Harkesh Sehrawat et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 8, Issue 2, June 2021, pp. 27-31

Security vulnerabilities in Wireless Sensor Networks

Harkesh Sehrawat, Vikas Siwach

Department of CSE, UIET, MDU, Rohtak
sehrawat_harkesh@yahoo.com

Abstract: **WSNs have large number of applications. For example, military and civil applications are using WSNs in various manners such as imaging of target field, detecting intrusions, monitoring weather, distributed computing, security and tactical surveillance, identifying environmental and surrounding conditions like sound, temperature, movement and light etc. WSNs have recently emerged as a technology that affects human life in various manners with its applications. WSNs are mostly deployed in hostile environment and remain unguarded. This attracts an attacker to capture or to make compromise a node physically. This can be done by modifying its code and attaining its secretive info like cryptographic keys. WSNs are more susceptible to network attacks like sniffing attack, spoofing etc. which can change the procedure of WSN and hence the very resolution of their positioning gets defeated. This paper presents an overview of different security vulnerabilities in WSN.**

Keywords: **WSN, Security, Design issue, Challenges**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of countless sensors which are self-sorted out to communicate deeds in military and non-military personnel applications, for example observation in a combat zone, location of woods fire, observation of quiet wellbeing, etc. In a WSN, sensors are thickly deployed having neighbouring sensor node quite near to each other. Thus, multi-hop correspondence in a WSN is most normally utilized than a solitary jump correspondence to devour less vitality. Every sensor node gathers information around its environment and transports information to the target node through a multi-hop network with the help of its routing capability. The open nature of WSNs makes it usually work in unattended or unfriendly conditions which effortlessly makes it prone to an assortment of assaults, for example, listening stealthily, trading-off of sensor nodes, i.e. malicious nodes and physical interruption.

WSN Architecture

There are different models for a WSNwhich are basically divided into different categories namely:

Single sink-Multi sinks WSN: A WSN can be composed in a topology in numerous sinks or a solitary sink. Sensors can send their information to the particular sink as per the topology or as per the kind of information which a sensor needs to send. A single BS (Base Station) is there to gather all the data in a single sink WSN whereas there are several BS for gathering all the data from several nodes in multi-sink WSN.

Information Centric WSN: Information driven WSN is a unique instance where no sink is accessible. Rather, the information is secured at various sensor nodes of the network.

Mobile sink-Static sink: Today sinks are portable as well as static which stays at one position. Mobile sinks have movable BS whereas BS is stationary in Static sink.

Mobile Sensors-Static Sensors: The sensors can be static, yet additionally portable. A static sensor does not move from its present position, while a portable sensor can move starting with one position to the next position.

Flat Level-Hierarchical Level: The coherent topology of a WSN can either be sorted out as a level structure or as a progressive structure. In a flat topology, all sensors are equivalent where sensor nodes send their reports through delegate sensor towards the sink where sensor nodes can directly communicate with a BS. In Hierarchical level, clustering is used whereby sensor nodes transfer their data through their respective cluster heads. These cluster heads communicate with each other for transfer of inter-cluster data transfer.

Homogeneous-Heterogeneous: All nodes in homogeneous architecture have equivalent resources i.e. they have a similar equipment stage, working framework and all utilizing similar power source thereby performing similar functions. All nodes in heterogeneous architecture have distinctive resources whereby they can gather varied sort of information.

Applications of WSNs:

The Applications of WSNs are not limited to a particular field. Some of the main applications of WSNs are listed here:

- Health care monitoring

© 2021 IJRAA All Rights Reserved

- Monitoring environments
- Medical diagnostics
- Disaster management
- Military surveillance and tracking
- Industrial automation
- Civil structural monitoring
- Traffic control
- Rapid Emergency Response

II. DESIGN ISSUES OF WSN

Various design issues for WSNs are as follows:

Operating Environment: The sensor networks can be set up anywhere in the world such as inside large machines, at the bottom of sea, in a biologically or chemically contaminated place, fitted with fast moving automobiles, in the battle field beyond the range of attacker, in our own homes or inside large buildings, in a large warehouse, tied to animals in forested area for habitat observation etc. Hence, operating environment is a very significant design factor in WSNs.

Power Consumption: Power consumption is an important factor in wireless sensor devices which are fitted at remote locations and have limited power capability used for calculation, distribution as well as routing the data. So, malfunctioning of any sensor node due to inadequate energy can cause important variations in topology of WSNs and therefore, rerouting and restructuring may be needed.

Fault Tolerance: Reliability or fault tolerance means that the failure of one or some of the sensor nodes shall not interrupt an entire WSN. It also outlines the sustaining abilities of functionalities of a WSN without any disorder due to let-down of few sensor nodes [16].

