IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

An Overview of Wireless Sensor Networks (WSN): Applications and Security

Aishwarya Kumar[1*], Awadhesh Kumar[2]

[1,2]Dept. of Computer Science and Engineering K.N.I.T, Sultanpur, U.P, India

[*]*Corresponding Author: Aishwarya Kumar_aishwaryasri2202@gmail.com, Tel.: 7905981009*

DOI: https://doi.org/10.26438/ijcse/v7i7.98100 | Available online at: www.ijcseonline.org

Accepted: 13/Jul/2019, Published: 31/Jul/2019

Abstract— Wireless correspondence innovations keep on experiencing fast headway. Wireless sensor nodes have restricted handling capacity, store-up and active minerals. The presence of sensor network rely on the life of sensor nodes i.e., eventually on the energy inhalation during its procedure. Therefore, in WSN, the effective use of energy resources is very much essential. Clustering is one of the viewpoints for energy saving in WSN. As of late, there has been a lofty development in research in the zone of Wireless sensor systems (WSNs). In WSNs, correspondence happens with the assistance of spatially dispersed, self-governing sensor hubs prepared to detect explicit data. WSNs can be found in an assortment of both military and regular citizen applications around the world. Models incorporate recognizing adversary interruption on the war zone, object following, natural surroundings checking, tolerant observing and fire recognition. Sensor systems are rising as an alluring innovation with extraordinary guarantee for what's to come. Nonetheless, challenges stay to be tended to in issues identifying with inclusion and arrangement, versatility, nature of-administration, estimate, computational power, vitality proficiency and security. This paper exhibits an outline of the various utilizations of the wireless sensor systems and different security related issues in WSNs.

Keywords— Wireless, Network, Self-governing, Explicit Data.

I. INTRODUCTION

Wireless Sensor Network (WSN) [1], [2] is a wireless system comprising of spatially disseminated self-sufficient gadgets that utilization sensor to screen physical or ecological conditions. These self-governing gadgets, or hubs, join with switches and a passage to make a common WSN framework. The circulated estimation hubs impart wirelessly to a focal portal, which gives an association with the wired existence where you can gather, process, break down, and present your estimation information. To expand separation and unwavering quality in a wireless sensor arrange, you can utilize switches to pick up an extra correspondence connect between end hubs and the door. Right now, wireless sensor systems are starting to be conveyed at a quickened pace. It isn't nonsensical to expect that in 10-15 years that the world will be secured with wireless sensor systems with access to them by means of the Internet. This can be considered as the Internet turning into a physical system. This new innovation is energizing with boundless potential for various application regions including ecological, therapeutic, military, transportation, amusement, emergency the board, country barrier, and brilliant spaces.

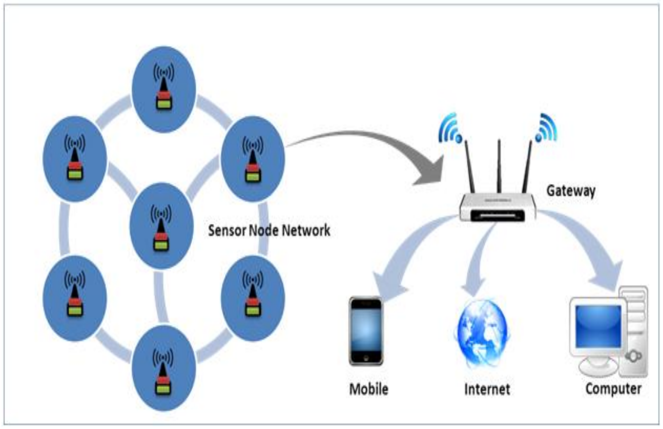

Figure 1. Wireless Sensor Network (WSN)

In the above mention figure 1 its shows wireless sensors network mainly consists of one or more than one base station and thousands of sensors network scattered in physical space. With integration of information sensing, computation and wireless communication, the sensor node, sense physical information and process the information to base station. The real difficulties to be tended to in WSNs are inclusion and arrangement, adaptability, nature of-administration, estimate, computational power, vitality proficiency and security [3]. Among these difficulties, security is a noteworthy issue in wireless sensor systems. The vast majority of the dangers and attacks against security in wireless systems are practically like their wired partners while some are exacerbated with the incorporation of wireless availability. Truth be told, wireless systems are generally progressively defenceless against different security dangers as the unguided transmission medium is more vulnerable to security attacks than those of the guided transmission medium. The communicate idea of the wireless correspondence is a basic possibility for listening in. In this paper we present a review of the applications and security issues identifying with Wireless Sensor Networks (WSNs).

