IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 20-24

A study of wireless sensor networks-issues and challenges

M. Infant Angel[1], Dr.R.Sudha[2]

[1]Research scholar, Department of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India
[2] Assistant professor, Dept of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India

Abstract :-*. Remote sensor systems (WSN), now and again called remote sensor and actuator systems (WSAN), are spatially dispersed independent sensors to screen physical or ecological conditions, for example, temperature, sound, weight, and so on and to agreeably go their information through the system to a primary area. WSN are assuming an awesome job in the controlling and overseeing conditions in various circumstances and has turned out to be essential piece of research territory. WSN inquire typically ordered into three classes i.e. equipment and programming of the sensors nodes, application zone, and correspondence and security. Reducing vitality utilization in remote interchanges has pulled in expanding consideration as of late. The programming sensor systems and applications to be sent in them is to a great degree testing. It has generally been a blunder inclined undertaking since it requires programming singular nodes, utilizing low-level programming issues and interfacing with the equipment and the system. This viewpoint is presently changing as various abnormal state programming reflections and middleware arrangements are coming into the territory. In this paper survey a different security, vitality effectiveness, control utilization, Biometric similarity issues in WSNs.*

Keywords: - *Biometric, Energy efficiency, Security, Wireless Sensor Network*

I. Introduction

Over the most recent couple of years' remote sensor networks(WSNs) have drawn the consideration of the examination network, driven by an abundance of hypothetical and commonsense difficulties [1]. This dynamic research in WSNs investigated different new applications empowered by bigger scale systems of sensor nodes fit for detecting data from the earth, process the detected information and transmits it to the remote area [2-4]. WSNs are generally utilized in, low transfer speed and defer tolerant, applications running from common and military to ecological and medicinal services checking

WSNs has appeared in Fig.1 for the most part comprise of at least one sinks (or base stations) and maybe tens or thousands of sensor hubs scattered in a physical space. With incorporation of data detecting, calculation, and remote correspondence, the sensor nodes can detect physical data, process unrefined data, and report them to the sink. The sink thus questions the sensor hubs for data. WSNs have a few unmistakable highlights like:

a) Unique system topology
b) Diverse applications
c) Unique activity qualities, and
d) Severe asset imperatives

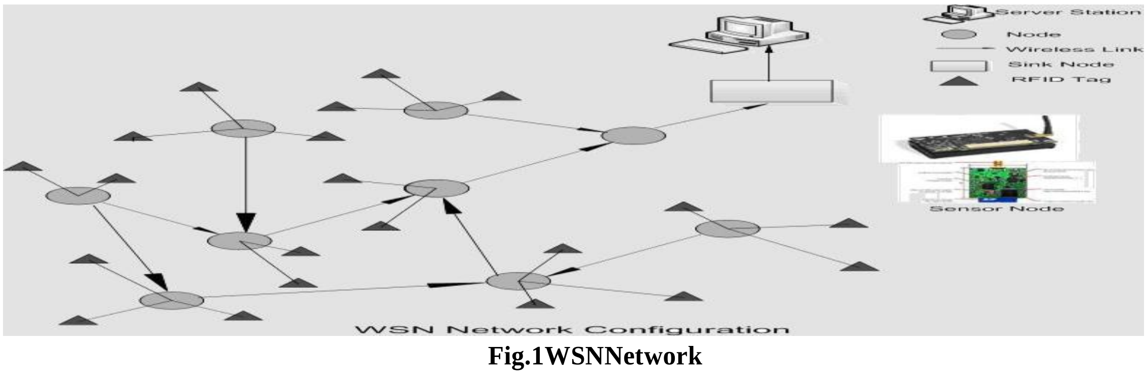

Fig.1WSNNetwork

WSN node is contained low-control detecting gadgets, installed processor, correspondence channel and power module. The inserted processor is by and large utilized for gathering and handling the flag information taken from the sensors. Sensor component creates a quantifiable reaction to an adjustment in the physical condition like temperature, moistness, particulate issue (e.g. CO2) and so on.

