ISSN: 2456-9348
Volume (01) _Issue (05)

iJETRM
International Journal of Engineering Technology Research & Management

REVIEW ON FEATURES, PROTOCOLS, THREATS AND CHALLENGES OF WSN

*Dr.I.Lakshmi
*Assistant Professor, Department of Computer science, Stella Maris College
Chennai-600086, Tamil Nadu, India

ABSTRACT
This paper gives an overview of WSNs advances, conventions, principle applications, dangers and difficulties in WSNs. Because of the incomprehensible capability of sensor systems to empower applications that interface the physical world to the virtual world, the efficient outline and usage of remote sensor systems has turned out to be a standout amongst the most vital advancements for the twenty-first century. A WSN regularly comprises of a substantial number of minimal effort, low-control, and multifunctional remote sensor hubs, with detecting, remote correspondences and calculation capacities. The movement of detecting, preparing, and correspondence under restricted measure of vitality, lights a cross-layer configuration approach commonly requiring the joint thought of disseminated flag/information handling, medium get to control, and correspondence conventions. In this paper different conventions for remote sensor system are talked about. WSN might be vulnerable for different assaults, which are examined under dangers. The fundamental application ranges for WSNs are additionally examined here.

Keywords:
WSN, Protocols, Sensors, Threats.

INTRODUCTION

With the prominence of tablets, PDAs, PDAs, GPS gadgets, RFID, and canny hardware in the post-PC period, figuring gadgets have turned out to be less expensive, more versatile, more circulated, and more unavoidable in everyday life. It is presently conceivable to develop, from business off-the-rack (COTS) parts, a wallet estimate inserted framework with the equal ability of a 90's PC. Such implanted frameworks can be bolstered with downsized Windows or Linux working frameworks. From this viewpoint, the development of remote sensor systems (WSNs) is basically the most recent pattern of Moore's Law toward the scaling down and universality of processing gadgets. Ordinarily, a remote sensor hub (or basically sensor hub) comprises of detecting, processing, correspondence, activation, and power parts. These parts are incorporated on a solitary or numerous sheets, and bundled in a couple of cubic inches. With cutting edge, low-control circuit and systems administration advances, a sensor hub controlled by 2 AA batteries can keep going for up to three years with a 1% low obligation cycle working mode. A WSN for the most part comprises of tens to a great many such hubs that impart through remote channels for data sharing and helpful handling. WSNs can be sent on a worldwide scale for natural observing and living space consider, over a combat zone for military observation and surveillance, in new situations for inquiry and safeguard, in manufacturing plants for condition based support, in structures for foundation wellbeing checking, in homes to acknowledge savvy homes, or even in bodies for patient checking. After the underlying arrangement (normally specially appointed), sensor hubs are in charge of self-sorting out a fitting system foundation, data handling and directing in Wireless Sensor Networks with multi-jump associations between sensor hubs. The installed sensors then begin gathering acoustic, seismic, infrared or attractive data about nature, utilizing either consistent or occasion driven working modes. Area and situating data can likewise be gotten through the worldwide situating framework (GPS) or neighbourhood situating calculations. This data can be accumulated from over the system and suitably handled to develop a worldwide perspective of the observing wonders or questions. The essential theory behind WSNs is that, while the capacity of every individual sensor hub is restricted, the total force of the whole system is adequate for the required mission. A WSN can be by and large portrayed as a system of hubs that helpfully sense and may control the

earth empowering connection between per sensor PCs and the encompassing Environment.

