International Journal of Security Technology for Smart Device
Vol. 6, No. 1 (2019), pp.9-16
http://dx.doi.org/10.21742/ijstsd.2019.6.1.02

A Detailed Review about Attacks on WSNs

N. Thirupathi Rao[1], Debnath Bhattacharyya[2]

[1,2]Department of Computer Science and Engineering
Vignan's Institute of Information Technology (A)
Visakhapatnam, AP, India,
[1]nakkathiru@gmail.com,[2]debnathb@gmail.com

Abstract

Remote sensor systems have an arrangement of calculations and conventions with self-building up abilities. The current sensors or the sensors used in these sensor networks will work wirelessly by locating at various locations of the actual requirement. The major advantage of these sensor networks are that these network nodes can be placed at various locations where it will be more difficult for the human beings or persons to enter and collect data. In such dangerous places also these nodes can be placed and can collect the data from time to time. As a result of such important facilities, the utilization such node sin these networks are becoming very high and the usage of such networks had grown a lot. In these current days, the networks which were built with the combination of such nodes and networks are built and the attackers always are ready to tap or attack such networks and hack the data. Once the data had collected and can be used for various other benefits and the actual user or the network established person or the company had to lose the data and also can be used such important data for various other anti social issues. Hence, the attacks on these nodes and networks can be treated seriously and can be considered with various preventive measures. In the current paper an attempt has been made to present some important points and issues to be noted for the establishment and working of the network. Different assaults are performed in this system, for example, inactive and dynamic assaults or insider and outcast assaults. The remotely arrange required continuously security as information respectability, secrecy, legitimacy and so forth.

Keywords: *Security, networks, sensors, attacks, cyber threats, physical attacks on nodes, nodes, issues.*

1. Introduction

In recent days or research on sensor networks or the wireless sensor networks, the big challenge in research area or the research topic was to establish a wireless sensor network that was less vulnerable to attacks[1]. The major role or the major part of these networks is the sensors that collect the data from various sources and the same will be transferred to the networks for further processing of such data. Several forma of the data will be collected from these sensor nodes placed at various locations. Some sorts of such data are like the temperature, humidity, heat, pressure, light. The basic function or the source that was being generated from these sensors is the electrical signal or an electrical pulse that can be suited for the better functioning of the networks [1][2][3].

Article history:
Received (April 17, 2019), Review Result (June 25, 2019), Accepted (August 9, 2019)

Print ISSN: 2205-8451, eISSN: 2207-4244 IJSTSD

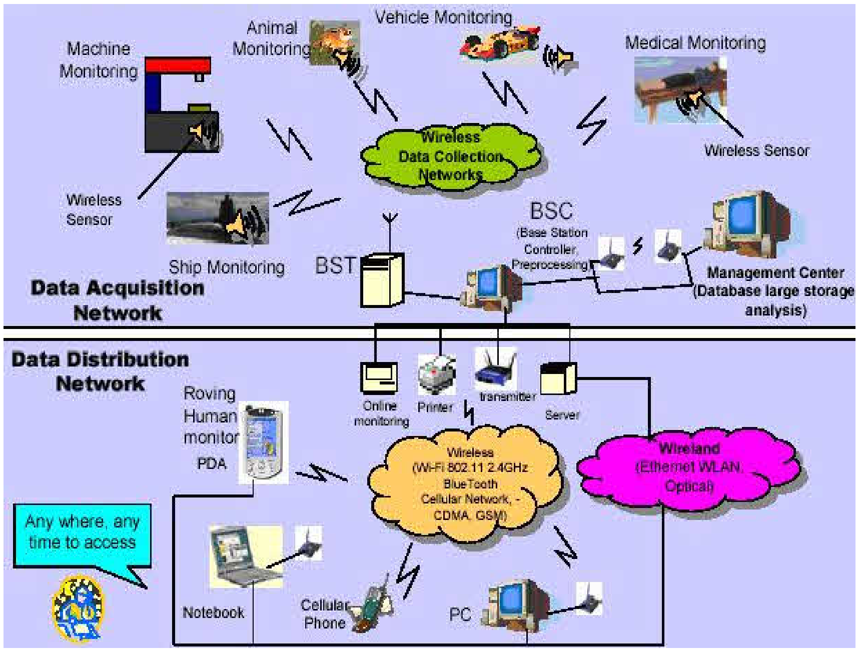
Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC
(Base Station Controller, Preprocessing)
Management Center (Database large storage analysis)
Data Acquisition Network
Data Distribution Network
Online monitoring
Printer
transmitter
Server
Roving Human monitor
PDA
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