Scalability: It is a serious feature in large scale WSNs having large count of nodes which guarantees that the performance of the network will not get reduced expressively with increase in size of a WSN. The routing techniques must be scalable enough so that it can respond to events in a scaled-up WSN.

Production Costs: The costs of both initial deployment as well as cost of possession are the two crucial issues which always will determine the adoption of newer technologies in any WSN. Also, the deployment cost is significantly impacted by the size and price of every sensor node. Physical sizes also have a bearing on the ease of deployment of network whereby small size nodes can be positioned at more locations for usage in more surroundings.

Data Delivery Models: These models decide how and when to transport the collected data by a sensor node. Contingent on the nature and solicitation of the WSN, these models to the sink can be of different sorts such as event driven, continuous, query driven and hybrid. In Event-driven models, the data transfer mode is triggered only on occurrence of any event. In Continuous delivery model, several sensor nodes transport data periodically from time to time. In "Query driven" models, transport of data is initiated only after a query is made by the sink. Some WSNs applies a "hybrid model" by using a blend of all these available models.

Data Aggregation: The data aggregation function of data compression is utilized for jointly processing readings gathered from every sensor node for reducing the amount of info which is to be communicated towards the next node. However, it poses severe security glitches linked both to the fundamental network protocols where routing is done via "compromised" nodes and also to the requisite of data processing at the network itself which generally doesn't permit to concurrently realize "end-to-end" confidentiality, authenticity, etc., as data is also dealt at intermediary nodes.

Quality of Service (QoS): Data in some WSNs needs to be transported to an end point within a specified time else it would be useless. In various applications, a pre-defined latency time is a condition to stipulate such validity of data. In some other types of applications, conservation of energy of the sensor nodes has more importance than quality of data sent, so the routing protocol should consider the energy intake as well as reduce the QoS [20] for extending the lifetime of the network.

Data Latency and Overhead: These are significant features that affect the design of any routing protocol. Data Latency results due to data accumulation as well as multi-hop communication. Additionally, few routing protocols produce needless overheads for implementing their processes, which is not fit for serious energy Scarce networks.

Node Deployment: It is solicitation specific and is either deterministic or self-organizing which disrupts the performance of the routing protocol. In "deterministic" locations, the sensors are physically placed one by one whereby data is routed via pre-decided routes.

III. SECURITY REQUIREMENTS

The security necessities in a WSN embrace both the classic network necessities as well as the special desires suitable exclusively to these networks. Some of them are discussed below:

Availability: The accessibility or availability of a sensor can be lost because of higher loss of energy during processes of computation and communication whereby even a single node failure in the network can destroy the entire network.

Data Confidentiality: In most WSNs, nodes transfer very subtle information like information captured by surveillance and hence such solicitations necessitate higher level of confidentiality. The typical scheme for upholding confidentiality is the usage of encryption.

Self-Organization: Distributed WSNs have to self-establish themselves for supporting multi-hop routing. Maintaining such sort of self-association is very problematic to be accomplished in a secured mode.

© 2021 IJRAA All Rights Reserved

Data Integrity: Upholding data integrity is additional significant factor for ensuring that info is not conceded during data communication which may either be due to some malicious resolve of any node or by coincidence.

Data Freshness: Garnering the latest and fresh info is always significant for the WSNs for which efforts are to be made to ensure the novelty of every message, endorsing that recent data is received along with ensuring that no older messages can be repetitive.

Secure Localization: The usefulness of a WSN every so often is contingent upon on its capability of precisely as well as certainly discovering the location of every sensor in it. Nevertheless, an invader can easily sway non-secured place data by reporting false signal-power, repeating signals etc.

Authentication: Authentication is core prerequisite of any kind of data communiqué which can be achieved by providing appropriate proof of identity by "Confirming that principals of for whom they are claiming".

Survivability: Survivability is the competence of providing a minimum level of capability in the occurrence of power let downs or by some attacks etc.

Resilience to attacks: Several WSNs are very susceptible to insider as well as outsider attacks for which it is compulsory to withstand the network functionalities when a node or a number of nodes are compromised.

IV. CHALLENGES IN WSN

For outlining the extremely effective WSNs, it is very useful to understand its critical elements. WSNs likewise have numerous resemblances with the current specially appointed networks yet additionally have specialized contrasts with the conventional impromptu networks. The necessities and conventions of WSNs are altogether different from the customary wireless specially appointed network and impromptu calculations are not well working for these networks. Challenges between customary networks and sensor networks are recorded beneath one by one:

Limited memory and storage: Sensor nodes of WSN have a limited memory for storing information because of which security mechanisms cannot be applied. Security algorithm requires complex calculations and for their efficient running, they require high memory which is not available in sensor nodes of a WSN.