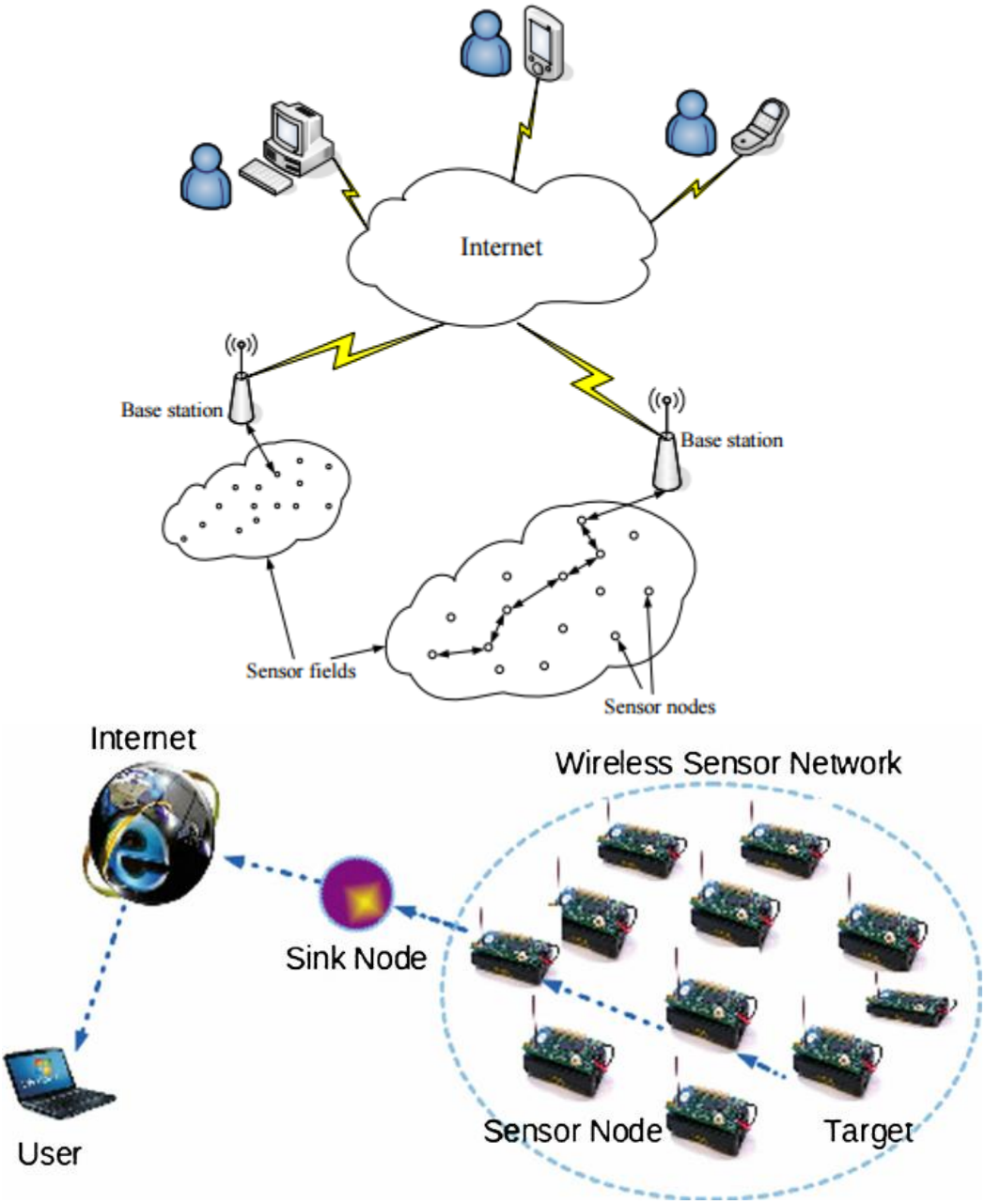

Fig 1: Accessing WSN through internet

Figure-1 demonstrates to get to WSN through web [1]. Remote sensor systems (WSNs) are an imperative innovation for huge scale checking, giving sensor estimations at high transient and spatial determination. It empowers new applications and along these lines new conceivable markets, however the plan is influenced by a few imperatives that call for new ideal models. A WSN comprises of spatially disseminated sensor hubs. In a WSN, every sensor hub can autonomously play out some preparing and detecting assignments. Besides, sensor hubs speak with each other to forward their detected data to a focal handling unit or lead some neighbourhood coordination, for example, information combination. One broadly utilized sensor hub stage is the Mica2 Mote created by Crossbow Technology. The standard equipment parts of a sensor hub incorporate a radio handset, an installed processor, interior and outer recollections, a power source and at least one sensors

