Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

A Detailed Survey on Challenges, Applications and Attacks in Wireless Sensor Network

[1]Dr Shubhra Saxena, [2]Shumaila Akbar

[1]Assistant Prof. SKIT Jaipur
[2]Assistant Prof. CITM Jaipur

Abstract— *Due to wireless mode of communication, sensors could be deployed at any corner and could be easily monitored from different locations. WSN have much less maintenance, economical and without difficulty deployable in assessment to its counter elements. In WSNs, the energy is scattered while detecting, handling, transmitting or getting information. The detecting subsystem is utilized for data obtaining. A sensor network is an infrastructure produced from sensing, computing and conversation elements that provide a consumer the potential to observe instrument and react to events and phenomena in a specified environment. To design and develop protocols or algorithms some challenges are needed to be understood. It is infrastructure less which makes them vulnerable to various attacks and it should be known by the users to reduce its impact and maintain the efficiency of the network.*

Keywords—*Wireless Sensor Network, Communication, Energy, Attacks, Security.*

I. INTRODUCTION.

WSN's is the most unmistakable existing wireless technology wherever all through the world. In contrast with different wireless remorse procedures, for example, specially appointed system or work organizes and so on. Sensor network has its own limitation in exchanging data from a measuring point to the destination. In WSN, sensor units are conveyed at different areas in the system, and they ceaselessly measures the physical parameters, for example, temperature, mugginess, weight and so on. Commonly, a sensor node is a small device that incorporates four principle parts in particular a detecting unit, microcontroller unit, correspondence unit and a power source. The significant preferred standpoint of such network is the arrangement of nodes at any area and trade of data by means of strong intermediates nodes which go about as routers to switch data. From one to other node. Due to wireless mode of communication, sensors could be deployed at any corner and could be easily monitored from different locations.

WSN have less maintenance, economical, and easily deployable in contrast with its counter parts. Application situations for WSNs regularly include battery-powered nodes which are active for a long period, without human control after beginning arrangement. Without energy efficient systems, a node would deplete its battery inside couple of days.
These protocols are comprehensively characterized in to four classes i.e. in view of Network Structure, Communication Model, Topology and Reliable Routing. This paper gives an entire review on the energy-efficient routing protocols for WSNs in view of Network structure. The focus is on the techniques these protocols use in order to route messages, based on the energy they consume so that the lifetime of the network is extended [1].

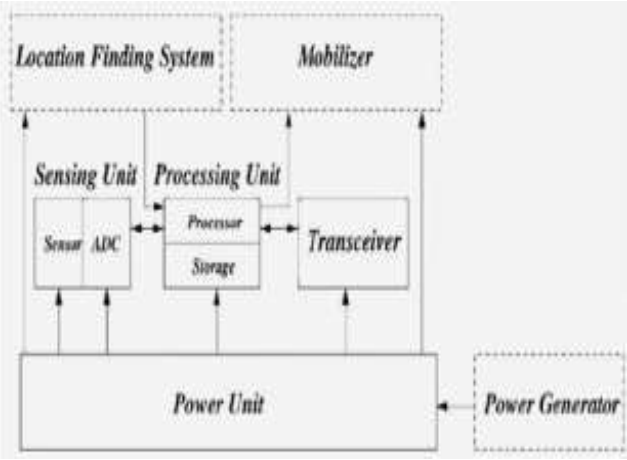

Fig 1.1 WSN

In WSNs, the energy is scattered while identifying, dealing with, transmitting or tolerating data. The detecting subsystem is used for data securing. Clearly limiting data expelled from transducer will save imperativeness of constrained sensors.

Different trial comes about confirm that correspondence subsystem is a noticeable wellspring of energy scattering. Indeed, even in correspondence, substantial measure of energy is squandered in states, for example, impact, catching, control parcel overhead, sit without moving tuning in, impedance and so forth [2] ,[3], [4].

