International Journal of Computer Science Engineering & Technology
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

CHALLENGES OF WIRELESS SENSOR NETWORK SECURITY REQUIREMENTS AND ARCHITECTURE

[1] B. yazhini
[1] Assistant Professor,
[1] PG & Research Dept of Computer Science,
[1] Hindusthan College of Arts & Science.

Abstract: Wireless Sensor Network (WSN) is an exceptional sort of ad-hoc network. WSNs are utilized as a part of numerous basic applications like military and surveillance, habitat monitoring, and so on. Security has been a noteworthy worry in these networks because of confinements of assets in the sensor nodes and less human mediation amid its activity. The plan of a WSN depends fundamentally on the application, and it must consider factors, for example, the environment, the applications outline objectives, and cost, hardware, and framework imperatives. The sensor nodes will perform huge signal processing, computation, and network self-arrangement to accomplish scalable, robust and seemingly perpetual networks. All the more particularly, sensor nodes will do neighborhood processing to decrease interchanges, and subsequently, vitality costs. This paper plots the WSN architecture, security requirements and security challenges.

Keywords: [Security, Architecture, Challenges, Wireless Sensor Network.]

1. INTRODUCTION

A wireless sensor network is an accumulation of countless nodes and no less than one base station. The sensor node is a self-governing little gadget that comprises of primarily four units that are sensing, processing, communication and power supply. These sensors are utilized to gather the data from the environment and pass it on to a base station. A base station gives an association with the wired world where the gathered information is handled, investigated and exhibited to helpful applications.

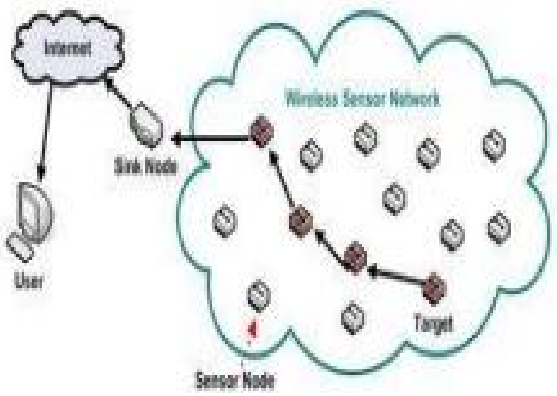

Figure 1: Wireless Sensor Network

Wired networks likewise called Ethernet network are the most widely recognized types of local zone network (LAN) innovation. The types of wired network are PAN, LAN, mesh, MAN, WAN and the cell network. In this way by inserting processing and communication inside the physical world, Wireless Sensor Network (WSN) can be utilized as an

apparatus to connect genuine and virtual environment. A wireless network is any sort of PC network that uses the wireless information association for interfacing network nodes. Peer to peer/Ad-hoc and infrastructure (Wi-Fi) are the fundamental two types of wireless networking. As both of the networks have their own particular advantages and disadvantages, the wireless network is more advantageous than wired network since it permits simple availability between PCs, cost-compelling. As the wireless innovation advances, there is a fast development in wireless sensor network examine. This is a network, which incorporates disseminated sensors to screen the physical or environmental conditions like temperature, sound, vibration, pressure and humidity. A sensor node has radio transceiver, microcontroller and a battery. Assets like energy, memory, speed, bandwidth, is fluctuated by the measure of the node. In this paper, we talk about the Security requirements, attacks, security threads and vulnerability and threats guard techniques in WSN.

2. LITERATURE SURVEY

NishantSitapara et al. proposed an answer where black hole node is identified (expect) and endeavored to take out its effects. Arrangement tries to dispose of the black hole impact at the route assurance mechanism of the AODV protocol that is done before the nodes start the packets. Moreover, creator utilized UDP Connection to have the capacity to check the packets at Sending nodes and receiving nodes. **Deng et al.** proposed an answer for the black-hole assault issue in AODV routing protocol. They enabled the intermediate node to send an answer message in the event that it had a sufficiently crisp route to the goal. In any case, the intermediate node could be a malignant node and could send route answer regardless of whether it had no sufficiently new route to the goal to influence a black hole to assault. They proposed an answer that the source node would send another route request to the following jump of the intermediate node to check the legitimacy of the route from the intermediate node to the goal node. In the event that the route exists, the intermediate node is put stock in; something else, the answer message from the intermediate node is disposed of. **Ning LIU et al.** proposed an adaptive approach to recognize black and dark hole attacks in ad hoc network based on a cross layer configuration network. In OSI network layer, a way based strategy to screen the following jump's activity. This technique does not toss out additional control packets and recoveries the network framework assets of the identifying versatile node. In network, The Media Access Control Layer a collision rate detailing framework is set up to evaluate dynamic distinguishing limit in order to bring down the false positive rate under high network overload. They choose to pick DSR protocol to test proposed calculation and ns-2 as reenactment instrument. **Dr.E.Karthikeyan et al.** proposed arrangement that the nodes validate each other by issuing security endorsement in advanced shape to the various nodes in the network. The proposed strategy is to be adjusted on DSR protocol and should be reproduced and examined for various execution parameters. This strategy is equipped for recognizing and evacuating black hole nodes in the MANET. **Sanjay Ramaswamy et al.** proposed a method for distinguishing numerous black hole nodes inMANET. They are at first proposing answer for helpful black hole assault in ad-hoc network. Creator in some degree altered AODV protocol by presenting data routing information table (DRI) and cross checking of routing table data where, every section of the versatile node is kept up. They are relying upon the trustworthy nodes to transmit the packets. Source sends The Route request (RREQ) to each node and it send parcel to the node from where it gets the RREP.