II.APPLICATIONS OF WIRELESS SENSOR NETWORK

A. MILITARY APPLICATIONS

Wireless Sensor Networks are turning into a basic piece of military direction, control, correspondence and knowledge frameworks. Sensors can be conveyed in a front line to screen the nearness of powers and vehicles, and track their developments, empowering close reconnaissance of contradicting powers.

B. NATURAL APPLICATIONS

Natural applications incorporate following the developments and examples of bugs, winged creatures or little creatures.

C. MEDICINAL SERVICES APPLICATIONS

Wireless sensor systems can be utilized to screen and track older folks and patients for social insurance purposes, which can altogether mitigate the serious deficiency of human services staff and diminish the medicinal services consumptions in the present medicinal services frameworks. For instance sensors can be conveyed in a patient's home to screen the practices of the patient. It can caution specialists when the patient falls and requires quick restorative consideration.

D. NATURAL CONDITIONS MONITORING

WSN applications here incorporate observing the ecological conditions influencing yields or domesticated animals, checking temperature, stickiness and lighting in places of business, etc. These observing modules could even be joined with actuator modules which can control, for instance, the measure of manure in the dirt, or the measure of cooling or warming in a structure, in light of disseminated sensor estimations.

E. HOME INTELLIGENCE

Wireless sensor systems can be utilized to give progressively helpful and insightful living conditions for individuals. For instance, wireless sensors can be utilized to wirelessly peruse utility meters in a home like water, gas, power and after that send the readings to a wireless focus through wireless correspondence.

F. MECHANICAL PROCESS CONTROL

In industry, WSNs can be utilized to screen assembling process or the state of assembling gear. For instance, concoction plants or oil purifiers can utilize sensors to screen the state of their miles of pipelines. These sensors are utilized to alarm in the event of any disappointments happened.

G. AGRICULTURE BUSINESS

Using Wireless sensor organizes inside the agrarian business is progressively normal; utilizing a wireless system liberates the rancher from the upkeep of wiring in a troublesome situation. Gravity feed water frameworks can be checked utilizing weight transmitters to screen water tank levels, siphons can be controlled utilizing wireless I/O gadgets and water use can be estimated and wirelessly transmitted back to a focal control place for charging. Water system computerization empowers progressively productive water use and diminishes squander.

H. AUXILIARY MONITORING WIRELESS SENSORS

It can be utilized to screen the development inside structures and framework, for example, spans, flyovers, dikes, burrows and so forth empowering Engineering practices to screen resources wirelessly without the requirement for expensive site visits, just as having the benefit of day by day information, though generally this information was gathered week by week or month to month, utilizing physical site visits, including either street or rail conclusion at times. It is additionally undeniably more exact than any visual examination that would be done

III. ATTACKS ON WIRELESS SENSOR NETWORKS

Coming up next are the sorts of attacks on wireless sensor systems:-

- Normal Attacks
- Disavowal (Denial) of service (DOS) Attack
- Hub bargain
- Pantomime Attack
- Convention explicit Attack

A. NORMAL ATTACKS

The main regular attack is listening stealthily i.e.., an enemy can without much of a stretch recover important information from the transmitted bundles that are sent. The second regular attack is Message adjustment i.e.., the foe can capture the bundles and change them. The third regular attack is message replay that is; the enemy can re-transmit the substance of the bundles sometime in the future.

B. DISAVOWAL (DENIAL) OF SERVICE (DOS) ATTACK

A DOS attack [4] on WSN may take a few structures. The first is hub cooperation, in which a lot of hubs act maliciously and forestall communicate messages from achieving certain areas of the sensor systems. The second one is sticking attack, in which an assailant sticks the correspondence channel and maintains a strategic distance from any individual from the system in the influenced territory to send or get any parcel. The third one is fatigue of intensity, in which an assailant over and over solicitations bundles from sensors to exhaust their battery life.