II. APPLICATIONS OF WIRELESS SENSOR NETWORK

Wireless sensor networks enable a paradigm shift in the science of monitoring, and constitute the foundation of a broad range of applications related to security, surveillance, military, medical, and environmental monitoring. They can altogether enhance the exactness and scientific of logical estimations of physical phenomena since substantial quantities of sensors can straightforwardly be sent where tests are occurring. In wireless sensor network the idea of miniaturized scale detecting and remote association of sensor nodes constitute the establishment of an expansive scope of utilization identified with military observation, security condition checking, restorative, home and other business application regions. They can fundamentally enhance the exactness and thickness of logical estimations of physical wonders since substantial number of sensor can specifically be sent at places. Where experiments are failing. Some existing real life applications are given below.

1) Military Applications

Sensor network look into was at first determined by military applications, for example, reconnaissance and adversary following. Since sensor networks depend on the thick organization of sensor nodes, pulverization of a few nodes by threatening activities does not influence a military operation as much as destruction of traditional sensor, which improves sensor systems idea an approach for front lines. To screen well disposed powers, hardware and ammo pioneers and commandants can always screen the status of agreeable troops, the condition and the accessibility of gear and ammo in a combat zone by the utilization of sensor networks. In war zone observation, basic landscapes approach and ways can be quickly secured with sensor systems and nearly looked for the exercises of the opposing forces.

2) Environment Observation

Environment monitoring networks span large geographic areas to monitor and forecast physical processes such as environment pollution, forest fire detection and flood detection and so forth. In forest fire detection, sensor nodes might be deliberately, arbitrarily and densely sent in forest. Sensor nodes can transfer the correct inception of the fire to the end utilizes before the fire is spread. A few sorts of sensors are conveyed for precipitation, water level and climate sensor. The sensors supply data to the unified database predetermined.

3) Precision Agriculture

They are also helping in strategic planning and counter measures to increase the yield of the crop.

4) Medical Applications

In medical, sensor networks are used for tracking and monitoring doctors and patients inside a hospital. Every patient has little and light weight sensor nodes connected to them. Doctor may likewise convey a sensor node which enables different specialists to find them inside a hospital. Sensors are greatly valuable in expire analysis and checking. Biosensors are embedded in the human body to screen the patient's physiological parameters, for example, heart beat or blood pressure. The data so gathered is sent frequently to caution the concerned specialist on locatiosn of an irregularity. Such a game plan gives patients a more prominent flexibility of development as opposed to being always restricted to the healing center bed. Fast headways in MEMS innovation has made bio-sensors so complex as to empower adjust recognizable proof of hypersensitivities and related conclusion.

5) Habitat Monitoring

Researchers in the life sciences are ending up progressively worried about activities of birds, little animals and insects. WSNs along these lines can be utilized to accumulate data on the natural surroundings of creatures without irritating them.

6) Home Automation

As technology progresses, smart sensor nodes and actuators are utilized as a part of utilizations, for example, vacuum cleaners, microwave oven and refrigerator. These sensor nodes inside the local gadgets can interact with each other and with the outside network by means of the internet or satellite. They allow end users to manage home devices locally and remotely more easily.

7) Other Commercial Applications

Sensors can be used in building for detecting and controlling of fire and smoke. In case of a fire in building, the deployed sensor network can track and scan the direction in which fire is expanding. Also sensors can be used to monitor the vibration in the building that can damage the structure.

8) Disaster Management

The early cautioning framework in light of WSN can be dependably sent in regions with high danger of disasters. The utilization of WSN promises to give continuous data of the hazardous situation to protect groups making coordination and arranging more compelling. Area data of casualties, rescuers and questions in the disaster is essential for the protect operations. It has been realized that, for an operationally compelling disaster management detecting, monitoring and decision-making ought to be incorporated consistently. Timely and refreshed debacle data is critical for proficient reaction and successful activities; it will help disaster managers with making better decisions and take activities in time. Fig. 2 shows the application of wireless sensor network [5].

