IJO-SCIENCE

(INTERNATIONAL JOURNAL ONLINE OF SCIENCE)

ISSN: 2455-0108 VOLUME II ISSUE V AUGUST 2016

A Review over Classification and Challenges of Congestion Control in Wireless Sensor Network

Sandhya Yadav

M. tech, Computer Science & Engineering

Technocrats Institute of Technology Bhopal

Deepak Tomar

Asst. Proff, Department of Computer Science & Engineering

Technocrats Institute of Technology Bhopal

Abstract
Wireless Sensor Networks are used to perform distributed sensing in various fields, such as health, military, home etc. Sensing is done in order to have a better understanding of the behavior of the monitored entity or to monitor an environment for the occurrence of a set of possible events, so that proper action may be taken whenever necessary. In, wireless sensor networks, sensor nodes should communicate among themselves and do distributed computation over the sensed values to identify the occurrence of an event. The aim of this paper is to present the review of recent sensor network here we have discussion regarding the protocol stack of WSN and various network services and congestion control on WSN.

Key words: - Wireless Sensor Network, Classification, Congestion Control, Sensor Node

I. INTRODUCTION

Wireless sensor networks (WSN), has been focused by many researchers, in order to developers applications for the end user in recent years [1]. WSN have the potential for numerous applications in a wide range of areas, such as military target tracking and monitoring, disaster management, biomedical health monitoring, exploration of hazardous environments, and seismic detection. The type of unstructured WSN, sensor nodes can be deployed in about ad hoc basis in a field, many challenges imposed on network designers who are routing protocols for the development of these networks. [2] In particular, the design of routing algorithms for wireless sensor networks have to solve many problems because of its special features, be distinguished from mobile ad hoc networks (MANET), such as the inability to get an overview Global addressing requirements of most applications -To the sensor nodes send the data to a special sink node, redundancy in the data traffic generated by multiple nodes, sensors and the limited capacity of the node in terms sensors transmit power, with embedded energy, processing power and storage space.

In general, a routing technique may be either a single path or multiple paths constructed between a source and a destination. A unique approach routing path is generally simpler and cheaper to build. However, only one routing path in the sensor network does not provide the reliability required for the manipulation of data. From a routing path may select the same diversion of nodes each time a source node transmits a packet to the sink, the limited power resource is exhausted these nodes before other nodes and cause a network partition. In addition, sensor nodes are vulnerable to failure devices due to many factors, such as the reliable wireless communication, or an unpredictable disk for the deployment environment. In addition, a multi routing is characterized by

A wireless sensor network is a group of specialized transducers with a communication infrastructure for the conditions of monitoring and recording in different locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, the intensity of the lighting, the intensity of vibration, sound intensity, voltage line feed, concentrations of chemicals and pollution levels vital body functions.

II. WIRELESS SENSOR NETWORK

Wireless sensors WSN also known as the network of sensors and wireless player [1] is a independent spatially dispersed sensors to supervise substantial or ecological circumstances such as temperature, sound, pressure, etc., and spend the cooperative data through the network to the home page

A network of stations called multi-sensor detection sensor nodes, each of which them are small, light and portable. Each node is equipped with a sensor adapter, microcomputer, transceiver and power supply. Here the Adapter generates electrical signals depending on the effects of the detected physical phenomena. Microcomputer executes the operations and stores the output. Based on the command is received from the transmitter and receiver host or sensors In this type of network each node derives its power from the battery sensor. Sensor network consists of multiple stations called detection sensor nodes, each of which is small, light and portable. Each node is equipped with a sensor adapter, microcomputer, transceiver and power supply. Adapter generates electrical signals depending on the effects of the detected physical phenomena. Microcomputer operations and stores the sensor output. Command is received from the transmitter and receiver host computer and transmits the data to that computer. And each node derives its power from the battery sensor.

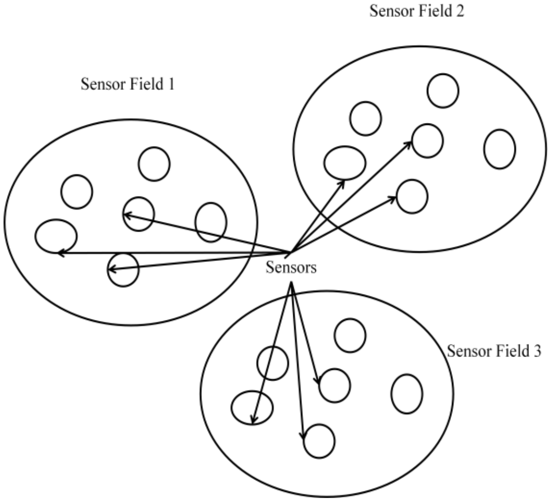

Figure 1 Wireless sensor Network

III. CLASSIFICATION OF WSN

WSNs have maximum likeness with Mobile Ad-hoc Networks (MANET). WSNs also create network that contains sensor nodes connecting with each other, in an Ad-hoc style and no accurate communications is there for both but WSNs have the collection of data with the sensor nodes but MANET might or might not use sensor nodes. In this paper, we gave the description of WSNs and its types with the text analysis, as shown in the Figure 1. WSNs consist of tiny and low power sensor nodes that collect data through petite sensors, process the data and propel to exacting setting. We also describe the types of WSNs with the research work. We incorporate the flaws of accessible technology or in a fastidious type and how we can cover those open holes by using various techniques, protocols or algorithms.