C. Hub Bargain

A sensor hub is said to be undermined when an aggressor increases control or access to the sensor hub itself after it has been conveyed. Different complex attacks can be effectively propelled from traded off hubs, since the subverted hub is an undeniable individual from the sensor organize.

D. Pantomime Attack

The most well-known attack that can be propelled utilizing a bargained hub is the pantomime attack, in which a malevolent hub mimics a real hub and utilization its character to mount a functioning attack, for example, Sybil [5] or hub replication. In a Sybil attack, a solitary hub takes on different personalities to bamboozle different hubs. Then again, the hub replication attack is the duplication of sensor hubs.

E. Convention explicit Attack

The attacks against directing conventions in WSN are: Spoofed steering data debasement of the interior control data, for example, the steering tables, Selective sending specific sending of the parcels that cross a noxious hub relying upon certain criteria, Wormhole attack Creation of a wormhole [6] that catches the data at one area and replays them in another area either unaltered or altered, Hello flood attack making of false control bundles during the organization of the system.

IV.SECURITY MECHANISMS FOR COUNTERING ATTACKS ON WIRELESS SENSOR NETWORKS

To counter regular attacks like listening stealthily, message change, message replay attacks, solid encryption procedures and time stamps are to be utilized. The instruments to counteract Denial of Service attacks incorporate instalment for system assets, push-back, solid confirmation and distinguishing proof of traffic.

To counter Sybil attack appropriate confirmation is a key safeguard. A believed key server or base station might be utilized to confirm hubs to one another and bootstrap a common session key for encoded correspondences. This necessitates each hub share a mystery key with the key server. In the event that a solitary system key is utilized, bargain of an any hub in the WSN would vanquish all validation.

To counter HELLO flood attack, checking the bi-directional of the neighbourhood interfaces before utilizing them is compelling if the aggressor has indistinguishable gathering capacities from the sensor gadgets.

To counter specific sending attack, Using various disjoint directing ways and assorted variety coding are utilized.

For countering worm gap attack, geographic sending is an alter safe directing convention. Each message is sent separately, picking the following bounce hub to be the neighbour nearest to a definitive goal. Such a plan would not support wormhole attack in the system; however it might incidentally utilize it.

V.CONCLUSION

In this paper we present an outline of the utilization of WSNs and various applications and security issues identifying with Wireless Sensor Networks (WSNs).After study of various researches related to Wireless Sensor Network (WSN) is a developing innovation that shows extraordinary guarantee for different advanced applications both for mass open and military. The detecting innovation joined with preparing force and wireless correspondence makes it rewarding for being misused in wealth in future. We made a theoretical observation during study and we found numerous uses of WSNs incorporate military, well-being, ecological, water, enterprises, home, farming, etc. Other than these applications, security is the fundamental issue in WSNs. There are numerous attacks on WSNs including wormhole attack, Sybil attack, particular sending, and pantomime attack.

REFERENCES

[1] J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, "*System Architecture Directions for Networked Sensors*", ASPLOS, November **2000**.

[2] Culler, D. E and Hong, W., "*Wireless Sensor Networks*", Communication of the ACM, Vol. **47**, No. **6**, pp. **30-33**, June **2004**.

[3] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "*Security for Sensor Networks*", CADIP Research Symposium, **2002**.

[4] A.D. Wood and J.A. Stankovic, (2002) "*Denial of Service in Sensor Networks*," Computer, vol. **35**, no. **10**, pp. **54– 62**, **2002**.

[5] J. R. Douceur, "*The Sybil Attack*," in 1st International Workshop on Peer-to-Peer Systems (IPTPS ‟02), **2002**.

[6] Zaw Tun and Aung Htein Maw, "*Worm hole Attack Detection in Wireless Sensor networks*", proceedings of world Academy of Science, Engineering and Technology Volume **36**, ISSN **2070-3740**, December **2008**.