Fig 1.2 Applications of WSNs

III. CHALLENGES OF WSN

With the continued advancement in micro electro mechanical systems the miniaturization and increased communication capabilities of sensors has empowered their omnipresent and imperceptible arrangement anyplace whenever. A sensor network is a foundation involved detecting (measuring), figuring and correspondence components that give a client the capacity to watch instrument and respond to events and phenomena in a specified environment. To design and develop protocols or algorithms some challenges are needed to be understood [5]. These major challenges are summarized below:

a) Limited Functional Capabilities

A sensor node has low end processor, small memory and small amount of stored energy. This limits many of the functional capabilities in terms of processing and communication.

A good algorithm should make utilization of shared resources inside an organizational structure, while considering the confinement on individual node capacities.

b) Limited Energy

A sensor node has constrained energy storage. Hence, effective utilization of this energy will be crucial in deciding the scope of use for these sensor networks. In most cases, renewing energy is not feasible or even impossible. Sensors are usually unattended in the field. The limited energy in sensor nodes must be considered as proper consumption or utilization that can reduce the overall energy uses in a network.

c) Network Lifespan

Limited resources and energy in sensor nodes results in limited lifespan in a network. Ideally, a network should become ineffective only when all nodes become exhausted. In reality, the lifespan of a sensor network is the minimum time upto which the network is functionally effective. A network is functionally effective, if it can monitor the entire sensor field

and collect the sensed data with a predefined quality of service (QOS). Proper techniques should attempt to reduce the energy usage and thereby increase network lifetime.

d) Scalability

Sensor nodes conveyed in a detecting zone ought to be optimal. To suit some more nodes later on, network scalability is one of principle obstacles to accomplish this goal. Scalability in the sensor organize shows the capacity to deal with developing measures of work in a powerful way and be readily enlarged [6].

e) **Redundancy**

Because of the frequent node failures and unavailability of failed nodes, Absence of worldwide distinguishing proof Due to extensive number of sensor nodes in a sensor organize the worldwide global identification (GID) is for the most part impractical. Despite the fact that at times, the Global Positioning System (GPS) [7] gives situating data to sensor nodes yet it requires observable pathway to a few satellites, which is by and large not accessible within working, underneath thick foliage, submerged, when stuck by a foe or amid MARS investigation and so forth.

f) Storage, Search and Retrieval

The sensor network can produce a large volume of raw data such as continuous time-series of observations over all points in space covered by the network. Since the data source is continuous traditional database are not suitable for WSNs.

g) Production Cost

The cost of a single node is critical to legitimize general cost of the network; since the sensor networks comprise of an expansive number of sensor nodes consequently cost of every sensor node must be kept low.

a) In- network Processing

As a rule transport conventions utilized as a part of wired and In general transport protocols used in wired and wireless networks [8] Be that as it may, in WSNs data can be altered or intermediate nodes so as to expel excess of data. The previous solutions did not accommodate concept of in network processing, called data aggregation or diffusion in WSNs.

b) Latency

Latency refers to delay from when a sender sends a packet until the point that the packet is effectively received by the receiver. The sensor data has a temporal time interval in which it is substantial, since the idea of the earth changes continually, it is in this manner essential to receive the data in an opportune way.

c) Fault tolerance

Sensor nodes are delicate and they may fail because of consumption of batteries or destruction by an outer occasion. Understanding a blame tolerant operation is basic, for fruitful working of the WSN, since defective segments in a network prompts lessened throughput, accordingly diminishing productivity and execution of the network.

IV. SECURITY ISSUES IN WSN

I. **Data Integrity:** It is very crucial in sensor network to ensure the reliability of the data. It guarantees that data packets that are gotten by the destination are precisely the ones sent by the sender and any one can't change that packet in the middle.

II. **Data Confidentiality:** Confidentiality means to protect data during communication in a network to be understood other than intended recipient. Cryptography techniques are used to provide confidentiality. It is the one of the most important issue in network security.

III. **Data Availability:** It ensures that the services are constantly accessible in the network even under the attack, for example, Denial of Service attack (Dos). Availability is of primary importance to maintain an operational network. Accessibility guarantees that a sensor node remains constantly dynamic in the network to satisfy the usefulness of the network.

