RESEARCH ARTICLE OPEN ACCESS

Classification of Various Attacks and Security Issues in Wireless Sensor Network

Samapika Parida
Assistant Professor, Raajdhani Engineering College, Bhubaneswar

ABSTRACT
Wireless sensor networks (WSN) have a set of algorithms and protocols with self-establishing capabilities. These sensors work with each and every different to sense some bodilyphenomenon after which the information gather is processed to get relevant outcomes. These sensor nodes can calculate, sense,and assemble particulars from the atmospheres and basedtotally on some nearby decision process, they are in a positionto transmit the sensed files to the person. The battery is theforemost electrical energy grant in a sensor node andsecondary energy supply that harvests energy from theatmospheres together with photo voltaic panels mayadditionally be brought to the node depending on theappropriateness of the atmospheres where the sensor will bediffuse. Clustering is the method which performs the groupingof similar nodes and then starts communicating into theclusters. Security can be finished by means of encrypting anddecrypting the facts and make them unable to read that fromthe malicious users. Cryptography is the useful techniquewhich contains symmetric and asymmetric methods. In thispaper we find out about about WSN and its utility or a numberof assaults which exist in the sensor community in the middleof paper we talk about a variety of existing technique and it'sworking. Various assaults are carried out in this communitysuch as passive and lively assaults or insider and outsiderattacks. The wirelessly network always required protection inthe form of information integrity, confidentiality, authenticityand etc.

Date of Submission: 20-05-2025 Date of acceptance: 30-05-2025

I. INTRODUCTION

A WSN involves of spatial allotted self-directed sensors toenvironment circumstances or display physical, e.g. sound,pressure, temperature, etc. [1]. These sensors are slight, and theyare inexpensive and with restrained processing and computing assets as equaled to fashionable sensors. These sensor nodes canmeasure, sense, and accumulate information from theatmospheres and, primarily based on some local decisionprocess, they are successful to transfer the sensed archives to theperson. Sensor nodes are lowest energy device ready with one orgreater sensors, a processor, memory, a energy supply, a radio,and an actuator.A variety of thermal, organic, optical, mechanical, and magneticand chemical sensors can be linked to the sensor node to measure belongings of the atmosphere. Since the sensor nodeshave limited reminiscence and are usually diffuse in thedifficult-to-get entry to places, a radio is carried out forwirelessly communiqué to transfer the documents to a basestation (BS) (e.g., a computer, a non-public handheld device, ora get proper of entry to aspect to a set infrastructure). Battery isthe important electricity provide in a sensor node. Secondarypower furnish that harvests electricity from the atmospherescollectively with solar panels might also be add to the noderelying on the appropriateness of the atmospheres the place thesensor will be diffuse. Depend on the utilization and the varietyof sensors utilized; actuators may additionally be integrated inthe sensors [2].

II. WSN APPLICATION

We can categorize the tradition of WSN into defenseapplications, forest applications, as well as domesticapplications.

A. Defense applications

WSNs can be an indispensable section of protection command,security control, records communications, computation, intelligence, concentrated on systems such as surveillance etc.

B. Forest applications

Certain environmentally utilization of sensor networks (SN)contain recording and notice the activities of minor birds andinsects, monitoring environmental conditions, animals, earthmonitoring and exploration.

C. Medical Science applications

Certain of the purposes of health for SN are diagnosing thepatients, tracking region and motion of patients and medicalpractitioner inside health facility etc.

D. Industrial applications

Certain industrial functions of WSNs are make virtualkeyboards, environmental control in office constructions, robot control, interactive toys, monitoring product fantastic etc.

III. TYPE OF WSN

According to previously lookup art work accomplished fivevarieties of WSN are possible relying upon wherein and howSensors are hooked up to reveal info. According to thesehomes of sensor deployment we are in a position to classifyWSNs into five essential kinds namely; underground WSN,Ground (terrestrial) WSN, aquatic (underwater) WSN, andmobility WSNs.

