International Research Journal of Emerging Trends in Multidisciplinary

ISSN 2395-4434

Volume 1, Issue 6 August 2015

www.irjetm.com

A Review on Security Issues & Routing Protocols of Wireless Networks

J V N Ramesh
Assoc Professor
Dept of Electronics and ComputerEngg.
K L E F University
jvnramesh@gmail.com

Ch.Sree Harsha
Dept of Electronics and ComputerEngg
K L E F University
Sreeharsha2058@gmail.com

S.Eswar Reddy
Dept of Electronics and ComputerEngg
K L E F University
eswar12100@gmail.com

Abstract

Wireless networks method is the most popular technique used in the present day. Wireless sensor networks and wireless communications are the most popular applications of wireless network. These networks use some devices to work and implement. There are many devices that are used in this network area. These devices are distributed over a large areas and are used to collect data from that particular area. Due to large number of devices the input data collection is also large. To reduce processing of this collected data there is a need to enlarge the processing space. This is knows as data aggression. There are many approaches used in classification of data of sensors. This paper is a general review of wireless sensor network. It also gives some idea on the protocols and security issues of Wireless networks.

Keywords: Wireless Network, Data Aggression, Security, Protocol.

1. Introduction

The rapid growth of wireless technology takes an interest of researchers in the era of wireless sensor network. The sensor network is a collection of the small sensors which are self-configured. These nodes are connected with wireless media. As far as the Wireless Sensor Network is concert it is A Network formed by the economical and Simple Processing Devices called Sensors. These sensors are work with Temperature, Humidity for Environmental Sensors. In this network the node are able to communicate with other nodes using a Wireless Radio Device. Some time it seems to be that such communication cause the problem Secure Administration of network. Like all Network, Sensor Networks may show the Security loopholes. If these loopholes are not Addressed Properly, it becomes the Large Number of Vulnerabilities. Due to this Vulnerabilities Attackers Can able to access the network and can modified the data which break the authenticity.

A wireless sensing element network consists of spatially distributed autonomous sensors to observe physical or environmental conditions, like temperature, sound, vibration, pressure, humidity, motion or pollutants and to hand in glove pass their information through the network to a main location A sensing element node would possibly vary in size from that of a shoebox right down to the scale of a grain of mud. every node represents a possible purpose of attack, creating it impractical to observe and shield every individual sensing element from either physical or logical attacks. Security could be a common concern for any network system, however security in Wireless sensing element Network is of nice importance to confirm its application success. for instance, once sensing element network is employed for military purpose, it's vital to stay the detected data confidential and authentic providing security for WSN represents a chic field of analysis issues as several existing security schemes for ancient networks aren't applicable for WSN. Moreover, analysis of security needs provides right directions to develop or implement the right safeguards against the protection violations.

This paper has divided into five major sections including this one. In section one there is a brief introduction of the topic. The section two explains the data aggregation in WSN. Section three throws some light on the security issues of the sensor network. Section four is for literature review and finally conclusion is defined in section five.

2. Data Aggregation

A Wireless sensing element Network (WSN) generally consists of a sink node typically mentioned as a Base Station and variety of tiny wireless sensing element nodes. the bottom station is assumed to be secure with unlimited accessible energy whereas the sensing element nodes ar assumed to be unsecured with restricted accessible energy. The sensing element nodes monitor a region and collect sensory data. Sensory data is communicated to the bottom Station through Wireless hop by hop transmissions. To conserve energy this data is aggregative at intermediate sensing element nodes by applying an acceptable aggregation perform on the received knowledge. Aggregation reduces the number of network traffic that helps to cut back energy consumption on sensing element nodes. It but complicates the already existing security challenges for wireless sensing element networks and needs new security techniques tailored specifically for this state of affairs. Providing security to combination knowledge in Wireless sensing element Networks is understood as Secure knowledge Aggregation in WSN were the primary few works discussing techniques for secure knowledge aggregation in Wireless sensing element Networks.

Attacks in Wireless sensing element Networks Attacks against wireless sensing element networks might be loosely thought-about from 2 totally different levels of views. One is that the attack against the protection mechanisms and another is against the fundamental mechanisms (like routing mechanisms). Here we tend to suggests the key attacks in wireless sensing element networks.

3. Security Issues

There are many security issues in wireless sensor network.

