International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 2 February 2015

Analysis of Routing Protocols for Data Aggregation in Wireless Sensor Network

Roopesh Kumar Sharma[1], B. P. Patel[2], Y. K. Rana[3] and R. S. Pippal[4]
M.Tech Scholar, Deptt. of CSE REC, Bhopal[1]
Asst. Professor, Deptt. of CSE REC, Bhopal[2]
Asso. Professor, Deptt. of CSE RIRT, Bhopal[3]
Asst. Professor, Deptt. of CSE REC, Bhopal[4]
roopesh.bist@gmail.com[1], patel.rec@gmail.com[2], yuvrajkrishnarana@gmail.com[3], ravesingh@gmail.com[4]

Abstract: *Wireless network is a most popular technique now days where wireless Sensor network is one of the emerging applications of wireless network. The sensor network uses some kinds of devices. There are large number of devices are used in such type of network. These devices are use to collect the data from sensing the environment. Due to huge number of devices the input data collection is also high. To reduce processing of this data there is a need to narrow the processing space. This is knows as data aggression. As there are many approach 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 WSN.*

Keywords: *Wireless Sensor 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 sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location A sensor node might vary in size from that of a shoebox down to the size of a grain of dust. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attacks. Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. For example, when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations.

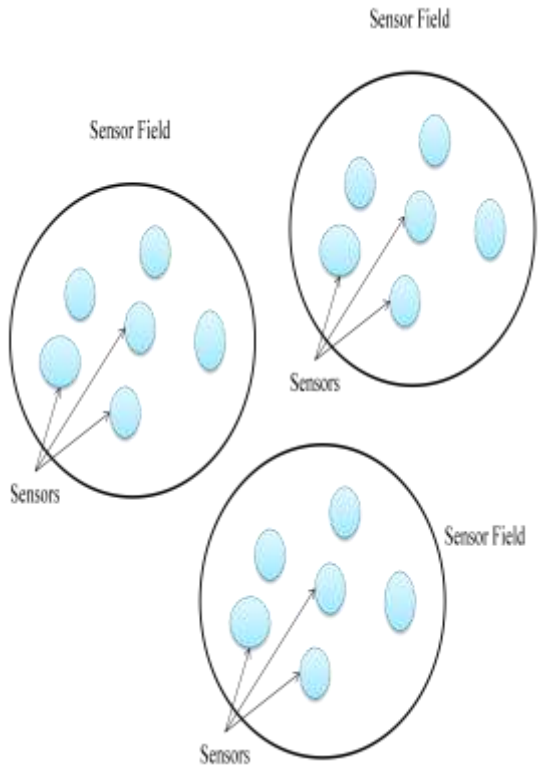

Figure 1:- Wireless Sensor Network

2. DATA AGGREGATION

As earlier section there was a discussion about the sensor network it means there are large number of devices has been used called sensor. Over all these sensor collects the large amount of data. Data aggregation is a mining approach to retrieve the information. Here data will collect, search, and may present.

In wireless sensor network the numbers of sensors are very large. So the processing data is also has been increased. Now this can easily understand that large data means the large processing power. When the processing power will need the battery consumption gets increased.

The solution is the minimized the data. Here the data minimization will do by the data aggregation. The basic goal of data aggregation is to remove the ambiguity from the transmitted data and improve the performance of the system in terms of energy.

3. CHALLENGES IN SENSOR NETWORK

There are many security issues in wireless sensor network. Some of them are discussed below:

A. 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.

b. 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.

c. 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.

d. 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.

e. 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.

4. ENERGY ISSUE IN WIRELESS SENSOR NETWORK

We mainly focus on the distributed (and local) designing algorithms for these problems, where individual nodes perform their own algorithms for computing solutions to a global problems. A distributed algorithm is one in which the nodes individually execute the same algorithm and make decisions accordingly without knowing the general network topology. However, in some distributed algorithms, it is permissible that the nodes can learn some overall information (for example, the number of sensors in the Network and / or the maximum level of the underlying curve). A stronger version of distributed algorithm is known as the local algorithm. Unofficially, a local algorithm, allows a node to communicate only with their neighbors, which are plus a constant jump away to make decisions during the execution of the algorithm

a. Broadcasting issues

Diffusion is a process by which a message generated by a node of the network, is sent to all other nodes in the network. After a simple approach to flooding is inefficient. This is because many useless transmissions (or transmissions only) messages are generated and transmitted in the network, which in turn makes the nodes to quickly dissipate their precious energy. Therefore, we have to design energy efficient algorithms that can prevent or at least reduce the amount of redundant transmissions.

b. Clustering

Clustering is a well-studied topic in the community of sensor networks, where the goal is to divide the entire network in a number of groups (not necessarily disjoint) and select a node in the cluster head (CH) of each group. each Maybe CH is assumed to be active and do all the work of coordination, eg, detection, data collection and data transmission on behalf of the group to the base station, while the other cluster nodes can enter sleep mode. Based on grouping the problems is to minimize the number of CHs, provided of any node in the network or a CH group or at least directly connected to CH. That would leave more detectors in low energy reserve. This problem is also known as the minimum set of key problem. However, like all CHS (even minimal CHS) is busy all the time for detection, processing and transmission of such data, power running quickly, while other nodes (CHS) are not left with a lot of energy.