Figure 1. A Sensor network model example [1]

Various types of topologies are used to build these sensor networks for the functioning of the real time scenarios. Some of them are like the Star topology, Tree topology and mesh topology. Out of other various scenarios, these three topologies are mainly used for the building of these wireless sensor networks[1]. The main advantage of star topology was that all the nodes in the network are connected directly with the gateway of the network such that easy to transfer and easy to process even though there s a break in the network chain. The other important topology was the tree topology in which all the nodes in the network model are connected with the next upper nodes such that dependency will be there only on the upper node and data can be transferred easily. The other important topology was the mesh topology. In the current topology, the nodes to which the data needs to be transferred should be in the range of the transmission such that the data can be transferred easily and also for the better flow of data to the other nodes in the network. Rely on the utilization and the sort of sensors used; actuators might join in the sensors[2].

Based on various conditions and environmental issues, these network models are classified into the following models and explained as follows,

Mobile WSNs
Underwater WSNs
Multimedia WSNs
Terrestrial WSNs

The applications of these sensor networks are as figure 2.

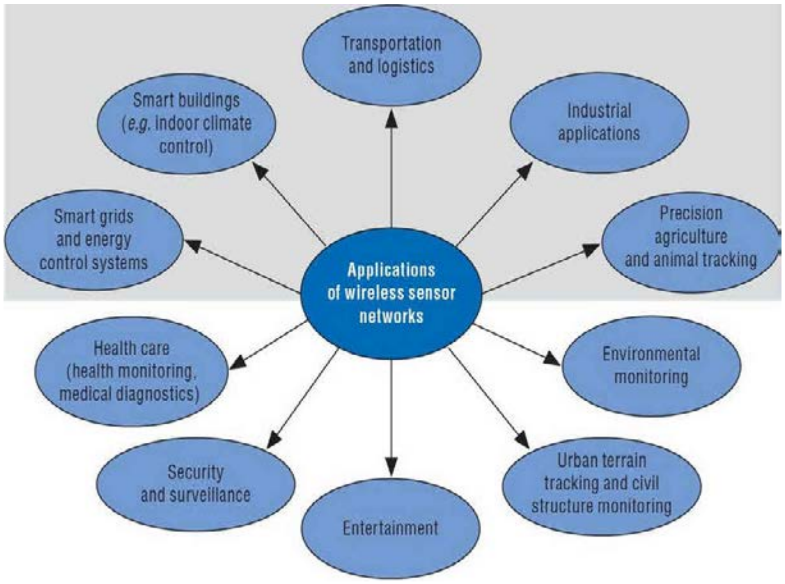
Transportation and logistics
Smart buildings (*e.g.* indoor climate control)
Industrial applications
Smart grids and energy control systems
Applications of wireless sensor networks
Precision agriculture and animal tracking
Health care (health monitoring, medical diagnostics)
Environmental monitoring
Security and surveillance
Entertainment
Urban terrain tracking and civil structure monitoring

Figure 2. Applications of wireless sensor networks [1]

1.1 MOBILE WSNs

This type network models consists of various sensors and all those sensors are fixed at various locations for the collection of data and also for the transfer of data. These networks are mostly used for wireless mobiles and their usage[1]. These networks can be useful further for the better processing and better understanding of transfer of data from various locations to other locations. The transfer of data includes form villages to villages, cities to cities and countries to countries and continents to continents.