Some of them are discussed below:

Limited Resources

All Security Approaches Require A Certain Amount of Resources For The Implementation, Including Data Memory, Code Space, And Energy To Power The Sensor. However, Currently These Resources Are Very Limited In A Tiny Wireless Sensor.

Limited Memory

Sensor is a small in size so that the storage capacity of data is also small. To execute the programs there is a need of memory but in this types of devices have the limited memory.

Power consumption

Enrage is an important issue in any wireless network. As the nodes are able to move in the network, these node needs large amount of energy for the route selection, node searching etc. in sensor network sensing is also the higher priority task. This process always in execution so that there is a need of high performance battery. The node verification, encryption, decryption, protocols etc are the various programs in which the battery of nodes is mostly spend as an overhead. It should be minimized.

Unreliable transfer

Generally it seems to be that communication in the wireless sensor network uses the unreliable transfer. Here the connectionless routing is used, so the possibility of channel error rate may increase. So here mostly unreliable transfer has used.

Conflicts

Some time it is possible that the channel may reliable, but communication could be unreliable. It happened because the wireless sensor network uses the broadcasting. If packets meet in the Middle of transfer, conflicts will occur and the transfer itself will fail.

Security attacks

WSNs square measure liable to varied sorts of attacks. consistent with the protection needs in WSNs, these attacks will be categorized:

Attacks on secrecy and authentication: Normal cryptographical techniques will shield the secrecy and genuineness of communication channels from outsider attacks like eavesdropping, packet replay attacks, and modification or spoofing of packets.

Attacks on network availability: Attacks on convenience square measure typically stated as denial-of-service (DoS) attacks. DoS attacks might target any layer of a sensing element network. For securing the Wireless sensing element Networks, it's necessary to handle the attacks then take counter measures at the look time of WSN. This section lists and offers transient discussion regarding the foremost attacks against Wireless sensing element Network.

A. Physical Attack

B. Attacks at Different Layer

- **Physical layer**
- **Network layer**
- **Transport layer**

Denial of Service Denial of Service (DoS)

Dos is made by the unintentional failure of nodes or malicious action. the only DoS attack tries to exhaust the resources obtainable to the victim node, by causation additional inessential packets and so prevents legitimate network users from accessing services or resources to that they're entitled. DoS attack is supposed not just for the adversary's commit to subvert, disrupt, or destroy a network, however conjointly for any event that diminishes a network's capability to supply a service. In wireless sensing element networks, many sorts of DoS attacks in numerous layers may well be performed. At physical layer the DoS attacks may be ECM and change of state, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack may be performed by malicious flooding and asynchronism. The mechanisms to forestall DoS attacks embody payment for network resources, pushback, robust authentication and identification of traffic.

Attribute-Based or Data-Centric Routing Protocols

In these types of protocol system emphasizes on data. For example Flooding and gossiping are the protocol which only focuses on the data. These are the traditional routing protocols. These protocols do not need to know the topology used in the system. These protocols do not follow any routing algorithms. In flooding mechanism, each sensor node receives a packet and broadcasts this to all neighboring nodes.

Hierarchical-Based Routing (Clustering)

Hierarchical or cluster based mostly strategies square measure documented techniques with special advantage of measurability and economical communication. Nodes play totally different roles within the network. hierarchic routing maintains the energy consumption of detector nodes and performs knowledge aggregation that helps in decreasing the amount of transmitted messages to base station. the full WSN is split into variety of clusters in term with the precise rules. Some hierarchic protocols square measure mentioned here.

Location-Based Routing (Geographic Protocol)

Most of the routing protocols require location information for sensor nodes in wireless sensor networks to calculate the distance between two particular nodes on the basis of signal strength so that energy consumption can be estimated. It is also utilized in routing data in energy efficient way when addressing scheme for sensor network is not known. It is worth noting that there have been many location-based protocols in Ad Hoc networks and it makes great effects when we transplant those research achievements for wireless sensor networks in some ways.

Multipath Routing Protocol

Due to the limited multi-hop path and the strong momentum of wireless backhaul capacity, the development of a single route path is not able to provide an efficient high-speed transmission of data in wireless sensor networks. Today, the focus of multi routing is widely used as one of the possible solutions to overcome this limitation.