A. Ground (Terrestrial) WSNs

Usually consist of hundreds to thousands of cheap WSNarranged randomly in a given sensing region. Sensor nodes can be plunged from a randomly and plane situated into the targetregion in ad hoc diffuse. In a position (terrestrial) WSN, reliablecommuniqué in a intense atmosphere is very vital. Ground sensornodes must be able to efficiently communicate info return to theBS. Whereas battery power is constrained resource aid and it'simportant restraint on network performance and its competent tonot be rechargeable or replaceable again, ground sensor nodesyet can be well- found with a secondary power source e.g batteryor solar cell. So due to this it is forever important for sensornodes to preserve energy.

B. Underground WSNs

Underground WSNs are sequence of few of the sensor nodesplaced inside the earth crust or in a cave or in a mine and theymay be utilized to reveal underground things to do collectivelywith volcanic situations and many others. Extra sink or BS nodesare positioned above crust of earth to transmit info from thesensor nodes to the BS.These category of WSN are an entire morehigh cost than a ground (terrestrial) WSN in stages of equipment, maintenance and deployment. Subversive sensor nodes areadditional high priced because vital device parts ought to bedecided on to ensure reliable communiqué thru soil, water, rocks, and other stuffing residing internal crust. The insidecircumstances atmosphere produce wirelessly communiqué achallenge because of highest levels of signal losses andreduction.

C. Aquatic (Underwater) WSNs

Aquatic WSNs consist of few of sensor nodes and vehiclesdisperse under water. As conflicting to ground WSNs, aquaticsensor nodes are extra high-priced and lesser sensor nodes aredisperse in sensing region. Self-directed aquatic vehicles are utilized for accumulating or exploration facts from sensor nodes.As in evaluation to a dense diffuse of sensor nodes in a floorWSN, a sparse diffuse of sensor nodes is positioned at sea level.Typical aquatic (underwater) wirelessly communications areapplied thru transmission of acoustic waves.

D.Multi-media WSNs

Multi-media WSNs are mixture of a no. of lowest chargesensor nodes well-appointed with microphones and cameras.These sensor nodes interconnected with each and every one of akind over a wirelessly connection for information sensing,documents processing, records correlation, and recordscompression. Multi-media WSNs are utilized to allowmonitoring of activities inside the form of multimedia programs.

E.Mobile WSNs

Mobility WSNs are a no. of transferring sensor with theirinteraction with sensing atmosphere. Moving sensor nodes havethe viable to compute, like non-moving nodes. Mobility WSNsare utilized in navy and other industrial applications [3].

IV. ATTACKS ON WSN

A. Internal Attacks

These are mainly performed due to the fact of the compromisednodes. These compromised nodes always are searching for todisrupt or parallelize the network. Based on kind of undertakingperformed by using attacker, it can be further classified as:Outside Attack- in which, an attacker can replace/introduce newmalicious node from outside. Inside Attack- in which, an attackercan two seize any node; reprogram it, to act as malicious node.

B. External Attacks

In these attacks, the attacker node isn't forever an endorsedcontribute of SN. Depend on the behavior of attacker node, itcould be classified as:

Passive Attack- it includes snooping on or observingpackets exchanged with WSN. It engages only unauthorizedlistening to the routing packets.
Generally, encryption is the standard solution to preservebeside these attacks.

Power Exhaustion

I. Device Level Capability Attack

This type of assaults is labeled depend on the functionality of thegadget that is being used for attacking. An attacker mayadditionally assault the WSN both the use of a sensor machine(Sensor Level) or more effective laptop computer machine(Laptop Level). An adversary can fairly injury the machine ifhe/she makes use of Laptop Class assault having extra effectivecomputation, storage and battery life. Beside the above notedclassifications, an attacker may utilize one or greater of thesubsequent assault techniques.

J. EavesdroppingIn which an attacker mutely listen to media for announcementamid two parties and don't adapt the data. It's a passive technique.

K. Radio jamming

In this attack, the attacker tries to disrupt the conversation bysending few radio waves at the comparable frequency resultingin interference or collisions of packets over network. Jammingcan be intermittent or non-stop depend on the time for whichcommunity is kept jammed.