1.2 UNDERWATER WSNs

The most interesting and important point or the issue to be considered was that the almost 70% of the earth was covered with water[1][2]. These sorts of sensor networks are placed under water that means a number of sensor nodes are placed under water and communication can be started without any interruption much. The nodes can be deployed in under water at various locations to collect the data from various sources by the autonomous under water vehicles.

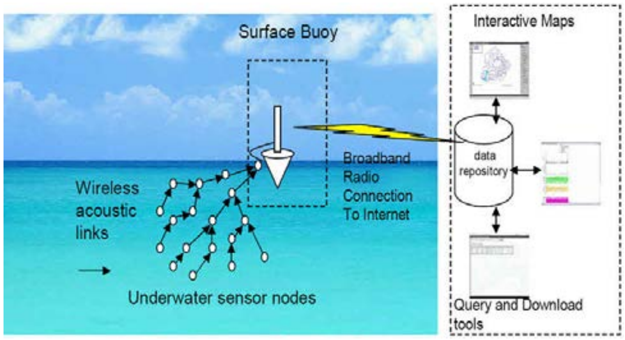

Figure 3. Under water sensor network model example[1]

These vehicles can move under water and cannot be traced by anyone mostly secretly. The data can be gathered secretly and can be used for various sorts of applications [3]. The most considered or important point to be discussed was that the power backup of such nodes which were deployed under water. If the sunlight was reached to such sensors, they can recharge if it's not the only problem was to provide power backup. This point was the important point consideration for research now days for further development of this area of research.

1.3 MULTIMEDIA WSNs

The main motto or the application of using these sorts of sensor networks is to provide a vast number of information by collecting from various sensors placed at various events. The data collected from these sorts of networks are like the images, movies and small bytes of data [12,13]. These networks consists of sensor nodes which can work very easily and can also consume very less power for further processing of such huge data and collection of sources.

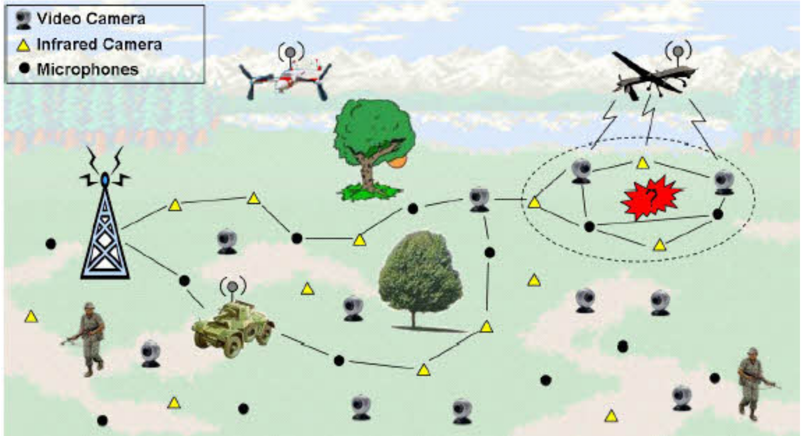

Figure 4. Multimedia network applications example[1]

The main challenge for the working of these network models are the applications process through internet. For sending and receiving such huge amounts of data and also sometimes the data should be transmitted live, it requires a huge amount of internet data and faster internet connectivity is required.

1.4 TERRESTRIAL WSNs

These sorts of wireless sensor networks are capable of communicating data to various nodes in the upper territory. The data can be transmitted to various stations located at various locations in the form of territories [11][13][14]. The data cab transferred easily as very few connections or the very few nodes are sometimes requiring in some small set of cases. The networks may be of nodes that may have some other problems also. Some of them are the power problems of the nodes in the networks. The appropriate time processing or supplying of data to such network models is always a critical problem. Hence such important issue sot be dealt very seriously and can also be dealt with more care in real time situations.