The remote correspondence channel gives a medium to exchange the data removed from the sensor hub to the outside world which might be a PC arrange and between hub correspondence [5]. Be that as it may, WSN utilizing IEEE 802.15.4 Wireless Personal Area Network convention (WPAN) or Bluetooth is confounded and exorbitant [10, 18]. Utilizing RFID to actualize remote correspondence is generally basic and shoddy [6]. Zigbee convention can likewise be utilized for correspondence; on the other hand the RS232 standard for remote transmission of information can be received in light of the fact that the information rate of RFID and that of RS232 is same regarding bits every second (bps).

II. Framework Requirements

The framework ought to be:

- **Blame tolerant:** the framework ought to be powerful against hub disappointment (coming up short on vitality, physical decimation, H/W, S/W issues and so on). Some signal system ought to be joined to demonstrate that the hub isn't working legitimately.
- **Adaptable**: The framework should bolster vast number of sensor hubs to provide food for various applications.
- **Long life:** The hub's life-time altogether characterizes the system's life-time and it ought to be sufficiently high. The sensor hub ought to be control effective against the restricted power asset that it have since it is hard to supplant or energize a huge number of hubs. The hub's correspondence, figuring, detecting and impelling activities ought to be vitality effective as well.
- **Programmable**: the reconstructing of sensor hubs in the field may be important to enhance adaptability.
- **Secure**: the hub should bolster the accompanying

a. **Access Control**: to counteract unapproved endeavours to get to the hub.

b. Message Integrity: to recognize and counteract unapproved changes to the message.

c. Privacy: to guarantee that sensor hub ought to encode messages so just those hubs would listen who have the mystery key.

d. Replay Protection: to guarantee that sensor hub ought to give security against foe reusing a bona fide parcel for picking up certainty/arrange get to, man in the center assault can avoidedby time stamped information bundles.

- **Reasonable:** the framework should utilize ease gadgets since the system involves thousands of sensor nodes, labels and mechanical assembly. Establishment and upkeep of framework components ought to likewise be fundamentally low to make its arrangement sensible.

III. Related Work

Attacks:

Raja Waseem Anwar, et al., discussed in this research work, the creators propose a confided in remove vector steering convention (T-AODV) to secure the system of remote sensors from wormhole assaults. The Wormhole assault in WSN can be utilized to misuse directing correspondence in the system by an adversary tuning the messages got in a piece of the system and replaying them in an alternate part. A plan in light of certainty AODV proposed to assess neighbouring trust nodes. The blueprint diminishes generally organize delay and enhances arrange execution within the sight of a distinctive number of vindictive nodes [1].

R. W. Anwar, et al., analysed in this short survey, the security issues and physical attacks were examined. The methodology comprises in arranging and looking at physical assaults their properties, for example, their procedures and their belongings, lastly their related identification and protection systems against these assaults to treat them in an autonomous andthorough way [2].

H. Ehsan and F. A. Khan, et al.,explained in his work the re-enactment of the creators demonstrates that flooding assaults, for example, flooding RREQ and hi surge incredibly increment the directing over-burden of the convention. Street alteration attackssuch as the deplete opening what's more, the dark gap are deadly and genuinely influence the proficiency of the bundles and decrease the stream to unsatisfactory reaches [3].

M. Medadian,et al.,discussed in this work, the steering security issues of MANET are talked about. One sort of assault, the dark opening, which can be effortlessly sent against the MANET, is portrayed. The level of parcels got under the proposed technique is higher than that of the AODV within the sight of a dark opening helpful assault. The arrangement is re-enacted utilizing the worldwide versatile test system and is found to accomplish the required security with insignificant postponement and overhead [4].