ISSN: 2456-9348
Volume (01) _Issue (05)

iJETRM
International Journal of Engineering Technology Research & Management

WIRELESS SENSOR PROTOCOLS

The convention stack utilized by the sink, bunch head and sensor hubs are appeared in Fig. 2. As indicated by (Akyildiz et al., 2002), the sensor arranges convention stack is much similar to the customary convention stack, with the accompanying layers: application, transport, organize, information interface, and physical. The physical layer is in charge of recurrence choice, bearer recurrence era, flag discovery, and regulation and information encryption. The information connect layer is in charge of the multiplexing of information streams, information outline recognition, medium get to and mistake control. It guarantees solid indicate and point multipoint associations in a correspondence arrange. The system layer deals with steering the information provided by the vehicle layer. The system layer plan in WSNs must consider the power proficiency, information driven correspondence, information total, and so on. The transportation layer keeps up the information stream and might be critical if WSNs are wanted to be gotten to through the Internet or other outside systems. Contingent upon the detecting errands, diverse sorts of use programming can be set up and utilized on the application layer. Directing in remote sensor systems contrasts from customary steering in settled systems in different ways. There is no foundation, remote connections are questionable, sensor hubs may come up short, and directing conventions need to meet strict vitality sparing necessities [5]. Many steering calculations were produced for remote systems when all is said in done [3].

Category	Representative Protocols
Location based Protocols	MECN, SMECN, GAF, Span, TBF, BVGF, GeRaF
Data Centric Protocols	SPIN, Directed Diffusion, Rumour Routing, COUGAR, ACQUIRE, EAD, Information – Directed Routing, Gradient based Routing, Energy – aware routing, Information – Directed Routing, Quorum – Based Information Dissemination, Home Agent based Information Dissemination
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Mobility based Protocols	SEAD, TTDD, Joint Mobility and Routing, DATA MULES, Dynamic proxy Tree Based Data dissemination
Multipath based Protocols	Sensor – Disjoint Multipath, Braided Multipath, N – to – 1 Multipath Discovery
Heterogeneity based Protocols	IDSQ, CADR, CHR
Qos Based Protocols	SAR, SPEED, Energy – aware Routing,

Table 1: Routing Protocols for WSNs

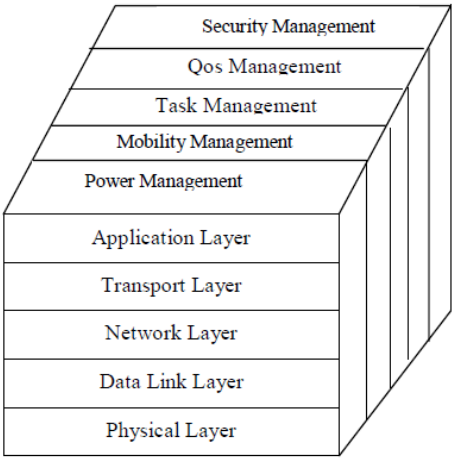

Figure 2: The protocol stack of WSN

Medium Access Control Protocols: Medium Access Control (MAC) conventions for commonplace specially appointed systems have fundamentally centred around advancing decency and throughput proficiency, with less

accentuation on vitality protection. [2]. The concentration of most MAC conventions for sensor systems is to diminish this sit out of gear power utilization by setting the sensor radios into a rest state as regularly as could be expected under the circumstances.