2. LITERATURE SURVEY

Xiaoliang Meng et al. [2016] in the strategy of choosing the multi-bounce hubs in the WSN, it is noteworthy to choose the rear ideal sending hub to rely upon a specific run the show. Ideal choosing component rely upon topographical area data is a convention which abuses separations and points, as the criteria of steering decision. TBF convention presents directing bundles along a predefined scatters hubs course slightly[8].

Hacène Fouchal et al. [2016] had a circulated arrangement ready to guarantee validation of hubs whenever without having any online access to an authentication specialist. The declaration issued disconnected when setting-up the hub. At the point when a hub speaks with another, it needs to sign the message with its particular private key (done safely by the TPM), the mark and the testament of the general population key. The assessment of the arrangement has been finished utilising reenactment, and the overhead included by coordinating validation does not surpass 15% of vitality utilization [9].

Gagandeep Kaur et al. [2016] Sensor hubs assemble the information from the air and transmit to BS. In any case, assailants degenerate information while transmitting in this manner information security is fundamental worry of WSN. In characterize convention; we diminish the detached assault on sink hub through reducing the movement on sink hub. The reproduction results exhibit the characterize method can every hub will pack their information before sending to the group head. In the wake of compacting, the bundle size of the hub will diminish. This will diminish the movement over-burden. In this pressure system, they reduce the span of the parcel [10].

Janusz Furtak et al. [2016] discussed about utilization of IoT is a most significant test. The principal purposes behind this issues state are that the sensor hubs of the n/w are generally versatile, utilize interfaces remotely, have a little handling power and have little vitality assets. The paper characterizes the answer for cryptographic security of transmission between sensors hubs in the information connect layer and for cryptographic assurance of information spare in the sensor hub assets. The characterize result makes it conceivable to assemble secure and blame tolerant SN [11][12].

Pooja.Shukre et al. [2016] Security and secrecy of information are exceptionally basic while sending a WSN. ly upon WSN is broad. Security result usage is a primary issue as these systems shaped from asset obliged modest sensor hubs which have pitiful computational power and system lifetime. Besides, the applications require a unique period of security. A standard security arrangement is not achievable in such systems [14].

3. ASSAULTS ON WSNs

Interior Attacks: These are for the most part done due to the traded off hubs. These bargained hubs consistently try to upset or parallelize the system. Because of sort of movement performed by the aggressor, it can be additionally named: Outside Attack-in which, an assailant can supplant/present new malignant hub from outside. Inside Attack-in which, an assailant can catches any hub; reconstruct it, to go about as vindictive hub.

Outer Attacks: In these assaults, the aggressor hub is not generally an approved take part of SN. Rely upon the direct of assailant hub, and it could classify as:

Passive Attack: It involves listening in on or checking parcels swapped inside a WSN. It includes just unapproved tuning into the steering bundles.

Assaults

By and large, encryption is the standard answer for guard against these assaults. • Active Attack-it incorporates a couple of changes of the information stream or the making of a wrong stream. Additionally, it brings about upsetting system functionalities by presenting DOS assaults, Jamming assaults and Power Exhaustion.

Gadget Level Capability Attack: This class of assaults sorted relies upon the capacity of the gadget that is utilised for assaulting. An assailant may assault the WSN either utilising a sensor gadget (Sensor Level) or all the more effective workstation gadget (Laptop Level). An enemy can exceedingly harm the framework on the off chance that he/she utilises Laptop Class assault having all the more intense calculation, stockpiling and battery life. Close to the previously mentioned groupings, an assailant may use at least one of the resulting assault strategies, for example,

Spying: In which an assailant quietly tune in to media for dispatch in the midst of two gatherings and don't adjust the information. It is an uninvolved method.

H. Hub trade-off (Destruction or robbery): This incorporates physical catching of a hub in succession to arrange by breaking the correspondence way or reinventing a hub, so it goes about as a government operative in organizing.