Limited power: The main issue with the nodes is consumption of energy. If nodes do not have sufficient energy, the network fails and if they have more than required energy, then also the network fails. So, power consumed must be accurate with security efficiency for longer life of the network.

Unreliability of communication: Because of the inherent nature of wireless medium, WSNs are insecure to attacks. Due to open medium communications, a WSN can be tempered by the attacker. The medium is hostile, so anybody can access the network. Packet can also be damaged in case of unreliable communication.

Deployment and immense scale: Millions of nodes are deployed over a large area where position of these nodes is not known in advance. Providing security to millions of nodes is self-challenging. Hence, strong security mechanisms are required because of the dynamics of changing environment.

Operations unattended: Due to unattended nature as well as improper infrastructure of WSN, there is no central controller for processing the operations for sensing the attacker. Security mechanism should be cooperative as well as distributed for all sensor nodes of the network.

V. ATTACKS ON WIRELESS SENSOR NETWORKS

WSNs are self-organizing networks which once positioned are expected to run alone and that too without human presence. Major attacks on sensor networks are as follow:

Physical Layer Attacks: The attacker initiates attack at the physical layer which are of two types of attacks at physical layer.

Jamming: Jamming is an attack on sensor node availability thereby tempering the transmission signal and emit radio frequency signal. It is unwanted, so it differs from radio propagation. There are different types of jammers such as "Constant jammer, Deceptive jammer, Random jammer, Reactive jammer" etc.

Tampering: In this attack, the attacker captures a node and makes it malicious thereby completely destroying and modifying the nodes.

Data Link Layer Attack*:* These are the attacks which take place at the second layer and include collision and exhaustion.

Collision: Here, a single bit error can cause total retransmission of data. If attacker can generate collisions in transmission, then it can destroy the entire packet.

Exhaustion: If an attacker reduces the energy of a node in WSN by sending unwanted info using malicious nodes again and again, then it causes exhaustion of the battery as well as total network failure.

Network Layer Attacks: These are the attacks which take place at the third layer i.e. network layer which are as follows:

Hello flood attacks: In this attack, the attacker impersonates as neighbour in the sensor network by sending high transmission power signals and replays hello packets. It disrupts routing protocols and instantiated other types of attack.

Wormhole attack: Since, intruders here are tactically placed at ends of the network, so these are difficult to prevent and detect. They receive information and send back this information to different nodes via a tunnel.

© 2021 IJRAA All Rights Reserved

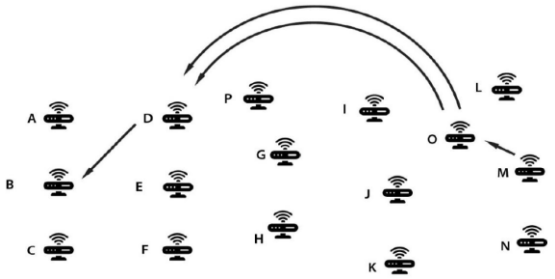

Fig 1: Wormhole Attack

Sybil attack: Here, Intruder can make usage of identities of others nodes in order to capture necessary information. Topology maintenance, fault tolerance is attacked by Sybil attack.

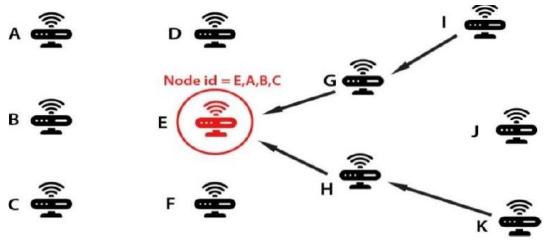

Fig2: Sybil attack

Sinkhole attack: It is an insider attack where the goal of a malicious node is to attract whole network traffic towards itself so that the BS cannot acquire complete information of the data packet. Then, it purposely changes the data content or completely destroys it.

Selective forwarding: In this attack, compromised nodes may decline to pass on some messages and will straightforwardly drop them.

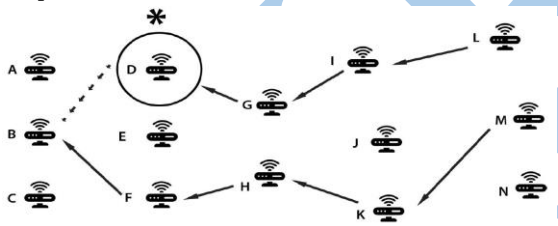

Fig 3: Selective Forwarding Attack

Blackhole attack: Its only goal is to pass nothing and then making a black hole in the network.

