INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Attacks and threats in Wireless Sensor Networks

G. V. Pavan Nikhil
pavannikhil99@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

Anisetti Kalyan Rahul
anisettikalyan.rahul2016@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Chikoti Akash
chikoti.akash2016@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Prathik Reddy
prathikr1999@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

K.Manikandhan
kmanikandan@vit.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

ABSTRACT

Wireless sensor networks is a rising subject to research and improvement, The advances and traits in Wireless Communication technology have made the deployment of small, low fee wireless sensor nodes connected through a wireless medium, known as Wireless Sensor Networks (WSNs), technically and economically possible. These WSNs have were given several packages in diverse fields like an army, environmental monitoring, fitness, enterprise and so on. Security has already ended up a primary subject for WSNs because of the wide utility of WSNs in security-vital regions. In this paper, we check out the security-related troubles and demanding situations in wi-fi sensor networks. We identify the security threats, overview proposed safety mechanisms for wi-fi sensor networks

Keywords—*Wireless Sensor Networks (WSNs), Security, Attacks and challenges, Security mechanism*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-much less wi-fi networks to screen bodily or environmental situations, together with temperature, sound, vibration, stress, movement or pollution and to cooperatively skip their information thru the community to a first-rate place or sink wherein the facts may be determined and analysed. A sink or base station acts as an interface among users and the network. One can retrieve required data from the network via injecting queries and collecting consequences from the sink. Typically a wireless sensor network carries loads of heaps of sensor nodes. The sensor nodes can communicate amongst themselves the use of radio indicators. A wireless sensor node is ready with sensing and computing gadgets, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are inherently aid confined: they have got limited processing speed, garage ability, and communique bandwidth. After the sensor nodes are deployed, they may be answerable for self-organizing the suitable community infrastructure often with multi-hop communique with them. Then the onboard sensors begin accumulating facts of the hobby. Wireless sensor gadgets additionally reply to queries sent from a "manage web page" to perform precise instructions or offer sensing samples. The running mode of the sensor nodes can be either continuous or event-driven.

2. WHY USED WIRELESS NETWORKS?

Wireless networks have become famous due to their ease of use. Consumer/person is no greater dependent on wires wherein he/she is, easy to move and revel in being connected to the network. One of the splendid functions of a wireless network that makes it captivating and distinguishable amongst the traditional wired networks is mobility [1]. This characteristic gives a person the capability to transport freely, at the same time as being connected to the network. Wireless networks comparatively easy to put in the then wired community. There is nothing to worry approximately pulling the cables/wires in the wall and ceilings. These can variety from a small quantity of users to massive complete infrastructure networks in which the range of customers is in lots.

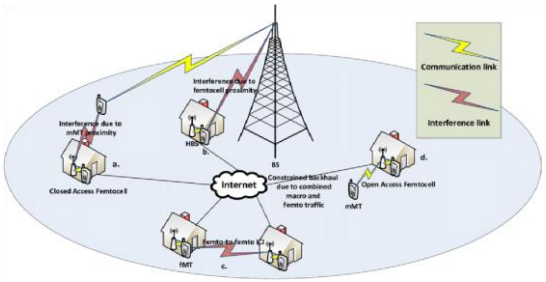

Fig. 1: Communications in wireless networks

2.1 Wireless Ad-hoc Networks

A wireless ad-hoc community includes a collection of nodes that talk with every Other through wi-fi hyperlinks without a pre-installed networking infrastructure. The community is advert hoc as it does no longer rely on a pre-present infrastructure, together with routers in stressed networks or access factors in

managed (infrastructure) Wi-Fi networks. It originated from battlefield communique applications, wherein infrastructure networks are often impossible [2]. The decentralized nature of wireless advert-hoc networks makes them suitable for a variety of packages in which valuable nodes can not be depended on and can improve the scalability of networks compared to wireless controlled networks, even though theoretical and realistic limits to the general capacity of such networks were diagnosed.

Minimal configuration and brief deployment make ad hoc networks appropriate for emergency situations like herbal screw ups or military conflicts. The presence of dynamic and adaptive routing protocols enables advert hoc networks to be fashioned quickly.