IV. **Data Authentication:** It ensures that the data received by beneficiary has not been altered amid the transmission. It is accomplished through symmetric or deviated instruments where sender and collector nodes share secret keys.

V. **Data Freshness**: It guarantees that the data received by the collector is latest and fresh data and no enemy can replay the old data. It is achieved by using mechanisms like nonce or adding timestamp to each data packet [9].

V. VARIOUS WSN ATTACKS

- **Data integrity and confidential related attacks**: In this sort of attack, endeavors to reveal or compromise the unwavering quality and privacy of data contained in the transmitted packets.

- **Denial of Service (DOS) Attack:** Denial of Service assault endeavors to make a network unavailable to its real users. An attacker alters the data before it is perused by sensor nodes, in this manner bringing about off base readings and in the end prompting a wrong decision. This by and large targets physical layer applications where sensor nodes are found.

- **Node Capture Attack:** The attacker may likewise endeavor to extricate critical cryptographic keys like a gathering key from wireless nodes which are utilized to ensure interchanges in many wireless networks.

- **Eavesdropping attack:** To eavesdrop is to covertly catch an individual discussion over a secret correspondence in an unauthorized way. In eavesdropping data isn't influenced however its protection is compromised.

- **Service accessibility and bandwidth capacity utilization attacks:** These attacks essentially plan to demolish the sending ability of sending nodes or expend deficiently accessible bandwidth; they are more probable identified with accessibility of service and bandwidth consumption.

- **Flooding Attack:** An attacker utilizing this sort of attack typically sends a substantial number of packets to the casualty or to an entrance point to maintain a strategic distance from the casualty or the whole network from setting up or proceeding with communications.

- **Jamming (Radio Interference) Attack:** attacker can excellently cut off the connection among nodes by imparting consistent radio signals so other approved clients are not permitted to get to a specific frequency channel.

- **Replay Attack:** In replay attack, a substantial information transmission is falsely rehashed or deferred either by the originator or by an attacker, as a piece of masquerade attack by an IP packet substitution. An attacker duplicates a sent bundle and conveys the duplicates consistently to the casualty keeping in mind the end goal to debilitate the cradles of the casualty or power supplies and access indicates all together disgrace network performance.

- **Selective forwarding attack:** This attack is now and again called Gray Hole attack. In a straightforward type of particular sending, malicious nodes attempt to end the packets in the network by declining to forward or drop the messages going through them. There are different types of specific forwarding attack. In one type of the specific sending, the malicious node can specifically drops the packets that are originating from a specific node or a gathering of nodes.

- **Identity related attacks** when all is said in done, these attacks collaborate with eavesdropping attacks or other network-sniffing software to accomplish powerless MAC and network addresses. They focus on the verification element.

- **Impersonate attack:** An attacker emulate another node's identity (either MAC or IP address) to set up an association with or dispatch different attacks on a sufferer; the attacker may likewise utilize the casualty's personality to build up an connection with different nodes or dispatch other attacks for the benefit of the victim.

- **Sybil attack:** The attacker can imitate other nodes identities or plainly create numerous random identities in the MAC and/or network layer.

VI. LITERATURE SURVEY

Rong Du, et al. [2017] in this paper, such a trouble is formulated as an integer optimization whose solution is challenging due to the binary choice variables and non-linear constraints. To resolve the hassle, an method based totally on two steps is proposed. First, the essential situation for which the WSN is immortal is established. Based on this result, an algorithm to solve the node deployment problem is developed. Then, the optimal WET scheduling is given by a scheduling algorithm. The WSN is appeared to be unfading from a networking perspective, given the optimal deployment and WET scheduling [10].

DINA S. DEIF et al. [2017] in this paper, the issue of sending a WSN with a wonderful minimal phase of constancy in any event organization esteem is tended to. This hassle is wrote the base esteem reliability confined sensor node sending issue (MCRC-SDP). The MCRC-SDP is ended up being a NP-Complete. An ACO algorithm joined with a nearby search heuristic is proposed as a course of action. Extensive experimental results uncover the adequacy of the proposed technique in finding high-quality solutions for the hassle [11].