Dissent of Service (DoS): In this, the assailant will routinely send bundle in grouping to upset administrations or battery control by utilising pernicious hubs. This is a dynamic kind of assault.

Particular Forwarding (Gray Hole Attack): In this assault, the assailant will embed hub of noxious in the n/w which tries to change the directing and catch information simply like dark gap assault however not usual for it will individually forward information (not all) thus hard to distinguish.

Wormhole Attack: This sort of assault finished with no less than two malevolent hubs which have high data transmission between them either wired or remotely. These vindictive hubs will demonstrate other typical hubs that they give the shorter way to the objective regardless of whether they are laying far away in the system. In this way, the hub will forward information to the noxious hub that can be caught by assailant effectively.

Boundless Loops: In this assault, at least two malignant hubs try to course parcels unendingly in the n/w in succession to debilitate energy of the system.

Message Alteration: In this assault, the hub of noxious will catch and adjust bundles on the system. It can include false information or erase information so bundle will end up adulterated.

Lack of sleep torment: In this assault, the malignant hub will keep a hub from resting by sending messages to it or requests count. This is finished so the hub will expand its energy rapidly[4][5].

4. SECURITY REQUIREMENTS IN WSNs

A WSN is an extraordinary kind of framework. It gives a couple of shared attributes to a run of the mill PC mastermind, yet likewise demonstrates various features that are sole to it. The organizations of security must guarantee the information passed on finished the n/w and the advantages from strikes and nodal lousy behaviour in a WSN. The fundamental security necessities are recorded underneath in WSN:

A. Information privacy: The security system needs to ensure that no message in the n/w comprehended with the guide of anyone other than the assumed beneficiary. In a WSN, the hazardous of classification should address the following necessities.

B. Accessibility: These necessities ensure which the WSN administrations ought to be available constantly even in the event of an outside or inside assaults, e.g. DoS. Disparate techniques have been characterised through examiners to achieve this target. While a few components make an adventure of special dispatch among hubs, others propose the use of a focal access control framework to ensure effective exchange of all messages to its collector.

C. Self-association: Every hub in a WSN must act naturally sorting out and self-recuperation. This normal for a WSN also postures excellent difficulties to wellbeing. The WSN dynamic nature makes it once in a while impractical to establishment any pre-introduced crucial shared system the few hubs and the BS. A no. of critical pre-dispersion frameworks have been characterizing inside the setting of symmetric encryption, However, for programming of open vital cryptographic systems, a proficient instrument for crucial appropriation could be exceptionally an impressive arrangement essential. It is ideal that the hubs in a WSN self-set up among themselves no longer least complex for multi-bounce directing however additionally to carryout scratch control and developing confide in relations.

D. Secure restriction: In numerous conditions, it will end up necessary to precisely and consequently find every sensor hub in a WSN. For example, a WSN wanted to find blunders would require specific regions of sensor hubs perceiving the shortcomings. A limit foe can without trouble furnish and control counterfeit territory data with the guide of announcing counterfeit sign resource, replaying messages et cetera. On the off chance that the information insights not generally secured appropriately. The journalists in have characterised a route called as certain multilateration (VM). In multilateration, the situation of a gadget precisely processed from a succession of known reference focuses. The creators have used separation jumping and verified extending to ensure the precise placement of a hub. Due to the remove jumping utilization, an assaulting hub can best use it is guaranteed separate from a circumstance factor.

The reference point messages scrambled to use a mutual worldwide symmetric key which is pre-appropriated in the sensor hubs. Misusing the data from each of the reference points which a sensor hub acknowledges, it ascertains it evaluated area rely upon the locators facilitates [6,7]. The sensor hub at that point figures covering reception apparatuses is abusing a dominant part race plot. The last sensor hub region resolved through processing the gravity focal point of the covering radio wire territory.