L. Message's injection

In this the attacker broadcasts many false messages abovenetwork in lieu of humiliating the packet data or to simply fatiguenetwork.

M. Message's replicationIn this the attackers imprison and resend the identical packetmany times to similar or different sensor and at dissimilar times insuccession to make receiver foolish.

N. Node compromise (Destruction or theft)

This includes physical capturing of a node in succession tointerrupt network by flouting the communication alleyway orreprogramming a node so that it acts as a spy in network.

O. Denial of Service (DoS)In this the attacker will frequently sends packet in succession tointerrupt services or battery power through using malicious nodes.This is an vigorous type of attack.

P. HELLO Flooding

We recognize that HELLO message is used for discoveringneighbors. In this structure of attack, the attacker makes use ofextra effective nodes to ship HELLO messages to far awaysensor nodes so that they believe that the malicious node is theirneighbor and they will transfer future packets to it.Black Hole AttackIn this attack a node attempts to become receiver of packets ofadjacent nodes by altering their routing table and it will never aheadthe packets to exact destination.

Q. Selective Forwarding (Gray Hole Attack) in this attack, the attacker will insert node of malicious in then/w which tries to alternate the routing and capture data just likeblack gap attack however unlike it will selectively forward facts(not all) and so difficult to detect.

R. Wormhole Attack

This kind of attack is carried out with at least two maliciousnodes which have high bandwidth between them either wired orwirelessly. These malicious nodes will show different regularnodes that they furnish the shorter route to the goal even if theyare lying far away in the network. So, the node will forwardstatistics to the malicious node that can be captured by means ofattacker easily.

S. Sinkhole Attack

In this attack the malicious node exist in near the BS and it tries tofantasy to be contiguous node to the BS so that other neighboringusual node will change themselves and ahead info to the maliciousnode.

T. Sybil Attack

In this attack the adversary tries to have countlessindividualists to exclusive nodes and consequently can be inmore than one region at single time. Here it tries to be voted asthe cluster head. A Sybil assaults is enormous danger toGeographic Routing Protocols.

U. Infinite Loops-

In this assault two or extra malicious node tries to flow intopackets infinitely in the n/w in sequence to exhaust electricity ofthe network.

V. Message Alteration

In this assault the node of malicious will detain and adjust packetson the network. It can add bogus data or remove data so thatpacket will turn into tainted.

W. Sleep deprivation torture

In this assault, the malicious node will avert a node from latentby sending messages to it or asks for estimation. This is absoluteso that the node will devour its power rapidly [4].

V. SECURITY REQUIREMENTS IN WSN

A WSN is a distinct form of network. It shares few

Commonalities with a common laptop network, however alsoexhibitions many features that are sole to it. The offerings ofprotection have to be protecting the info communicated over then/w and the sources from attacks and nodal misconduct

in aWSN. The quintessential protection requirements are listedbelow:

A. Data confidentiality

The safety mechanism wants to make positive that no messagein the n/w is understood with the useful resource of everybodybarring supposed recipient. In a WSN, the complicated ofconfidentiality ought to tackle the next requirements.

B. Availability

This necessities make certain which the WSN offerings oughtto be handy constantly even in prevalence of an external orinterior assaults e.g. DoS. Dissimilar strategies have beendescribed thru investigators to accomplish this objective. While some mechanisms create exploit of extra communiqué amongnodes, others advocate utilize of a central get entry to manipulatesystem to make certain profitable transfer of all message to itsreceiver.

C. Data freshness

It implies which the information is cutting-edge and make surewhich no opponent can replay old messages. This requirement isespecially vast when the WSN nodes develop shared- keys formessage communiqué, whereas a potential opponent cancommence a repeat attack developing the old key as the latestkey is being broadcasted to every the nodes in the WSN.A time precisecounter may be placed in to all packet to ensure thepurity of the packet.