Denial of Service (DoS): Blackert,Wang,et al.,analysed in this work is delivered by the inadvertent disappointment of hubs or noxious activity. The least complex DoS assault endeavors to debilitate the assets accessible to the casualty hub, by sending additional superfluous bundles and in this manner keeps real system clients from getting to administrations or on the other hand assets to which they are entitled. DoS assault is implied not just for the enemy's endeavor to subvert, disturb, or crush a system, yet additionally for any occasion that decreases a system's ability to give an administration. In remote sensor systems, a few kinds of DoS assaults in various layers may be performed. At physical layer the DoS assaults could be sticking and altering, at interface layer, impact, depletion, shamefulness, at arrange layer, disregard and eagerness, homing, confusion, dark openings and at transport layer this assault could be performed by noxious flooding and desynchronization. The systems to counteract Do assaults incorporate installment for arrange assets, pushback, solid validation and recognizable proof of activity [5, 6].

Energy:

M.H.Anisi,W. Dargie,et al.,discussed in this work Sensors require control for different tasks. Energy is devoured in information accumulation, information handling, and information correspondence; likewise, persistent tuning in to the medium for unwavering activity requests a huge measure of energy by hub segments (CPU, radio, and so forth.) regardless of whether they are sit without moving. Batteries giving forceshould be changed or energized after they have been expended. Once in a while it winds up hard to revive or change the batteries in view of statistic conditions. The most vital research challenge for the WSN specialists is to outline, create and execute energy proficient equipment.[7,8].

R.Sudha, et al., discussed in this paper the most influencing factor to obtain such efficiency with respect to energyconsumption. Selection for optimized routing with the betterload balancing is determined and the enhanced uniformclustering of the sensor nodes is performed using the K-Nearest Neighbour algorithm with the best possible routeselection using the tree clustering techniques [19].

Equipment and Software Issues:

P. Zhang,A. Crnjin. R. Sugihara, analysed in this Sensor Networks comprises of countless hubs. It is favored just if the hub is modest. Streak memory is encouraged to be utilized in sensor organizes as it is modest. The focal preparing unit of sensor node decides energy utilization and computational abilities of a hub. Keeping in mind the end goal to give the adaptability to CPU execution, extensive number of smaller scale controller, microchip what's more, FPGAs (field programmable door exhibits) are accessible.

For sparing of intensity, microcontroller ought to have three states-dynamic, rest, sit without moving. Further energy utilization for FPGA can't be diminished; In addition isolate square can't be made for it. Sending of FPGA to lessen control utilization is an awesome test. In this way, other than being financially savvy, different issues resemble the radio range of one sensor hub must be high extending from 1 to 5 km. Radio range is basic for guaranteeing system availability and information gathering in a system as the condition being checked might not have an introduced framework for correspondence. Programming in WSN ought to be equipment autonomous other than being light and less energy devouring. Calculations and conventions ought to be planned in such a route, to the point that they ought to be less intricate and be supportive in decreasing energy utilization [9, 10, 11].

Self Management:

.K. Sohrabi , .S. Vaidyanathan ,et al., implemented in Wireless sensor organizes once conveyed ought to have the capacity to work with no human intercession. It ought to have the capacity to deal with the arrange design, adjustment, upkeep, furthermore, repair without anyone else [12, 13].

Security:

- P. Mohanty , M.K. Jain , et al., discussed in this paper Security is very testing issue as WSN isn't just being conveyed in combat zone applications yet in addition for reconnaissance, building observing, robber cautions and in basic frameworks for example, airplane terminals and clinics. Privacy is required in sensor systems to ensure data going between the sensor hubs of the system or then again between the sensors and the base station; else it might bring about listening in on the correspondence. In sensor systems, it is basic for every sensor hub and the base station to have the capacity to check that the information got was truly sent by a confided in sender and not by a foe that deceived genuine hubs into tolerating false information [14, 15].