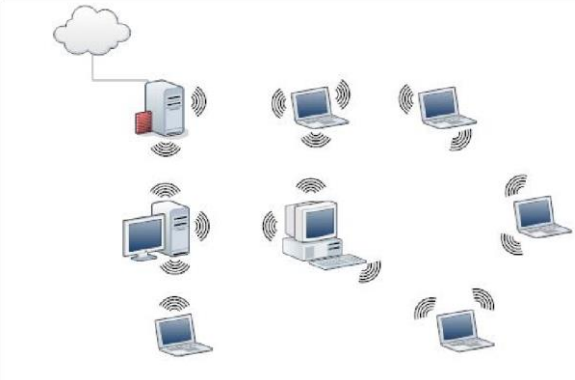

Fig. 2: Simple ad-hoc networks

2.2 Manet

A cellular advert hoc community is formed by using cellular hosts. Each tool in a MANET is free to move independently in any route, and will consequently trade its hyperlinks to different gadgets frequently. Each must forward visitors unrelated to its own use, and therefore be a router. The number one assignment in constructing a MANET is equipping each tool to constantly keep the statistics required to correctly path traffic. Mobile ad hoc networks can be used in many packages, starting from sensors for the environment, vehicular ad hoc communications, street protection, health, home, peer-to peer messaging, disaster rescue operations, air/land/army protection, guns, robots, etc.

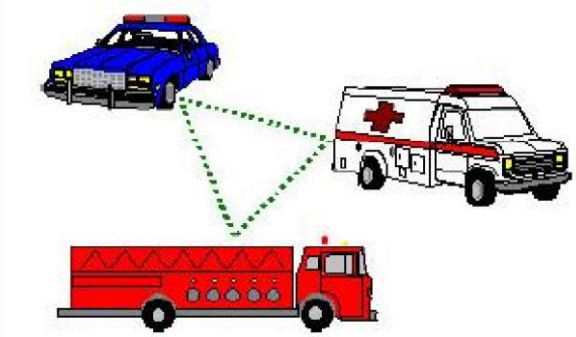

Fig. 3: Example of a vehicle-to-vehicle network

2.3 Wireless sensor networks

A sensor network is a deployment of big numbers of small, inexpensive, self-powered gadgets that can sense, compute, and talk with different devices for the purpose of amassing local facts to make worldwide decisions approximately a bodily environment WSNs measure environmental conditions like temperature, sound, pollution tiers, humidity, wind, and so forth. Currently, WSNs is the maximum widespread services employed in business and commercial packages, because of its technical development in a processor, conversation, and coffee-electricity usage of embedded computing gadgets. The WSN is built with nodes that are used to look at the surroundings like temperature, humidity, strain, position, vibration, sound and so forth. These nodes may be utilized in numerous real-time applications to carry out various obligations like smart detecting, discovery of neighbor node, records processing and storage, records series, goal tracking, reveal and controlling, synchronization, node localization, and powerful routing among the base station and nodes.

3. INTRODUCTION TO WIRELESS SENSOR NETWORKS

A wi-fi sensor and actuator community (parent 1.5) is a collection of small randomly dispersed gadgets that provide 3 essential features; the capability to screen bodily and environmental situations, regularly in actual time, which includes temperature, stress, mild and humidity; the potential to function gadgets together with switches, cars or actuators that manipulate those situations; and the capability to provide efficient, dependable communications via a wi-fi community.

Wireless sensor networks use three primary networking topologies; point-to-point, celebrity (factor-to-multipoint), or mesh (parent 1.6). Point-to-point is actually a devoted hyperlink between points. Star networks are an aggregation of factor-to-factor hyperlinks, with an important master node. In the mesh topology, each node has more than one pathways to every other node, supplying the most resiliency and versatility.

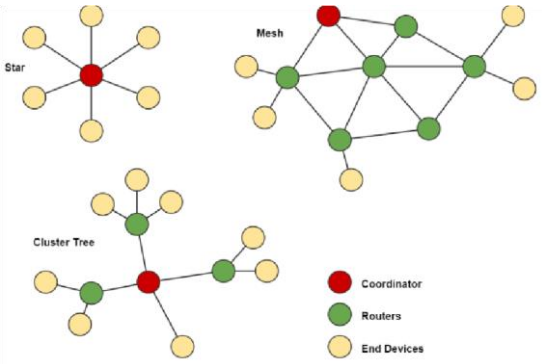

Fig 4. Basic wireless network topologies.

