: Issues and Challenges, the 8th International Conference on Advanced Communication Technology, ICACT 2006, vol. 2, 2006, pp. 1043-1048.

[28] XUAN, Y., Y. SHEN. N. P. NGUYEN, M.T. THAI, A Trigger Identification Service for Defending Reactive Jammers in WSN, IEEE Transactions on Mobile Computing, vol. 11, Issue 5, 2012, pp. 793-806.

[29] HARBIN, J., P. MITCHELL, D. PEARCE,Wireless Sensor Network Wormhole Avoidance using Reputation-based Routing, 7th International Symposium on Wireless Communication Systems (ISWCS), 2010, pp. 521-525.

[30] CHEN, S., G. YANG, S. CHEN, A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks, International Conference on Communications and Mobile Computing (CMC), Vol. 1, 2010, pp. 142-146.

[31] WANG, W., J. XU, J. WANG, Detection and Location of Malicious Nodes based on Source Coding and Multi-path Transmission in WSN, 11th IEEE International Conference on High Performance Computing and Communications, 2009, pp. 458-463.

[32] SLIJEPCEVIC, S., M. POTKONJAK, V.TSIATSIS, S. ZIMBECK, M. B.SRIVASTAVA, On Communication Security in Wireless Ad-hoc Sensor Networks, 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 10-12 June 2002, pp.139-144.

[33] DU, W., J. DENG, Y. S. HAN, P. K. VARSHNEY, A Pairwise Key Predistribution Scheme for Wireless Sensor Networks, Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003, pp. 42-51.

[34] KARAKEHAYOV, Z., Using REWARD to Detect Team Black-hole Attacks in Wireless Sensor Networks, in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

[35] KARLOF, C., N. SASTRY, D. WAGNER, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, 2º International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004, pp. 162-175.

[36] YEO, D.-G., H.-Y. YOUM, An μTESLA Protocols with Multi-senders Based on a 2-Level XOR Chain with Data-Loss, 10th International Symposium on Tolerance Applications and the Internet (SAINT), 2010, pp. 269-272.