3. WSN ARCHITECTURE

In a typical WSN we see following network components

- Sensor motes (Field devices)

– Field devices are mounted all the while and must be equipped for routing packets in the interest of different devices. Much of the time they portray or control the procedure or process gear. A router is an uncommon kind of field gadget that does not have process sensor or control gear and in that capacity does not interface with the procedure itself.

- Gateway or Access points
  A Gateway enables communication between Host application and field devices.
- Network manager

– A Network Manager is in charge of arrangement of the network, scheduling communication between devices (i.e., designing superframes), administration of the routing tables and monitoring and detailing the soundness of the network.

- Security manager

– The Security Manager is in charge of the generation, storage, and administration of keys.

4. SECURITY REQUIREMENTS IN WSN

A sensor network is a special type of network in which it shares some common properties of typical computer network. A goal of security services in WSN's is to protect network i.e. information and resources from attackers. These security requirements are as follows:

A. Data Confidentiality

Data Confidentiality in networking is most vital issue in network security. It guarantees that the given message is seen just by that coveted beneficiaries. The real issue in WSN is that wireless channels are available to everybody therefore that channels are utilized by anybody. Along these lines attackers can catch touchy information through that radio communication. Therefore it is exceptionally important to assemble a safe divert in WSN. Sensor node might be profoundly delicate, particularly in military applications. In this manner sensor network ought to be worked such that it ought not release any sensor readings to its neighbors. Applications like sensor personalities, modern mysteries, and open keys ought to be scrambled to some degree to shield from malignant action. The key approach to accomplish confidentiality is to encode the data with a mystery key that exclusive wanted beneficiaries knows. Cipher Block Chain (CBC) is the most proper encryption strategy for sensor network according to TinySec.

B. Data Integrity

An assailant might be not ready to take information with the execution of confidentiality. In any case, this doesn't imply that the data is sheltered. Data integrity guarantees that the message send starting with one node then onto the next node isn't altered because of noxious goal or by a mishap. For instance in hostile environment a pernicious node may add or control the data inside a packet. This controlled new packet then sends to the indented collector. At the point when the operational conditions are out of range like temperature, humidity, pressure, light, radiations and so forth, then that gadget works dishonorably this can cause blunders in packets. Those blunders may not be watched and those mistake packets are sent out. The garbled packets will be added at the other side's which can cause denial of service (DoS) assault that lessens or wipes out a network ability to play out its normal capacities. On the off chance that an aggressor knows the packet organize, then more genuine harms can be caused like he can adjust the area of critical occasion with the goal that recipient acquires wrong information. In this way the fundamental requirements for secure communication are that the information or packets are not altered amid communication. And furthermore the recipient has to know precisely what the sender needs to send. The utilization of message integrity code is the standard approach for guaranteeing data integrity.

C. Data Authenticity

Authentication is important for some, administrative assignments like network reinventing, basic leadership process and so forth. An adversary can without much of a stretch infuse messages on the off chance that he knows the packet organize characterized in the network. Along these lines, collector gets the packets conveying false information. So it is essential for the collector to ensure that the data utilized as a part of basic leadership process starts from the right source. Furthermore, the regular case of packet infusion is Sybil assault. Data authenticity guarantees that the communication in the middle of two nodes is real that is a noxious node can't carries on as a trusted network node. Utilization of message authentication code, signature authenticating open keys and so forth is the standard approach for guaranteeing authenticity.

D. Data Freshness

To accomplish either consistent monitoring or occasion heading applications, WSN are utilized. In consistent monitoring applications, every sensor node advances its detected data occasionally to the base station and in occasion bearing application, once an occasion happens, nodes answered to the base station. In nonstop monitoring application, for example, in healing center application, new data is required for making the important and preventive move. Data coming to the sink node or base station after a specific limit isn't helpful for further processing, in light of the fact that the information in it isn't substantial. An aggressor gets a packet from a network, and after that replays it to the network after some measure of time. An ordinary case of this is Wormhole assault in wireless network. Instead of confidentiality and data integrity, freshness of each message should be guaranteed. Data freshness infers that the data is a current and guarantees that no assailant can replay old messages. Data freshness is guaranteed by utilizing a timestamp i.e. a receiving node can contrast its own particular time clock and the timestamp and checked whether the packet is crisp i.e. substantial or not But rather this is an overhead on the grounds that each time data is sent, the timestamp of the got data packet must be checked.