3.1 Applications of WSN

- Forest fires detection
- Air pollution monitoring
- Landslide detection
- Greenhouse monitoring
- Industrial monitoring.
- Area monitoring
- Water/wastewater monitoring
- Volcano monitoring
- Agriculture
- Structural monitoring

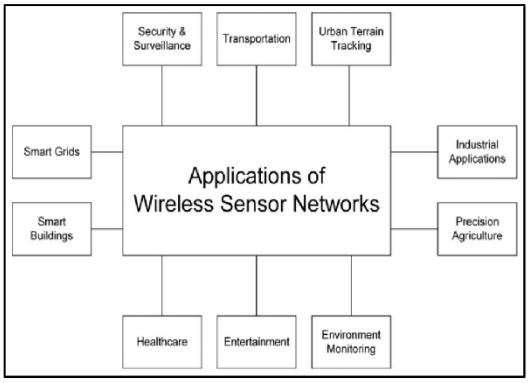

Fig. 5: Wireless sensor network applications

3.2 Components of Wireless Sensor Network

Sensor nodes coordinate among themselves to supply exceptional facts about the bodily environment. Basically, each sensor node contains sensing, processing, transmission, mobilizer, function locating system, and electricity units.

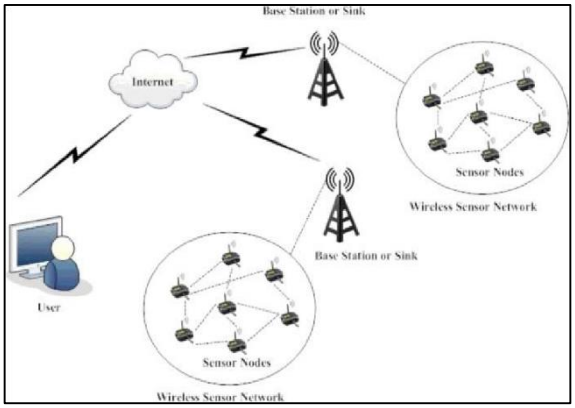

Fig. 6: Wireless sensor network

- Sensor Field: A sensor area may be considered as an area wherein the nodes are positioned.
- Sensor Nodes: Sensors nodes are the heart of the community. They are in the price of collecting records and routing this information back to a sink.
- Sink: A sink is a sensor node with the precise venture of receiving, processing and storing data from the alternative sensor nodes. Sinks are also called records of aggregation factors.
- Task Manager: The mission manager also called base station is a centralized point of control within the community, which extracts statistics from the community and disseminates control information back into the network. The base station is either a pc or a laptop.

4. TYPES OF ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are vulnerable to safety attacks because of the published nature of the transmission medium. Moreover, wi-fi sensor networks have an additional weakness considering hubs are frequently put in a threatening or volatile condition wherein they're now not bodily secured. Essentially assaults are named dynamic attacks and indifferent assaults.

4.1 Active attacks

The unauthorized people video display units listen to and modifies the facts circulation within the verbal exchange channel are called lively assault. These assaults are lively in nature. Routing Attacks in Sensor Networks, Denial of Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering and many others.

4.2 Passive attacks

The tracking and listening of the conversation channel by unauthorized attackers are known as passive assault. The Attacks in opposition to privacy is passive in nature. Some of the greater commonplace attacks [8] in opposition to sensor privacy are Monitor and Eavesdropping, Traffic Analysis, Camouflage Adversaries.

5. SECURITY MECHANISM

These mechanisms are clearly used to discover, save you and get over the security assaults. These safety mechanisms can be labelled as excessive stage and coffee-level.

5.1 Low-Level mechanism

Low-level security is for securing sensor networks consists of, Secrecy and authentication, Privacy Robustness to conversation denial of the carrier, Key establishment and consider setup Secure routing, Resilience to node capture and so on.

5.2 High-Level mechanism

The high-Level mechanism is for securing sensor networks, consists of cozy group management, intrusion detection, and cozy statistics aggregation.

6. CHALLENGES OF SENSOR

6.1 Wireless medium

The wi-fi medium is inherently much less cozy due to the fact it's broadcast nature makes eavesdropping easy.

6.2 Resource scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms.

6.3 Management at a distance

Sensor nodes may be deployed at our door discipline consisting of a subway station. It is difficult for managers or operators to manage the network immediately. Thus the framework should provide an oblique faraway manipulate/ management device.