D. Self-organization

Every node in a WSN have to be self-organizing and self-recuperation.This characteristic of a WSN moreover poses goodchallenges to safety. The WSN dynamic nature makes itsporadically not possible to fixing any pre-installed shared keymechanism the numerous nodes and the BS. A no. of key redistributionsscheme have been describe inside the context ofsymmetric encryption However, for software of public-keycryptographic methods an efficient mechanism for keydistribution could be extremely a great deal vital. It’s perfect thatthe nodes in a WSN self-establish between themselves no longer simplest for multi-hop routing though also to carryout keycontrol and growing trust relations.

E. Secure localization

In many conditions, it will befall necessary to precisely androutinely determine each sensor node in a WSN. For example, a WSN intended to locate errors would require accurate localitiesof sensor nodes distinguish the faults. A capacity challenger canwithout complexity provide and influence false locality info withthe help of reporting fake sign benefit, replaying messages andso on. If the info statistics isn't forever secured correctly. Thewriters in have distanced a way called as verifiablemultiliteration (VM). In multiliteration, the location of a device is precisely computed from a series of known orientation points. The authors have exploited distance bounding and genuine ranging to make sure precise place of a node. Due to the distance bounding usage, an attacking node can quality successful itsclaimed distance from a situation factor. However, to make positive location consistency, the attacker would additionally need to exhibit that its distance from every other reference factor is shorter. As it isn't usually practicable for the attacker to prove this, it is miles conceivable to come across the attacker. The system is a decentralized range self-governing localization scheme. It’s supposed that the locators are relied on and can’t be compromised thru any attacker. A sensor calculates its location thru listening to the beacon information sent via all locator that consists of the locator’s region info. The beacon messages are encrypted utilize a shared international symmetric key which is pre-distributed in the sensor nodes. Exploiting the data from each the beacons which a sensor node accepts, it calculates it estimated locality rely on the locators coordinates. The sensor node then calculates overlapping antennas are exploiting a majority election scheme. The ultimate sensor node locality is determined via computing the gravity middle of the overlapping antenna area.

F. Time synchronization

The purposes in SN necessitate time synchronization. two Any protection mechanism ought to moreover be time- synchronized. A collaborative WSN can additionally necessitate synchronization amongst a gathering of sensors. In define a gathering of tightly closed synchronization protocols for multihop sender receiver and team synchronization.

G. Authentication

The communicating node is the one that it claims to be. An adversary can’t solely alteration statistics packets however additionally can modify a packet move thru inserting fabricated packets. It’s, therefore, essential for a receiver to have a mechanism to affirm which the obtained packets have certainly arrive from the real sender node.

VI. SECURITY ISSUES IN WSN

A. Data Integrity

It's very essential in SN to make sure the data consistency. It ensures that data packets that are established through the aim areprecisely the ones transfer through the source and any one can't adapt that packet in among.

B. Data Confidentiality

Privacy means to defend data through communiqué in a n/w to be understood other than planned receiver. Cryptographymethods are used to offer confidentiality. It's a most important matter in network security.

C. Data Availability

These services are forever accessible in the n/w still in the attack like Dos. Accessibility is of main significance to preserve an operational network.

D. Data Authentication

The statistics familiar through goal has now not been modified at some stage in the transmission. It's reached by means of asymmetric or symmetric mechanisms in which goal and source nodes share secret keys.

E. Data Freshness

The data commonplace via the goal is commonly modern-dayand fresh information and no challenger can replay the historic info. It's reached via utilizing mechanisms as nonce or including timestamp to all data packet [5].

VII. TECHNIQUES TO DEFEND THREATS IN WSN

Security is a mainly utilized time period encompassing aspects of integrity, privacy, authentication, non-repudiation and anti- playback. The dangers of the information tightly closed transmission over the n/w increases with amplify in the dependency on the data give thru the network.

A. Encryption

That mechanism offers protection against passive attacks as eavesdropping. SN commonly run in wild or public location overinherently insecure wirelessly channels. It is therefore insignificant for a gear to eavesdrop or even add messages intothe n/w. The regular key to this issue has been two espouse approach e.g. method symmetric key encryption schemes, public key cryptography and authentication codes.