Cristina Albaladejo Perez et al. [2017] this paper gives the arrangement of an ad hoc WSN device and a direct software application for Mar Menor monitoring the usage of a float structure with sensors, energy harvesting, and trades organize. The take at invests noteworthy energy in the oceanographic interest of the chose marine region, data of network association, the custom-designed sensor nodes, and the effects of gadget operation [12].

Salgotra et al. [2017] this paper proposes new editions of FPA using new mutation operators, dynamic switching and progressed local search. A complete evaluation of proposed algorithms has been done for distinct population sizes for optimizing seventeen benchmark problems. The best form among these is adaptive Lévy flower pollination algorithm (ALFPA) which has been moreover contrasted and the famous algorithms like artificial bee colony (ABC), DE, BA and GWO. Numerical outcomes show that ALFPA gives propelled general execution for general benchmark highlights [13].

Shreshtha Misra, et al. [2016] in this paper our have exhibited different clustering approaches utilized as a part of WSN. Right off the bat, we have arranged the protocol utilized as a part of WSN as Protocol Operation (PO), Network Structure (NS) and Path Establishment (PE). Besides, we have given an expansive outline of the bunch based steering convention utilized as a part of WSN as square cluster, chain cluster and lattice group. We have additionally thought about different clustering routing protocols in view of various characteristics and furthermore talked about the different issues in these routing protocols [14].

Sekhar et al. [2016], in this paper, a protocol in view of open key cryptography for external agent authentication and session key foundation has been proposed. An outer agent imparts through an open key encryption method with a base station, which speaks with sensor nodes through sharing of a private key. The process for this protocol is broken down into three phases: registration, authentication and session key establishment [15].

Praveena et al. [2016], in this paper, MES V-II proposes a kind of symmetric key encryption. This algorithm, created by Nath et al., utilizes the TTJSA and DJSA algorithms in a randomized strategy. In this approach, a generalized and adjusted Vernam figure strategy is utilized with various piece sizes and keys for each square. As an extra security model for this calculation, criticism is additionally added to this technique. After the immediate stage encryption is finished, the whole document is separated into two traded parts and the adjusted Vernam figure strategy with criticism and another key will be rehashed. Rehashing this whole operation various circumstances brings about a framework that is very secure [16].

Navin et al. [2015], in this paper, the principal level will be begun with an interleaving technique. Second, the estimation of a pseudo-random number generator is seeded. Third, a number bank is conveyed at first. The last level is begun by applying operations to the number bank [17].

Celestine et al. [2015], in this paper, a flooding strategy routing technique is presented that relies upon dummy data sources. The primary thought behind this method is that every node can be considered as a dummy data source that sends genuine data subsequent to detecting an occasion to the goal node; the majority of this current node's neighbor nodes will get dummy data. Despite the fact that this approach has the benefit of making it troublesome for a foe to recognize the genuine packets and dummy ones, it leads to dummy traffic and power consumption as a result of this. A novel solution is proposed by using variable sized dummy packets. The dummy packets will differ in size from the real packets, thus saving energy; however, an adversary will still find it difficult to distinguish the real packet from the dummy ones [18].

Markert, et al. [2015], in this paper, the utilization of a honey pot structure for WSNs is appeared to give the capacity to investigate to security weaknesses, vulnerabilities and breaches. This proposed approach, in any case, remains a model that necessities additionally testing to evaluate its adequacy as an entire framework for recognizing genuine network attacks and different attacks. Another side effect of this technique is related to the power consumption of the honey pot sensor nodes. This technique does not apply to other security concerns so should be integrated with other solutions [19].

VII. CONCLUSION

With the continued advancement in micro electro mechanical systems the miniaturization and increased communication capabilities of sensors has empowered their pervasive invisible deployment anyplace whenever. There are a couple of terms identified with the essentialness profitability on WSN and they are used to survey the execution of the routing protocols. WSN have less support, economical, and effectively deployable in contrast with its partners. Application

situations for WSNs frequently include battery-fueled nodes which are dynamic for a long stretch, without human control after initial deployment.