6.4 Ad-Hoc deployment

The ad-hoc nature of sensor networks way no shape may be statically described. The community topology is usual a situation to changes due to node failure, addition, or mobility. Nodes can be deployed by way of airdrop, so nothing is understood of the topology previous to deployment. Since nodes may additionally fail or get replaced the community need to help self-configuration.

6.5 Challenges in energy management

Low-value deployment is one acclaimed gain of sensor networks. Limited processor bandwidth and small reminiscence are two controversial constraints in sensor networks, as a way to disappear with the improvement of fabrication techniques. However, the power constraint is not going to be solved quickly because of gradual development in growing battery potential. Moreover, the intended nature of sensor nodes and risky sensing environments preclude battery replacement as a viable answer. On the other hand, the surveillance nature of many sensor community packages requires an extended lifetime; therefore, it's miles a very important studies issue to offer a form of power-green surveillance service for a geographic area. Much of the current research makes a speciality of how to provide full or partial sensing coverage in the context of strength conservation.

6.6 Unreliable communication

Certainly, the unreliable communique is another hazard to sensor protection. The security of the network is predicated closely on a defined protocol, which in flip relies upon on verbal exchange.

6.7 Unreliable Transfer

Normally the packet-based totally routing of the sensor network is connectionless and for that reason inherently unreliable. Conflicts Even if the channel is reliable, the communique may nevertheless be unreliable. This is due to the published nature of the wireless sensor network.

6.8 Latency

The multi-hop routing, community congestion and node processing can cause extra latency within the network, as a

consequence making it difficult to achieve synchronization amongst sensor nodes.

6.9 Challenges in actual time

WSN cope with real global environments. In many cases, sensor records have to be introduced inside time constraints in order that appropriate observations can be made or movements taken. Very few results exist thus far regarding meeting real-time necessities in WSN. Most protocols either forget about actual-time or clearly try to process as rapid as possible and hope that this speed is sufficient to fulfil closing dates. Some preliminary outcomes exist for real-time routing. To date, the limited effects that have seemed for WSN concerning real-time troubles have been in routing. Many different functions have to additionally meet real-time constraints consisting of information fusion, records transmission, target and event detection and classification, query processing, and security. New results are needed to guarantee soft real-time requirements and that deal with the realities of WSN such as lost messages, noise and congestion. Using feedback control to address both steady-state and transient behavior seems to hold promise. Dealing with real-time usually identifies the need for differentiated services, e.g., routing solutions need to support different classes of traffic; guarantees for the important traffic and less support for unimportant traffic. It is important not only to develop real-time protocols for WSN, but associated analysis techniques must also be developed.

6.10 Unattended

Operation Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main cautions to unattended sensor nodes

- **Exposure to Physical Attacks:** The sensor may be deployed in an environment open to adversaries, bad weather, and so on.
- **Managed Remotely:** Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues.
- **No Central Management Point:** A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

7. CONCLUSION

Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless communications skills. The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are more and more being used in military, environmental, fitness and commercial packages. Sensor networks are inherently exclusive from traditional wired networks in addition to wi-fi advert-hoc networks. Security is a critical feature for the deployment of Wireless Sensor Networks. This paper summarizes the assaults and their classifications in wireless sensor networks and additionally, a try has been made to explore the security mechanism broadly used to deal with the one's attacks. The demanding situations of Wireless Sensor Networks also are in brief mentioned. This survey will with a bit of luck to inspire future researchers to give you smarter and extra robust protection mechanisms and make their community safer.

8. REFERENCES

[1] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, the year 2004

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International Conference on Advanced Computing Technologies, Page1043-1045, the year 2006

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (Elsevier), Page: 299-302, year 2003

[4] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "ASurvey on Sensor Networks", IEEE Communication Magazine, the year 2002

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10- 15, the year 2006.

[6] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced CommunicationTechnology (ICACT), Page(s):6, the year 2006

[7] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, the year 2009.

[8] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, the year 2002 http://www.cs.sfu.ca/~angiez/personal/papessenso rids.pdf

[9] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 –40, year 2006

[10] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, Sensor Network Security: A Survey, IEEE Communications Surveys & Tutorials, vol. 11, no. 2, page(s):52-62, year 2009.

[11] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[12] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, year 2005.