- R.Sudha, et al., analysed in this paper devised a new biometric fusion based trusted anonymous secured routing protocol which assures prevention against such attacks. More specifically, the route request packets were authenticated by an iris fused with DNA coding to generate a dynamic complex group signature and to secure beside possible active attacks exclusive of presenting the node identities. In addition this work also prevented revealing real destination to intermediate nodes by adapting key-encrypted pairing onion. Simulation results confirmed the efficiency of the biometric fusion based trusted anonymous secured routing protocol with enhanced performance as evaluated with the existing protocols [21].
- A.K. Pathan ,et al., implemented a false information can change the manner in which a system could be anticipated. Trustworthiness of information ought to be kept up. Information ought not change and exact information must reach at client end. Distinctive sorts of dangers in sensor systems are ridiculing and modifying the steering data, uninvolved data gathering, hub subversion, sinkhole assaults, Sybil assaults, Refusal of administration assault and sticking [16].
- R.Sudha, et al., discussed in this work each sensor node conserves its energy by switching between Sense/Receive (or) off states only until it senses an event in its proximity, after which it enters the transmit state to transmit the event information and also shows that the power saved in each node outperforms the power saved in any other previously known protocols and this work also shows that it is possible to minimize about 51% of the power and maintain 100% coverage and connectivity.It increase the life time of each sensor network by increasing the number of sensor nodes as well as the security of nodes using RSA algorithm [20].

Constrained Memory and Storage Space:

J. Polastre ,et al., evaluate a sensor is a modest gadget with just a little measure of memory what's more, storage room for the code. With a specific end goal to manufacture an compelling security system, it is important to constrain the code size of the security calculation. For model, one basic sensor compose [17] has a 16- bit, 8 MHz RISC CPU with just 10K RAM, 48K program memory, and 1024K blaze stockpiling. With such a restriction, the product worked for the sensor should likewise be very little.

Adaptation to internal failure:

.M.K. Jain ,et al., examined in this paper Sensor system ought to remain utilitarian regardless of whether any hub comes up short while the system is operational. System ought to have the capacity to adjust by changing its network if there should arise an occurrence of any blame. In that case, well-proficient steering calculation is connected to change the general setup of arrange [15].

In-network Processing:

D. Ganesan ,et al.,discussed in this paper to lessen correspondence costs a few calculations evacuate or lessen nodes repetitive sensor data and abstain from sending information that is of no utilization. As nodes can assess the information they forward they can quantify midpoints or directionality for instance of readings from different hubs.For instance, in detecting and checking applications, it is for the most part the case that neighboring sensor nodes checking an ecological component commonly enlist comparable values. This sort of information excess due to the spatial connection between's sensor perceptions moves the methods for in-arrange information total and mining [18].

IV. Conclusion

Different research issues and difficulties relating to WSNs that have been experienced by the analysts are exhibited in this work. Sensor systems have numerous challenges, yet its immense number of utilizations draws scientists to explore more into it. An exhaustive examination uncovers that WSN is a multidisciplinary field. On one side it requests versatile design from the equipment architects to guarantee great Quality of administration; on the opposite end, it requests vitality proficient calculations and conventions from programming designers to make them handy furthermore, possible. Vitality sparing is one of the primary concern and different research issues at last comes down to limit it definitely. By and large, an all encompassing methodology and composed exertion is wanted from the examination society to make WSNs a reality. These endeavors are worth as WSNs hold a huge potential for the general advantage of humankind and to make inescapable figuring a probability in the coming occasions.

References

[1]. Raja Waseem Anwar, Majid Bakhtiari, Anazidazainal, Abdul Hanan Abdullah And KashifNaseerQureshi,(2015): Enhanced Trust Aware Routing Against Wormhole Attacks In Wireless Sensor Networks, International Conference On Smart Sensors And Application, IEEE.

[2]. R. W. Anwar, M. Bakhtiari, A. Zainal, A. H.Abdullah, and K. N. Qureshi,(2014):Security Issues and Attacks in Wireless Sensor Network, World Applied Sciences Journal, vol. 30, pp. 1224-1227,.