B. Symmetric encryption

It's additionally recognized as sole one key cryptography. It makes use of a single key. In this encryption manner the goal andthe supply has to approve upon a sole secret (shared) key. Given a message (plain text) and the key, encryptions generate one intelligible records that is regarding the comparable size as the undeniable text was. Decryption is the encryptions reverses, and makes use of the similar key as encryption.

C. Asymmetric encryption

It's additionally recognized as public key cryptography. It uses two keys: public key, which known to the public, used for encryption and private key, which regarded solely to the person of that key, used for decryption. The non-public and public keys are associated with high-quality by any mathematical method. In exclusive words, information encrypted thru a public key can be encrypted only via its constant personal key [6].

D. Cryptography

Electing the most gorgeous cryptographic method is necessary as all security offerings ensure through cryptography in WSNs.

Cryptographic technique utilized in WSNs have to meet the sensor nodes constraints and be evaluated through facts size, processing time, and code size [7].

VIII. LITERATURE SURVEY

Xiao Liang Meng et al. [2016] in the technique of electing the multi-hop nodes in the WSN, it's substantial to select the subsequent most excellent forwarding node depend on a certainrule. Optimal electing mechanism rely on geographical locationdata is a protocol which take advantage of distances and angles, as the standards of routing election. TBF protocol confers routing packets along a predefined disperses nodes route as a substitute[8].

HacèneFouchal et al. [2016] in this paper a dispensed solution able to make sure authentication of nodes at any time without having any online get entry to a certificates authority. Each node will be device with a Trusted Platform Module (TPM) which is capable to keep keys with security. Each node will have its own public key and private key pair in the TPM and a certificate of the public key. The certificates is issued off-line when setting-up the node. When a node communicates with another, it has to signal the message with its personal key (done securely via the TPM) and sends the message, the signature and the certificates of the public key. The assessment of the answer has been whole the use of simulation and the overhead brought through integrating authentication does not exceed 15% of electricity consumption [9].

Gagandeep Kaur et al. [2016] Sensor nodes acquire the data from the surroundings and transmit to BS. But attackers corrupt statistics while transmitting therefore data security is major challenge of WSN. In define protocol; we reduce the passive assault on sink node through lessening the visitors on sink node. The simulation effects demonstrates the outline method can each node will compress their data earlier than sending to cluster head. After compressing, the packet measurement of node will decrease. This will limit the site visitor's overload. In this compression technique, they slash the measurement of packet via developing a code[10].

JanuszFurtak et al. [2016] Ensuring security in the navy utilization of IoT is a largest challenge. The predominant motives for this affairs kingdom is that the sensor nodes of the n/w are normally mobile, use wirelessly links, have a small processing energy and have a little power resources. The paper defines the answer for cryptographic safety of transmission between sensors nodes in the information hyperlink layer and for cryptographic safety of records save in the sensor node resources. The TPM used to be utilized. The define result makes it possible to build tightly closed and fault tolerant SN. The following aspects have been presented in the paper: the mannequin of such a network, utilized safety solutions, studies of the safety in the n/w and elected investigation effects of such a community were [11]

Mauricio Tellez et al. [2016] with the quickly technological progressions of sensors, WSNs have grow to be a typical technological know-how for the IoT. They examined the WSNs safety In an environment monitoring utilization with a goal to show the overall security. They applied a STMS, that served as our WSN usage. Our effects revealed a safety flaw located in the bootstrap loader (BSL) password utilized to guard MSP430 microcontroller units (MCUs). They illustrate how the BSL password can be brute pressured in a depend of days. Furthermore, we illustrate how an attacker can reverse engineer WSN functions to gain critical security information such as encryption keys. We make a contribution a answer to patch the susceptible BSL password protection flaw and better the protection of MSP430 MCU chips. The Secure-BSL patch we make a contribution permits the randomization of the BSL password. Our end result rises the brute force time to decades. The unusable brute pressure time accompaniments the security of the MSP430 and averts future reverse engineering devices. Our research serves as proof that the security of WSNs and the standard IoT technology is broken if we can't shield these everyday objects at the bodily layer [12]