This causes a significant power supply nodes and reduces disequilibrium web of life. One way to solve this situation is to find a family of disjoint sets of CHs and make iterative assets so that the energy consumption balanced between the nodes of the network.

c. Surveillance Target

Monitoring (also called coverage) is an important and widely studied issue in sensor networks. In general, the main objective of the research in this area is the design of scheduling algorithms, such as the individual sensors in the network slots to indicate that during the time interval that is active during those days are slots allocated to sleep. Given a WSN that monitors certain objectives, it is sometimes possible to find a subset of sensors and encourage them to do the same activity monitoring. So instead of all active nodes for this purpose (which is obviously redundant) we possibly can choose a small subset that can guarantee the same supervision. This observation led researchers to design efficient algorithms so that at any time a small number of nodes are only active for controlling all the objectives in question.

d. Self Protect sensor networks

We study an interesting problem which deals with the provision of the sensors with a level of protection by other sensors. Sensors for monitoring the target, it is often necessary to give a level of protection (additional sensors) so that the sensors can take certain actions when attacks are directed at them. A natural idea is to monitor sensors by neighbors as neighbors can inform the base station when other sensors are in danger (or not working due to a malfunction). We elaborate on this in what follows. Sometimes you may need to know if all the sensors in the network is healthy to do their homework. From a faulty sensor, ie, a defective or compromised sensor cannot report to the base station of your condition, targets controlled by the faulty sensor become unprotected and the system has no way to read about it vulnerability. In this case, we have to find a subset of sensors whose function is to control other sensors, so when all sensors (including themselves) failure or malfunction sensors reported the situation to the base station. The base station and then take appropriate action, such as the deployment of additional nodes to replace those that do not operate continuously to provide protection to these objectives.

5. Routing over Sensor

Routing in sensor networks involves finding a path from the source to the destination, and delivering packets to the destination nodes while nodes in the network are moving freely [5]. Due to node mobility, a path established by a

source may not exist after a short interval of time. To manage with node mobility nodes need to maintain routes in the network. Depending on how nodes establish and maintain paths, routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid, and location-based categories

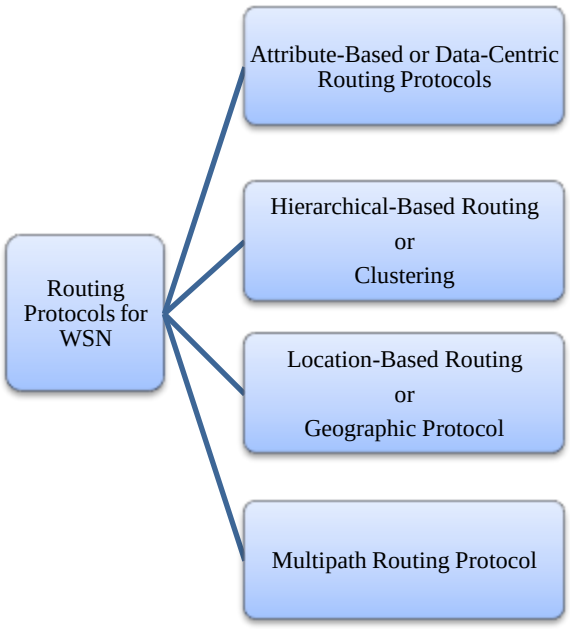

Figure 2:- Classification of Routing Protocol

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 methods are well known techniques with special advantage of scalability and efficient communication. Nodes play different roles in the network. Hierarchical routing maintains the energy consumption of sensor nodes and performs data aggregation which helps in decreasing the number of transmitted messages to base station. The whole WSN is divided into a number of clusters in term with the specific rules.Some hierarchical protocols are discussed 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 capacity of a multi-hop path and the high dynamics of wireless links, single-path routing approach is unable to provide efficient high data rate transmission in wireless sensor networks. Nowadays, the multipath routing approach is broadly utilized as one of the possible solutions to cope with this limitation. This section discusses some of the multipath routing protocols.