TYPES OF MAC PROTOCOLS:

[1] Sensor-MAC (S-MAC)
[2] Timeout-MAC (T-MAC)
[3] DMAC
[4] Traffic-Adaptive Medium Access (TRAMA)
[5] Sparse Topology and Energy Management (STEM)

THREATS AND THREAT MODELS

With the development of remote sensor organizes, the requirement for securing the information move through these systems is expanding. These sensor systems consider simple to-apply and adaptable establishments which have empowered them to be utilized for various applications. Because of these properties, they confront unmistakable data security dangers. A sensor system is commonly made out of hundreds, and some of the time a large number of hubs. These hubs are equipped for getting, handling and transmitting data, as in view of the allotted undertakings. Data coursing through WSN might be powerless to listening stealthily, retransmit past bundles, infusion of excess or causeless bits in parcels and numerous different dangers of various nature. To guarantee that the information being gotten and transmitted over these systems is secure and ensured, data security assumes an essential part. WSN can be agreeably assaulted by intriguing in which the foe makes utilization of ill-conceived hubs with indistinguishable capacities from of system hubs. Conveyed vindictive hubs can cooperate to take control of any system hub, which can be utilized further to make harms to the system or to open up the extent of the assault. An assailant may have admittance just to a couple of hubs which he or she has traded off. Such aggressor is delegated bit class assailant. Then again an assailant may have entry to all the more effective gadgets, for example, portable PCs, consequently the definition tablet class aggressor. Such aggressors have capable CPUs, awesome battery control, high power radio transmitter and delicate reception apparatuses available to them and represent a much bigger danger to the system. For instance a couple of hubs can stick a couple radio connections where as a portable workstation can stick the whole system. At long last, assaults propelled on a system might be insider or untouchable assaults. In pariah assaults the aggressor has no extraordinary access to the system. In insider assaults in any case, the assailant is thought to be an approved member of the system. Such assaults are either propelled from traded off sensor hubs running vindictive code or tablets utilizing stolen information (cryptographic keys and code) from honest to goodness hubs. Presently a portion of the real assaults on WSN are introduced. Sticking and physical assaults influence the physical layer of the WSN structure. Crash, weariness and injustice assault sorts have a place with the assaults on information interface layer of the WSN.

A.Denial of Service (DoS) Jamming hubs of systems, sending constant informing without taking after the framework correspondence convention (connect layer conventions) by any hub, noxious assaults and ecological condition may bring about asset depletion and disappointments of gadgets in the WSN. This causes debased framework execution and it is not ready to work not surprisingly. These are the types of Denial of Service (DoS) assaults that mean to influence the usefulness of WSN. These assaults are completed on the physical, interface, directing and transport layers of the WSN engineering.

B.Jamming Nodes in WSN use radio frequencies for the transmission of data, as these sensor systems utilize remote channels for interchanges. Sticking is one of the fundamental yet inconvenient assaults that expect to mediate in physical layer of the WSN structure. It is just the transmission of the radio signs having an indistinguishable frequency from being utilized by the remote system. Sticking causes lasting or impermanent suspension of message gathering and transmission from the stuck hub gadgets. WSN is broadly conveyed remote system, which makes finish sticking an unfeasible endeavour. As yet sticking of a couple of hubs in WSN can prompt to disintegration in viability of many neighbouring hubs.

C.Physical Attacks The WSN hubs very inclined to any physical hardening or different assaults performed on its development. Hubs can be adjusted to concentrate key and other essential cryptographic parameters that are critical for working of any security convention. So also foe can extricate source code which in the long run gives assailant the data about the system, which can alter the code to get access into the system. Aggressor can supplant the hubs with the ill-conceived and vindictive ones, in this way bargaining the operation of the entire sensor arrange. Physical assaults give the assailant the capacity to adjust the hubs and along these line the

system working. These assaults are difficult to stay away from because of the real attributes of any WSN to be modest and scatter [4].

D.Collisions cause retransmission of the impacted messages and in the event that it happens regularly then the vitality asset of a hub can be exhausted. Another type of this assault can happen when some part bundle is modified, which causes MAC crisscross at the recipient. The defiled parcels are transmitted once more, expanding the vitality and time cost for transmission. Such an assault when drawn out actuates the lessening of system realization.

E.Exhaustion This assault depletes the power assets of the hubs by making them retransmit the message notwithstanding when there is no crash or late impact. A hub can look for access to any channel purposely and interminably, constraining the neighbouring hubs to react consistently.