Transport Layer Attack: The attacker initiates attack in the transport layer for e.g. Flooding attack.

Flooding attack: This attack is introduced to bring down a WSN by flooding it with large amount of traffic so that memory buffers are flooded and no connections can be made further. It is a DoS attack.

Application Layer Attack:

Denial of Service attack (DoS): It consumes the resources thereby physically destroying the network. It is an intended attack which limits the functionality of a WSN.

Cloning attack: The attacker drops unlimited number of clones of malicious node in the WSN thereby causing a bundle of damage to the network.

VI. CONCLUSION

This paper contributes brief overview of the WSNs, its architecture, security requirements and routing attacks in WSN.

REFERENCES

[1]. F. L. Lewis, Wireless Sensor Networks, vol. 2. New York: John Wiley & Sons, 2004.

[2]. C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," Sensors, vol. 9, no. 9, pp. 6869–6896, 2009.

[3]. A. Shaikh and S. Pathan, "Research on Wireless Sensor Network Technology," Int. J. Inf. Educ. Technol., vol. 2, no. 5, pp. 476–479, 2012.

[4]. A. G. Dinker and V. Sharma, "Attacks and challenges in wireless sensor networks," in Proceedings of the 10th INDIACom; 3rd International Conference on Computing for Sustainable Global Development, 2016, pp. 3069–3074.

[5]. A. Tayebi, S. Berber, and A. Swain, "Wireless Sensor Network Attacks: An Overview and Critical Analysis," in Seventh International Conference on Sensing Technology, 2013, pp. 97–102.

[6]. M. Bhende, S. J. Wagh, and A. Utpat, "A Quick Survey on Wireless Sensor Networks," in Fourth International Conference on Communication Systems and Network Technologies, 2014, pp. 160–167.

[7]. G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," Int. J. Comput. Sci. Inf. Secur., vol. 4, no. 1, pp. 1–9, 2009.

[8]. G. Singh, E. Sandeep, and K. Dhanda, "Performance Analysis of Security Schemes in Wireless Sensor Network," Int. J. Adv. Res. Comput. Commun. Eng., vol. 2, no. 8, pp. 3217–3223, 2013.

[9]. M. Islam and S. AshiqurRahman, "Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches," Int. J. Adv. Sci. Technol., vol. 36, pp. 1–8, 2011.

[10]. T. Kavitha and D. Sridharan, "Security Vulnerabilities In Wireless Sensor Networks : A Survey," J. Inf. Assur. Secur., vol. 5, pp. 31–44, 2010.

[11]. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

[12]. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," ACM SIGOPS Oper. Syst. Rev., vol. 34, no. 5, pp. 93–104, 2000.

© 2021 IJRAA All Rights Reserved

[13]. I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, “Wireless Sensor Network Virtualization: Early Architecture and Research Perspectives,” IEEE Netw., vol. 29, no. 3, pp. 104–112, 2015.

[14]. H. Jadidoleslamy, “A Hierarchical Intrusion Detection Architecture for Wireless Sensor Networks,” Int. J. Netw. Secur. Its Appl., vol. 3, no. 5, pp. 131–154, 2011.

[15]. Karakaya, Aykut, and Sedat Akleylek. "A survey on security threats and authentication approaches in wireless sensor networks." *2018 6th international symposium on digital forensic and security (ISDFS)*. IEEE, 2018.

[16]. Seth B., Dalal S., Kumar R. (2019) Securing Bioinformatics Cloud for Big Data: Budding Buzzword or a Glance of the Future. In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence, vol 823. Springer, Cham. https://doi.org/10.1007/978-3-030-12500-4_8

[17]. Bhushan, Bharat, and Gadadhar Sahoo. "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective." *Handbook of computer networks and cyber security*. Springer, Cham, 2020. 683-713.

[18]. Burhanuddin, M. A., et al. "A review on security challenges and features in wireless sensor networks: IoT perspective." *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 10.1-7 (2018): 17-21.

[19]. Sinha, Preeti, et al. "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey." *2017 International Conference on Signal Processing and Communication (ICSPC)*. IEEE, 2017.

[20]. Seth B., Dalal S. (2018) Analytical Assessment of Security Mechanisms of Cloud Environment. In: Saeed K., Chaki N., Pati B., Bakshi S., Mohapatra D. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 563. Springer, Singapore. https://doi.org/10.1007/978-981-10-6872-0_20

IJRAA

© 2021 IJRAA All Rights Reserved