6. Related work

As pervasive interconnection of autonomous sensor devices gave birth to a broad class of exiting new applications, security emerges as a central requirement. Wireless sensor networks are vulnerable to attacks as they are frequently deployed in open and unattended environments. In this paper, the author has described the wormhole attack, a severe routing attack against sensor networks that is particularly challenging to defend against. We detail its characteristics and study its effects on the successful operation of a sensor network. We present state-of-the-art [7] research for addressing wormhole related problems in wireless sensor networks and discuss the relative strengths and shortcomings of the proposed solutions. To date, most of the proposed defenses focus on preventive mechanisms that can be applied to protect sensor networks from this kind of attacks. However, no work has been published

regarding the possibility of using more sophisticated methods, like intrusion detection systems, to achieve a more complete and autonomic defense mechanism against wormhole attackers. The author has presented their work on intrusion detection and introduces a lightweight IDS framework, called LIDeA, designed for wireless sensor networks. LIDeA is based on a distributed architecture, in which nodes overhear their neighboring nodes and collaborate with each other in order to successfully detect an intrusion. We conclude by highlighting how such a system can be used for defending against wormhole attackers.

WSNs are multi hop networks, [8] which depend on the intermediate nodes to relay the data packet to the destination. These nodes are equipped with lesser memory, limited battery power, little computation capability, small range of communication and need a secured and efficient routing path to forward the incoming packet. In this paper, we propose a secure cluster based multipath routing protocol (SCMRP). Researchers have proposed clustered sensor networks to increase the efficiency (i.e. increase system throughput, save energy and decrease system delay by data aggregation) and multipath sensor networks to increase the resilience and reliability of the network. The SCMRP is the combination of these two sensor networks; therefore, it provides efficiency as well as reliability and the proper use of cryptographic algorithm provides sufficient security to the sensor network. SCMRP provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc. Further, we have provided a brief analysis to various issues related to key management, orphan nodes, security and energy efficiency.

Wireless sensor networks [9] offer a practical and economically viable alternative to manual data gathering in general and military scenarios, providing a means of surveillance of a region of terrain and providing warning of any threats. However, in hostile scenarios, the network is likely to come under attack from malicious entities which seek to compromise routing diversity in these environments. This paper introduces a low overhead wireless sensor network routing technique which seeks to establish a set of trusted stable routes during the early deployment period of a wireless sensor network, and favor them during future network operation when less trusted devices may be introduced.

It is seen that most of the previous approaches for chose alternate path directly when any node shout down that dropped performance and have relative higher complexity. As the mobile nodes operate on the limited power of battery therefore it becomes very necessary to develop techniques which can successfully maintaining lesser complexity. The objective of this paper is to gives a proposal for a new approach which can successfully maintain the rout with lesser battery power in order to long survival of Sensor network.

7. Conclusion

The study gives an idea about the sensor network. The sensor network uses the huge number of sensor devices. Due to sensing device each node need to process the data. When there is a processing then energy loss will happen. To reduce the energy loss data aggregation can apply. This paper is a review about the wireless sensor network. It also throws some light on the protocol used over WSN.
In future there is a proposal for a new approach which can successfully maintain the route with lesser battery power in order to long survival of Sensor network.

References

[1]. Yong Wang, Garhan Attebury "A survey of security issue in wireless sensor network" IEEE Communications Surveys, • 2nd Quarter 2006

[2]. H. Chan and A. Perrig, "Security and Privacy in Sensor Network IEEE Communications Surveys & Tutorials • 2nd Quarter 2006

[3]. E. Shi and A. Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[4]. I. F. Akyildiz et al., "A Survey on Sensor Setworks," IEEE Commun. Mag., vol. 40, no. 8, , pp. 102–114 ,Aug. 2002.

[5]. A. Perrig et al., "SPINS: Security Protocols for Sensor Networks, "Wireless Networks, vol. 8, no. 5, pp. 521–34, Sept. 2002.

[6]. B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks", SenSys '03: Proc. 1st

[7]. Thanassis Giannetsos, Tassos Dimitriou, Neeli R. Prasad, "State of the Art on Defenses against Wormhole Attacks in Wireless Sensor Networks",pp 313-318, IEEE 2009.

[8]. Suraj Kumar and Sanjay Jena, "SCMRP: Secure Cluster Based Multipath Routing Protocol for Wireless Sensor Networks", IEEE 2010.

[9]. James Harbin, Paul Mitchell and Dave Pearce, "Wireless Sensor Network Wormhole Avoidance Using Reputation-Based Routing",pp 521-525, IEEE 2010.