[3]. H. Ehsan and F. A. Khan,(2012): Malicious AODV: implementation and analysis of routing attacks in MANETs, in Trust, Security and Privacy in Computing and Communications (Trust Com), 2012 IEEE 11th International Conference on,, pp. 1181-1187.

[4]. M. Medadian, A. Mebadi, and E. Shahri, (2009,): Combat with Black Hole attack in AODV routing protocol," in Communications (MICC), IEEE9th Malaysia International Conference on, pp. 530-535.

[5]. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., “Analyzing interaction between distributed denial of service attacks and mitigation technologies”, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[6]. Wang, B-T. and Schulzrinne, H., “An IP traceback mechanism for reflective DoS attacks”, Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[7]. M.H. Anisi, A.H. Abdullah, and S.A. Razak, “EnergyEfficient Data Collection in Wireless Sensor Networks”, Wireless Sensor Networks, vol. 3, 2011, pp. 329-333.

[8]. W. Dargie, and C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice. WileyBlackwell,2010.

[9]. P. Zhang, M. Sadler, A. Lyon and M. Martonosi, “Hardware Design Experiences in ZebraNet”, Proc. 2nd International Conf. Embedded Networked Sensor Systems (SenSys), Nov. 2004, pp. 227-238.

[10]. A. Crnjin, “Software Issues in Wireless Sensor Networks”, Wireless sensor networks: concepts, multidisciplinary issues, and case studies, Belgrade, 2009, pp. 1-9.

[11]. R. Sugihara and R.K.Gupta, “Programming Models for Sensor Networks: A Survey”, ACM Transactions on Sensor Networks, vol. 4, no. 2, 2008, pp. 8:1-8:29.

[12]. K. Sohrabi, J. Gao, V. Ailawadhi and G.J. Pottie, “Protocols for self organization of a wireless sensor networks”, IEEE Personal Communications, vol. 7, no. 5, 2000, pp. 16-27.

[13]. S. Vaidyanathan and M. Vaidyanathan, “Wireless Sensor Networks- Issues & Challenges”, Information Systems: Behavioral& Social Methods eJournal, 2011, pp. 7.

[14]. P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, “Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey”, Journal of Theoretical and Applied Information Technology, vol. 13, no.1, 2005-2010, pp. 14-27.

[15]. M.K. Jain, “Wireless Sensor Networks: Security Issues and Challenges”, International Journal of Computer and Information Technology, vol. 2, no. 1, 2011, pp. 62-67.

[16]. A.K. Pathan, “Security in Wireless Sensor Networks: Issues and Challenges”, Proc. 8th International Conf. Advanced Communication Technology (ICACT’08), vol. 2, 2006, pp. 1043-1048.

[17]. J. Polastre, R. Szewczyk and D. Culler, “Telos: enabling ultra-low power wireless research”, Proc. 4th International Symp. Information Processing in Sensor Networks (IPSN’05), Apr. 2005, pp. 364 – 369.

[18]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly resilient, energy efficient multipath routing in wireless sensor networks”, Proc. 2nd ACM International Symp. Mobile Ad Hoc Networking and Computing (MobiHoc’01), Oct. 2001, pp. 251–254.

[19]. R.Sudha, M.Devapriya, “An Energy saving approach in wireless body sensor networks for Health care monitoring” in International Journal of Applied Engineering Research with ISSN 0973-4562 Volume11, Number 7 (2016) pp 4797-4802.

[20]. R.Sudha, C.Nandhini, ”An Energy Efficient Secure Multipath RoutingAlgorithm for Wireless Sensor Network” in International Journal of Science and Research (IJSR) with ISSN (Online): 2319-7064Volume 4 Issue 7, July 2015,pp 245-248.

[21]. R.Sudha, M.Devapriya, “Enhanced Bio-trusted anonymous authentication routing technique of wireless body area network” in Biomedical Research2016; Special Issue: S276-S282, ISSN 0970-938X.