F.Unfairness MAC conventions represent the interchanges in systems by compelling need plans for consistent correspondence. It is conceivable to misuse these conventions subsequently influencing the priority plans, which in the long run outcomes in reduction in administration.

G.Neglect and Greed Attack During correspondence between any two hubs in WSN, there might be have to course and re-course bundles through numerous hubs. Transmission from source to goal relies on upon finish and effective steering of the predetermined parcels. Pernicious or bargained hub in the way can impact multi-jumping in the system, either by dropping some of bundles or by directing the parcels towards a false hub. This assault additionally exasperates the working of the neighbouring hubs, which will most likely be unable to get or transmit messages.

H.Homing In homing assault, the enemy examination the system activity to judge the geographic area of group heads or base station neighbouring hubs. It can then play out some other sort of assaults on these basic hubs.

I.Routing Information Alteration (parodying) In this assault, directing data is modified and tempered with. This can make new directing ways, or protract or abbreviate existing steering ways therefore expanding the end-to-end inactivity. It repulses or draws in activity diminishing the nature of administration. It can likewise create false mistake messages which cripple or increment inertness for hubs to get to the channel.

J.Black gaps In WSN, it is conceivable that hubs are not completely mindful with the total topology of the system due to the expansive volume of the system. On the off chance that separation vector-based conventions are utilized as a part of these sensor systems, they are exceptionally powerless to the arrangement of dark gaps. Vindictive hubs can promote zero-cost courses to different hubs in the systems, which causes more activity to stream toward these hubs. On the off chance that this state proceeds with, the neighbouring hubs should deplete bringing about a gap in the system. These assaults are otherwise called "sink gap" assaults.

K.Flooding An aggressor constantly sends association foundation solicitations to a hub in this sort of asset weariness assault. Each of such demands makes the hub allot a few assets to serve every demand. Hold on solicitations by a malevolent hub may deplete the memory and vitality assets of the hub under assault.

L.De-synchronization In this assault, an enemy can manufacture messages containing any control banners or succession quantities of past casings, and transmit them to two associated hubs. These fake messages make the hubs acknowledge as though they have lost their synchronization. Hubs retransmit the accepted missed edges, and if the foe is fit for tireless transmission of manufactured messages then the assets of the hubs will be soon drained. In addition the associated hubs are not ready to share any helpful data amid this assault, as they dig endlessly in synchronization-recuperation conventions.

M.Interrogation A cross examination assault misuses the two-route demand to-send/clear-to-send (RTS/CTS) handshake that numerous MAC conventions use to moderate the shrouded hub issue. An assailant can debilitate a hub's assets by more than once sending RTS messages to evoke CTS reactions from a focused on neighbour hub.

N.Sybil Attack In this fascinating assault, a hub can take different personalities which prompt to the disappointment of the excess instruments of conveyed information stockpiling frameworks in shared systems. Sybil assault works by its property of speaking to various hubs at the same time. The Sybil assault is fit for harming other blame tolerant plans, for example, disparity, multi way steering, directing calculations, information collection, voting, reasonable asset designation and topology support. This assault likewise influences the topographical steering conventions, where the pernicious hub introduces a few characters to different hubs in the system and in this manner has all the earmarks of being in more than one area at once.

O. Selective Forwarding A hub may drop halfway or finish parcels bouncing through it, along these lines irritating the nature of administration in WSN. On the off chance that all parcels are dropped, the neighbouring hubs get to be distinctly suspicious and may consider it to glitch in this manner finding new courses. Noxious

hub can specifically forward information to keep away from doubt. It can drop a portion of the information and passes all other to counteract issues that may emerge concerning its execution. Noxious hubs may just permit the information exchange from some specific hubs, giving them the space to change or stifle information from specific hubs. This sort of assaults turns out to be extremely hard to recognize.