References

[1] Ramesh Patil1 , Dr.Vinayadatt V. Kohir "Energy Efficient Flat and Hierarchical Routing Protocols in Wireless Sensor Networks: A Survey" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 6, Ver. I (Nov.-Dec .2016), PP 24-32.

[2] P. Minet, "Energy efficient routing", in Ad Hoc and Sensor Wireless Networks: Architectures: Algorithms and Protocols.Bentham Science,2009.

[3] L. Alazzawi, A. Elkateeb, "Performance Evaluation of the WSN Rout-ing Protocols Scalability," Journal of Computer Systems, Networks, and Communications, 2008, Vol. 14, Issue 2, pp. 1-9.

[4] L. Junhai, X. Liu, Y. Danxia, "Research on Multicast Routing Protocols for Mobile ad-hoc Networks," Computer Networks, 2008, Vol. 52, Issue 5, pp. 988-997.

[5] SANJEEV KUMAR GUPTA , POONAM SINHA "Overview of Wireless Sensor Network: A Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[6] Wassim Masri, Zoubir Mammeri, "Middleware for Wireless Sensor Networks: A comparative Analysis", IFIP International Conference on Network and Parallel Computing Workshops, September 18-21, 2007, pp. 349-356.

[7] C.C. Shen, C. Srisathapornphat, C. Jaikaeo, "Sensor Information Networking Architecture and Applications", IEEE Personal Communications, August 2001, pp. 52-59.

[8] P. Bonnet, J. Gehrke, and P. Seshadri, "Towards Sensor Database Systems," in proceedings of 2nd Int'l Conf. on Mobile Data Management (MDM'01), 2001, pp. 314–810.

[9] [9]Aditya Sharma, Garima Tripathi, Md Sohail Khan, Kakelli Anil Kumar "A Survey Paper on Security Protocols of Wireless Sensor Networks" International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 08 | Nov-2015.

[10] Rong Du, Carlo Fischione, Ming Xiao "Joint Node Deployment and Wireless Energy Transfer Scheduling for Immortal Sensor Networks" 2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks

[11] DINA S. DEIF, AND YASSER GADALLAH, "An Ant Colony Optimization Approach for the Deployment of Reliable Wireless Sensor Networks" Received May 15, 2017, accepted May 29, 2017, date of publication June 5, 2017, date of current version June 27, 2017.

[12] Cristina Albaladejo Perez, Fulgencio Soto Valles, Roque Torres S ´ anchez, Manuel Jim ´ enez Buend ´ ´ıa, Francisco Lopez-Castej ´ on, and Javier Gilabert Cervera "Design and Deployment of a Wireless Sensor Network for the Mar Menor Coastal Observation System" 0364-9059 © 2017 IEEE.

[13] Rohit Salgotra, Urvinder Singh, "Application of Mutation Operators to Flower Pollination Algorithm", *Expert Systems With Applications* (2017), DOI: 10.1016/j.eswa.2017.02.035, 23 February 2017

[14] Shreshtha Misra, Rakesh Kumar "' A Literature Survey on Various Clustering Approaches in Wireless Sensor Network" A Literature Survey on Various Clustering Approaches in Wireless Sensor Network" 978-1-5090-3210-5/16/$31.00 © 2016 IEEE.

[15] Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. in Computer Communication and Informatics (ICCCI), 2016 International Conference on. 2016. IEEE.

[16] Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensor networks using MES VU. in Intelligent Systems and Control (ISCO), 2016, 10th International Conference on. 2016, IEEE

[17] Navin, A.H., et al. Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network. in Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. 2015, IEEE.

[18] Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. 2015, IEEE.

[19] Markert, J. and M. Massoth. Honeypot framework for wireless sensor networks. in Proceedings of International Conference on Advances in Mobile Computing & Multimedia. 2015.