4. Related work

As generalized interconnect devices autonomous sensors gave birth to an oversized category of recent production applications, security emerges as a central demand. Wireless device networks ar at risk of attacks as a result of they're typically deployed in open environments and unattended. during this article, the author describes the hole attack; a severe attack against routing device networks is especially tough to defend. The author has given details of its options and studies its result on the right functioning of a device network. The author has bestowed technical analysis to resolve issues wormholes in wireless device networks and has been aforementioned concerning the strengths and weaknesses of the projected solutions. To date, most of the proposals of defenses specialise in preventive mechanisms which will be applied to safeguard sensing element networks from such attacks. However, no study has been revealed relating to the chance of victimization a lot of subtle ways, like intrusion detection systems, to realize a a lot of complete process against attacks and worm holes autonomous. The author has bestowed his add intrusion detection and introduces a light-weight IDS framework, referred to as Lidea designed for wireless sensing element networks. Lidea is predicated on a distributed design, within which nodes hear their neighboring nodes associated collaborate with one another so as to with success notice an intrusion. He ended by stressing that a system of this sort is wont to defend against attacks wormholes. WSN multi hop networks square measure, in step with the intermediate nodes relaying the information packet to the destination. These nodes square measure equipped with less memory, restricted battery power, low computing power, restricted communication vary and want a routing path safe and effective to transmit the incoming packet. during this paper, we tend to propose a routing protocol primarily based multipath secure cluster (SCMRP). Researchers have planned clustered device networks to extend potency (ie the performance of the system increase, save energy and cut back the info aggregation system delay) and multiple device networks to extend endurance and network reliableness. The SCMRP is that the combination of those 2 systems of devices; thus provides potency and reliableness and smart use of the secret writing rule provides spare security for the sensor network. SCMRP provides security against varied attacks like modification of routing info, selective forwarding attack, attack depression, hole attack, Sybil attack etc. additionally, we offer a quick analysis of varied problems associated with the key management Orphan nodes, security and energy potency.

Wireless sensing element networks supply a convenient and price effective for manual knowledge assortment normally and alternative military situations, providing a way to observe a vicinity of land and warning of threat. However, in hostile situations, the network is probably going to return vulnerable by malicious agents trying to compromise the routing diversity in these environments. during this paper, a way is conferred in overhead routing of wireless sensing element network may be a set of stable routes trust throughout the amount of fast preparation of a wireless sensing element network, and encourage them to the network once the long run operation less reliable devices is also introduced. Associate in Nursing example case study is conferred illustrating routing resistance continues in Associate in Nursing attack by inserting referred to as the hole attack malicious hardware.

5. Conclusion

The study provides a concept concerning the sensing element network. The sensing element network uses the massive variety of sensing element devices. attributable to sensing device every node ought to method the info. once there's a process then energy loss can happen. to scale back the energy loss knowledge aggregation will apply. This paper could be a review concerning the wireless sensing element network. It additionally throws some lightweight on the protocol used over WSN.

6. Acknowledgement

The analysis given during this paper wouldn't are attainable while not our faculty, at NRI, Bhopal. we tend to want to specific our feeling to all or any the those who helped flip the World-Wide net into the helpful and fashionable distributed machine-readable text. we tend to conjointly want to convey the anonymous reviewers for his or her valuable suggestions.

7. References

1. Ashwani et al., International Journal of Advanced Research in Computer Science and Software Engineering 2 (9), September- 2012, pp. 145-148
2. Security-aware ad hoc routing for wireless

networks ",MobiHoc - Yi, Naldurg, et al. – 2001

3. International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.4, August 2013
4. Efficient security mechanism for large-scale distributed sensor networks. Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 62 – 72, New York, USA, ACM Press.
5. Computing of trust in wireless networks. Proceedings of 60th IEEE Vehicular Technology Conference, California, USA.
6. Denial of service in sensor networks. IEEE Computer, Vol. 35, No. 10, pp. 54-62.
7. Towards resilient security in wireless sensor networks. Procedings of ACM MobiHoc, pp. 34 – 45.
8. New aggregation techniques for sensor networks. Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 239-249, ACM Press.
9. A survey of security issues in wireless sensor networks. IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2- 23.
10. security protocols for sensor networks. Wireless Networks, Vol. 8, No. 5, pp. 521-534.