P.Worm gaps Worm openings are framed by vindictive hubs working in various parts of the system. In this assault, the assailant gets messages in one area of system over a low-inactivity interface and sends them to another segment of the system. These messages are then replayed in the other part of the system hence shaping a worm gap in the present structure of the data stream in system. The impression can be negative if the enemy discovers its nearness close to the base stations, giving the removed hubs the acknowledgment that they are in the region of the base stations. Multi-bounce hubs get the idea through wormholes that they are just a single or two hubs far from the base station. Movement streams to the low-inactivity course that the enemy gives to these far off hubs. This may bring about blockage and further retransmissions of the bundles by the authentic hubs, dispersing their vitality.

Q.Hello Flood Attacks At the begin of correspondence, hub needs to declare itself to the system by communicating hi message to their neighbouring hubs. It likewise approves that the hub sending hi message is in the region. Enemy can misuse this component by utilizing a powerful remote connection. It can guarantee each hub in the system that he is their neighbour, therefore beginning correspondence with hubs. As self-evident, by utilizing this assault security of the data is traded off as the aggressor accesses the data stream in the system. On the off chance that some astound plan is utilized by the hubs to give access to any hub asking for association, then a variation of this assault can likewise be connected.

R.Acknowledgement Spoofing Acknowledgments assume an essential part in deciding the nature of administration at any connections and building up further associations in view of the this data. Enemy can modify affirmations to present to any transmitting hub that any frail connection is sufficiently solid for dependable correspondence.

S.Node Replication Attack Sensor hubs have IDs as their personality (and files of their area in geological steering calculations) in the WSN. An enemy can add new hub to the sensor arrange by duplicating the ID of an officially existing hub and doling out it to the malevolent hub. This guarantees nearness of the foe in the system permitting the malignant element to prompt ruinous effects to the sensor arrange. By utilizing the duplicated hub, bundles landing through it can be dropped, misrouted or modified. This outcome in wrong substance of data parcel, loss of association, information misfortune and top of the line to-end idleness. Duplicated hubs at particular area

WSN CHALLENGES

A. **Challenges** In Real Time WSN manages certifiable situations. By and large, sensor information must be conveyed inside time requirements so that suitable perceptions can be made or moves made [5]. Not very many outcomes exist to date with respect to meeting constant necessities in WSN. Most conventions either overlook ongoing or essentially endeavour to handle as quick as would be prudent and trust that this speed is adequate to meet due dates. Some underlying outcomes exist for continuous directing. For instance, the RAP convention [6] proposes another approach called speed monotonic planning. Here a bundle has a due date and a separation to travel. Utilizing these parameters a bundle's normal speed necessity is processed and at every bounce parcels are booked for transmission in light of the most noteworthy speed prerequisite of any bundles at this hub. While this convention addresses constant, no assurances are given. Another steering convention that locations continuous are called SPEED [7]. This convention utilizes input control to ensure that every hub keeps up a normal deferral for parcels travelling a hub. Given this postponement and the separation to go (in bounces), it can be resolved if a bundle meets its due date (in enduring state). In any case, transient conduct, message misfortunes, clog, commotion and different issues cause these assurances to be constrained. To date, the constrained outcomes that have showed up for WSN in regards to continuous issues has been in steering. Numerous different capacities should likewise meet continuous imperatives including: information combination, information transmission, target and occasion location and arrangement, inquiry handling, and security. New outcomes are expected to ensure delicate ongoing prerequisites and that arrangement with the substances of WSN, for example, lost messages, clamour and blockage. Utilizing input control to address both unfaltering state and transient conduct appears to hold guarantee. Managing ongoing more often than not distinguishes the requirement for separated administrations, e.g., steering arrangements need to bolster diverse classes of movement; assurances for the vital

activity and less support for insignificant activity. It is imperative not exclusively to grow ongoing conventions for WSN, yet related investigation procedures should likewise be produced.