E. Availability

Because of abundance computation and communication, sensor nodes may come up short on battery power and wind up inaccessible. An adversary may stick communication to make the sensor nodes inaccessible, which brings about the degradation of network security leading to DoS. Availability which guarantees that the coveted network services are accessible even within the sight of denial of service attacks.

F. Self Organization

Self organization is the property of framework to mastermind its parts, components in a deliberate or non-arbitrary way under suitable conditions however without controlled by any specialist or subsystem inside or outside of the framework. Numerous sensor nodes of various types are set in a heterogeneous and to some degree hostile environment therefore there is no settled infrastructure is accessible for WSN. Self organization of WSN is a testing undertaking due to restricted energy assets accessible in this network. Self organization guarantees that the decomposition of the network into associated, non-covering groups of limited size. Distributed sensor network must act naturally arrange to help multi-hop routing, to direct key administration and building confide in relations among sensors, deny contradict, withhold, dispose of.

G. Non-Repudiation

Non-Repudiation tells about wellspring of the packet. Source demonstrates of character of the packet in authentication process. Non-Repudiation gives specialist of source from denying that it sent a packet.

5. SECURITY CHALLENGES IN WSN

The idea of huge, ad-hoc, wireless sensor networks presents critical challenges in

outlining security plans. A wireless sensor network is an exceptional network which has numerous imperatives contrasted with traditional PC networks.

Wireless Medium: The wireless medium in characteristically less secure on the grounds that its broadcast nature makes spying basic. Any transmission can without much of a stretch be intercepted, altered, or supplanted by an adversary. The wireless medium permits an assailant effortlessly capture legitimate packets and effectively infuses malignant ones. In spite of the fact that this issue isn't extraordinary to sensor networks, traditional arrangements must be adapted to proficiently execute on sensor networks.

Ad-Hoc Deployment: The ad-hoc nature of sensor networks implies that no structure can be statically characterized. Nodes might be conveyed via airdrop, so nothing is known about the topology before deployment. Since nodes may fall flat or be supplanted, the network must help self-design. Security plans must have the capacity to work inside the dynamic environment.

Hostile Environment: The following test factor is the hostile environment in which sensor nodes work. Nodes confront the likelihood of decimation or caught by attackers. The exceptionally hostile environment speaks to a genuine test for security specialists.

Immense Scale: The proposed scale of sensor networks represents a critical test for security mechanisms. Just networking tens to a huge number of nodes have ended up being the generous undertaking.

CONCLUSION

The fundamental thought of this paper is to give point by point data about security issues and types of attacks WSN is presented to some conceivable measure for countering such attacks. An endeavor has been made to investigate security mechanism. Security in Wireless Sensor Network is fundamental to the acknowledgment and utilization of sensor networks. Specifically, Wireless Sensor Network item in the business won't get acknowledgment unless there is a confirmation security to the network. In this paper, we have thought about that diagram of WSN architecture, security requirements, and challenges.

REFERENCES

[1]. Hongmei Deng, Wei Li, and Dharma P.Agrawal “Routing Security in Wireless AdHoc Network” IEEE Communications Magzine, vol. 40, PP.70-75, 2002.

[2]. Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and KendallNygard “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”.

[3]. Wei Gong, Zhiyang You1, Danning Chen, Xibin Zhao, Ming Gu, Kwok-Yan Lam, “Trust Based Malicious Nodes Detection in MANET”, 2009 IEEE.

[4] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi, SarehBeheshti, “A Survey on Wireless Sensor Networks Security”, SETIT 2007, 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 25- 29, 2007 – TUNISIA.

[5] Daisuke Takaishi , Hiroki Nishiyama, Nei Kato, and Ryu Miura, “Towards Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks”, DOI 10.1109/TETC.2014.2318177, IEEE Transactions on Emerging Topics in Computing, 2014.

[6] M. Chen, T. Kwon, and Y. Choi, “Energy-efficient differentiated directed diffusion (eddd) in wireless sensor networks,” Computer Communications, vol. 29, no. 2, pp. 231–245, 2006.

[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: a scalable and robust communication paradigm for sensor networks,” inMobiCom’00 Proceedings of the 6th annual international conference on Mobile computing and networking, 2000.

[8] L. He, Z. Yang, J. Pan, L. Cai, J. Xu, and Y. Gu, “Evaluating service disciplines for on-

demand mobile data collection in sensor networks," vol. PP, no. 99, 2013.