E. Verification: The imparting hub is the one that it cases to be. An enemy cannot just change information bundles yet, also, can alter a parcel stream through embeddings manufactured bundles [8]. It is, hence, imperative for a recipient to have a component to affirm which they got bundles have in reality touch base from the original sender hub.

5. CONCLUSION

WSN are systems which are involved sensors that circulated in a specially appointed way. WSNs are turning into a cost-effective, viable approach to conveying sensor systems .we utilises the voracious calculation and framework based innovation. The plan is likewise ready to stay away from the voids and deterrents in the system by its decentralized sending strategy, in this way diminishing bundle drop because of system stack, as against the looked at the approach. The outcomes demonstrate that GBRR adequately distinguishes the repetitive hubs and timetable them on the other hand in the climate with irregular obstructions. All these make GBRR dependable plan that can enhance the general system nature of administration for WSN.

References

[1] https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications/ [Last Accessed on 10-05-**(2019)**]

[2] NM. Nair, JS. Terence, “Survey on Distributed Data Storage Schemes in Wireless Sensor Networks", Indian Journal of Computer Science and Engineering (IJCSE), Vol.4, No.6, pp.1-6, **(2014)**.

[3] P.Sengar, N. Bharadwaj, “A Survey on Security and Various Attacks in Wireless Sensor Network”, IJCSE, Vol.5, No.4, pp.78-84.

[4] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey”, Science direct, Vol.52, Issue.12, pp.2292– 2330, **(2008)**.DOI: 10.1016/j.comnet.2008.04.002

[5] AS. Mandloi, V. Choudhary, "An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.6-10, **(2013)**. DOI: 10.5120/9555-4013

[6] Sanchita Gupta, PoojaSaini, "Modified Pairwise Key Predistribution Scheme with Deployment Knowledge in Wireless Sensor Network", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.21-23, **(2013)**.

[7] N. Meenaksi, P. Rodrigues, "Tsunami Detection and forewarning system using Wireless Sensor Network - a Survey", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.76-79, **(2014)**.

[8] ChanchalYadav, SS. Hegde, NC. Anjana, Sandeep Kumar, “Security Techniques in Wireless Sensor Networks: A Survey”, International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.4, pp.289-295, **(2015)**. DOI: 10.1109/MWC.2004.1368893

[9] JaydipSen, “A Survey on Wireless Sensor Network Security”, International Journal of Communication Networks and Information Security, Vol.1, No.2, pp.1-16, **(2009)**.

[10] Hye Yun Kim, Seong Cheol Kim, Hyun Joo Park.Priority and Delay Aware packet transmission MAC Protocol for Wireless Sensor Networks, International Journal of Security Technology for Smart Device. Vol. 5. No. 2. Oct. **(2018)**.GVPress. pp. 9-14.

[11] Sengphil Hong “Enhanced Re-route Filtering Scheme for Data Reporting in Wireless Sensor Networks”, International Journal of Wireless and Mobile Communication for Industrial Systems. Vol. 3. No. 2. Oct. **(2016)**.GVPress. pp. 1-8.DOI: 10.1109/tnet.2009.2026901

[12] SystemRekha Purohit and Prabhat Mathur, “Role of Wireless Sensor Networks in Communication with Artificial Intelligence”, International Journal of Wireless and Mobile Communication for Industrial Systems. Vol. 3. No. 2. Oct. **(2016)**.GVPress. pp. 33-38.

[13] Chen Yu, Sonali Gupta, and Arun Agrawal, “Location based Technique to prevent Sybil attack in wireless sensor networks”, International Journal of Reliable Information and Assurance. Vol. 5. No. 1. Jun. **(2017).**GVPress. pp. 1-8.

[14] Hyun Joo Park, Seong Cheol Kim, Hye Yun Kim, “Delay Aware Data Gathering Mechanism in Wireless Sensor Networks”, International Journal of Security Technology for Smart Device. Vol. 5. No. 2. Oct. **(2018)**.GVPress. pp. 15-20.