Challenges in power administrations: Low-cost organization is one acclaimed preferred standpoint of sensor systems. Restricted processor transmission capacity and little memory are two questionable limitations in sensor systems, which will vanish with the improvement of creation procedures. In any case, the vitality limitation is probably not going to be unravelled soon because of moderate advance in creating battery limit. In addition, the untended way of sensor hubs and dangerous detecting situations block battery substitution as a plausible arrangement. Then again, the reconnaissance way of numerous sensor organize applications requires a long lifetime; along these lines, it is a critical research issue to give a type of vitality proficient observation benefit for a geographic range. A significant part of the momentum looks into spotlights on the most proficient method to give full or halfway detecting scope with regards to vitality protection. In such an approach, hubs are put into a torpid state the length of their neighbours can give detecting scope to them. These arrangements respect the detecting scope to a specific geographic territory as double, it is possible that it gives scope or not. In any case, we contend that, in many situations, for example, combat zones, there are sure geographic areas, for example, the general war room that are a great deal more security touchy than others. In view of the way that individual sensor hubs are not dependable and subject to disappointment and single detecting readings can be effortlessly contorted by foundation commotion and cause false alerts, it is essentially not adequate to depend on a solitary sensor to shield a basic zone. For this situation, it is sought to give higher level of scope in which numerous sensors screen a similar area in the meantime to get high trust in location. Then again, it is needless excess and vitality expending to bolster a similar high level of scope for some non-basic region. Middleware sits between the working framework and the application. On customary desktop PCs and compact figuring gadgets, working frameworks are settled, both as far as usefulness and frameworks. For sensor hubs, nonetheless, the distinguishing proof and usage of suitable working framework primitives is still an examination issue [6]. In numerous present undertakings, applications are executing on the uncovered equipment without a different working framework part. Henceforth, at this early phase of WSN innovation it is not clear on which premise future middleware for WSN can normally be assembled.

APPLICATIONS

There are different applications for WSNs like observing, following, or controlling are talked about underneath.

[1] **Area observing:** Area checking is a typical use of WSNs. It utilizes sensors which distinguishes the occasion to be observed and after that reports to base station. Contingent upon report fitting move is made. [8].

[2] **Environmental checking:** various WSNs have been sent for natural observing. Large portions of these have been fleeting, regularly because of the model way of the activities.

[3] **Water/Wastewater Monitoring:** There are numerous open doors for utilizing remote sensor organizes inside the water/wastewater businesses. Offices not wired for power or information transmission can be checked utilizing mechanical remote I/O gadgets and sensors controlled utilizing sunlight based boards or battery packs.

[4] **Landfill Ground Well Level Monitoring and Pump Counter**: Wireless sensor systems can be utilized to quantify and screen the water levels inside all ground wells in the landfill site and screen drain ate aggregation and expulsion. A remote gadget and submersible weight transmitter screens the filter ate level. The sensor data is remotely transmitted to a focal information logging framework to store the level information, perform counts, or tell faculty when an administration vehicle is required at a particular well. It is run of the mill for drain ate expulsion pumps to be introduced with a totalizing counter mounted at the highest point of the well to screen the pump cycles and to figure the aggregate volume of filter ate expelled from the well. For most current establishments, this counter is perused physically. Rather than physically gathering the pump check information, remote gadgets can send information from the pumps back to a focal control area to spare time and dispose of mistakes. The control framework utilizes this tally data to decide when the pump is in operation, to figure filter ate extraction volume, and to timetable upkeep on the pump.

[5] **Water Tower Level Monitoring:** Water towers are utilized to include water and make water weight to little groups or neighbourhoods amid pinnacle utilize times to guarantee water weight is accessible to all clients. Keeping up the water levels in these towers is imperative and requires steady checking and control. A remote sensor arrange that incorporates submersible weight sensors and buoy switches

screens the water levels in the tower and remotely transmits this information back to a control area. At the point when tower water levels fall, pumps to move more water from the store to the tower are turned on.

[6] **Agriculture:** Wireless sensor systems are utilized for different checking and control applications, for example, keeping up and observing water tank levels, and upheld by charging highlight. Water system robotization empowers more effective water utilize and decreases squander.