PoojaM.Shukre et al. [2016] Security and confidentiality of statistics is very tons critical whilst deploying a WSN. Depending on the surroundings in which network is deployed; configuration parameters of network nodes want to be updated time to time. This can be reached take advantage of dissemination protocols and statistics discovery. DiDrip is the preliminary dissemination protocol and records discovery that has been designed through taking distinct safety vulnerabilities in think. The protocol expedites community proprietor to permit a couple of community customers having distinctive privileges for simultaneous and direct dissemination of records into the n/w nodes. This paper outline a new technique to minimalize packet loss throughout data dissemination the use of DiDrip protocol and grant excessive safety to WSN. RSA and Diffie Hellman key trade algorithm are used as methods of encryption [13].

Muhammad Umar Aftab et al. [2015] this paper defines the sorts of WSNs and the likely results for tackling the listed difficulties and consequences of many different issues. This paper will transport the data related to the WSN and shape with literature assessment so that a person can get greater information concerning this emerging area [14].

Biji Nair et al. [2015] the purposes range rely on WSN is extensive. Security result implementation is a important hassle as these networks are shaped from useful resource constrained tiny sensor nodes which have meager computational energy and community lifetime. Moreover, the purposes necessitate numerous section of security. A well-known safety solution isn't possible in such networks. ECC is emerging like a promising protection end result for WSN. Certain functions that require primary protection degree need no longer be careworn with the aid of the use of trendy safety measures which may additionally tax on their efficiency. The correct selection of values of Elliptic Curves (EC) parameters is of paramount significance whilstimposing ECC for resource confined WSN. This paper identifies the relevant parameters of EC for ECC implementation in WSN and analyses the impact in their values on the extent of safety they provide [15].

CONCLUSION

WSN are networks which are comprised of sensors that are distributed in an advert hoc way. WSNs are turning into a cost-effective, sensible way to go about deploying sensor networks .we use the greedy algorithm and grid-based technology.

The scheme is additionally able to keep away from the voids and limitations in the community by means of its decentralized forwarding technique, thereby decreasing packet drop due to community load, as against the compared approach. The outcomes exhibit that GBRR successfully identifies the redundant nodes and agenda them on the other hand in the surroundings with random obstacles. All these make GBRR reliable scheme that has the potential to enhance the typical network nice of carrier for WSN.

REFERENCES

[1]. 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.

[2]. Jennifer Yick, Biswanath Mukherjee, DipakGhosal, "Wireless sensor network survey", Science direct, Vol.52,Issue.12, pp.2292– 2330, 2008.

[3]. AS. Mandloi, V. Choudhary, "An Efficient ClusteringTechnique for Deterministically Deployed Wireless Sensor Networks", International Journal of Scientific Research inNetwork Security and Communication, Vol.1, Issue.1, pp.6-10,2013.

[4]. Sanchita Gupta, Pooja Saini, "Modified Pairwise Key Pre- distribution Scheme with Deployment Knowledge in Wireless Sensor Network", International Journal of ScientificResearch in Network Security and Communication, Vol.1, Issue.2, pp.21-23, 2013.

[5]. 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.

[6]. ChanchalYadav, SS. Hegde, NC. Anjana, Sandeep Kumar, "Security Techniques in Wireless Sensor Networks: ASurvey", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.4, pp.289-295, 2015.

[7]. JaydipSen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks andInformation Security, Vol.1, No.2, pp.1-16, 2009.

[8]. XiaoliangMenga, Xiaochuan Shia, ZiWangb, ShuangWua, ChenglinLia, "A grid-based reliable routing protocol forwireless sensor networks with randomly distributedclusters",elsevier, Vol.51, NO.11, pp.47–61, 2016.

[9]. Hacenefouchal, javierbiesa, elenaromero, alvaroaraujo, octavionietotaladrez, "a security scheme for wireless sensornetworks", 2016 IEEE Global Communications Conference (GLOBECOM), Washington, pp.1-5, 2016.

[10]. Gagandeep Kaur, Deepali, RekhaKalra, "Improvement and analys security of WSN from passive attack", 2016 5thInternational Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),Noida, pp.420-425, 2016