[7] Windrow Composting: One of the essential techniques for fertilizing the soil includes utilizing windrows. Treating the soil is the high-impact disintegration of biodegradable natural matter to create compost, a supplement rich mulch of natural soil delivered utilizing sustenance, wood, fertilizer, and additionally other natural material. To guarantee proficient and compelling treating the soil, the temperatures of the windrows must be measured and logged continually. With exact temperature estimations, office directors can decide the ideal time to turn the windrows for snappier fertilizer creation. Physically gathering information is tedious, is impossible consistently, and may uncover the individual gathering the information to hurtful pathogens. Naturally gathering the information and remotely transmitting the information back to a brought together area permits treating the soil temperatures to be consistently recorded and logged, enhancing effectiveness, decreasing the time expected to finish a fertilizing the soil cycle, and limiting human introduction and potential hazard.

[8] **Greenhouse Monitoring:** Green house requires a consistent or endorsed temperature and dampness levels. At the point when these parameters drops beneath particular levels, WSN reports to the nursery administrator by means of email or mobile phone instant message, or direct activating of the applications frameworks, , turn on fans, or the water level by open vents, or control a wide assortment of framework responses.[9]

[9] **Vehicle Detection:** The nearness of vehicles can be identified utilizing Wireless sensor systems. For instance little vehicles like bikes and huge vehicles like prepare.

CONCLUSION

In this paper, we have reviewed an example of steering conventions by considering a few characterization criteria, including area data, arrange layering and in-system preparing, information centricity, way repetition, and organize elements, QoS prerequisites, and system heterogeneity. As included above in this paper WSN is utilized as a part of wide range of utilizations, however the difficulties to WSN are one of a kind, along these lines the outlining of WSN is troublesome so their security plans ought to be considered. A portion of the real assaults on WSN are exhibited here. Remote sensor systems are entering in people to come. The past era has seen numerous new research difficulties being characterized and comprehended. In future we should be prepared to acknowledge numerous more interesting outlines of WSN, more modern assaults and their preventions.

REFERENCES

[1] BhaskarKrishnamachari, Dr. Yang Yu, and V. K. Prasanna Kumar, “Information Processing and Routing in Wireless Sensor Networks”, Chapter 1, World Scientific Publishing, ISBN: 978-981-4476-70-6

[2] QinghuaWang, IlangkoBalasingham, “Wireless Sensor Networks - An Introduction” http://cdn.intechopen.com/pdfs/12464.pdf

[3] Shio K. Singh, M.P. Singh, D.K. Singh, “Routing Protocols in Wireless Sensor Networks –A Survey”, IJCSES: Vol.1, No.2, November 2010,pp63-83

[4] M. YasirMalik,”An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations”, Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management DOI: 10.4018/978-1-4666-0101-7.ch024

[5] Challenges in wireless Sensor Network, Er. Barjinder Singh Kaler# 1 Er.ManpreetKaurKaler# www.rimtengg.com/iscet/proceedings/pdfs/misc/176.pdf

[6] Perrig,A.,Szewczyk,R.,Wen, v., Culler, D.andTygar, J. SPINS: Security protocols for sensor networks

[7] Przydatek, B., Song, D., and Perrig, A. SIA: Secure information aggregation in sensor networks. In Proceedings of the 1st ACM nternational Conference on Embedded Networked Sensor Systems (SenSys 2003) (Los Angeles, Nov (5–7). ACM Press, New York, 2003, 255–265.

[8] E. Altman, T. Basar, T. Jimenez, and N. Shimkin, “ Competitive routing in networks with polynomial costs,” IEEE Trans. Automat. Control, vol. 47, no. 1, pp. 92-96,

[9] N. Bulusu, J. Heidemann, D. Estrin, and T. Tran, "Selfconfiguring localization systems: design and experimental evaluation," pp. 1-31, ACM TECS special Issue on Networked Embedded Computing, Aug. 2002.
[10] S.Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009. [11] Realistic Applications for Wireless Sensor Networks /John A. Stankovic, Anthony D. Wood, Tian He
[11] Some issues and challenges of Wireless Sensor Networks HimaniChawla ,ijarcsse Volume 4, Issue 7, July 2014