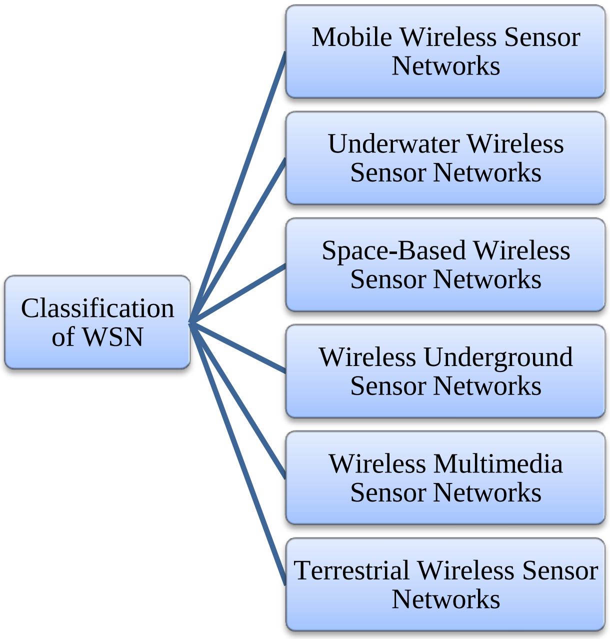
Classification of WSN
Mobile Wireless Sensor Networks
Underwater Wireless Sensor Networks
Space-Based Wireless Sensor Networks
Wireless Underground Sensor Networks
Wireless Multimedia Sensor Networks
Terrestrial Wireless Sensor Networks

Figure 2 Classification of WSN

Mobile Wireless Sensor Networks

Generally it seems to be that the mobile network is like the static network but MWSNs can be explain as type of a Wireless Sensor Network that have the sensing nodes having the capacity of mobility with compared to the usually used WSN where the nodes have the sensors but in a static mode. MWSNs have more versatility than the static

Underwater Wireless Sensor Networks (UWSNs)

Underwater wireless communication network or UWSN creation is a huge challenging task It seems to be that the Radio Frequencies and acoustic waves having narrow bandwidth are highly dynamic in water. There is alternative or temporary solution is the use of optical communication, with respect to short range distance. But this approach is a quite difficult to implement and maintain it.

Space-Based Wireless Sensor Networks (SB-WSNs)

The wireless sensor networks have the micro sensors in order to monitor and gathering of data for some of the environment parameters like pressure, temperature, voice, here such networks may be accessed for space purposes in implementation of wireless sensor networks within a spacecraft in single probe missions or in order to interchange electrical wires.

Wireless Underground Sensor Networks (WUSNs)

Wireless Underground Sensor Networks are the unique and advance enhancement of a traditional wireless sensor network. There are lots of connectivity issues in WUSNs' architecture. These connectivity problems may not be discussed in past. So that there is a need of a mathematical model in order to study and examine the WUSNs, based on probabilistic connectivity theory.

Wireless Multimedia Sensor Networks (WMSNs)

Multimedia wireless sensor networks (WSN list) consist of tiny sensors that can detect compute nodes,, action, communicate, and control-have component. Several applications of multimedia wireless sensor networks (Wmns) are FIN, home monitoring, traffic management systems and ecological monitoring of leakage; kind of these applications involving effective communication of events and media events functions as saying the image, audio and video

Terrestrial Wireless Sensor Networks (TWSNs)

Most generally the Terrestrial WSNs contains hundreds to thousands of cheap wireless sensor nodes installed in a given geographical area. This development can apply on Ad-hoc network. Here 2-D and 3-D placement models can be apply.

IV. WSN SECURITY AND SECURITY ISSUES

Commonly WSNs are used to gather information from a variety of locations of physical world and also they are deployed in controlled and uncontrolled environment [3]. So by their applications and deployment nature Wireless sensor networks are ultimately insecure. These networks have numerous limitations like node (less computational power, less memory, less energy etc.), network (because they are acting as mobile as hoc network) and physical (deployed in different environments like public and hostile) limitations which makes them supplementary vulnerable to various security attacks. Ad hoc nature of sensor networks opens the unique challenges to the reliability and security. Owing to the limited computational and processing constrains traditional security techniques and policies are not suitable in order to maintain confidentiality, Authentication, Availability and Integrity in WSN, s

Wireless sensor networks are a collection of small, autonomous devices with wireless networking capabilities. Rapid development of wireless technology, the Sensor network has emerged as a new type of wireless network. The world today is living a combat, and the battle field lies on the roads, the estimated number of deaths is about 1.2 million people yearly worldwide [4, 8,]. Sensor network are new type of networks which are expected to support a large spectrum of mobile distributed applications. A sensor network is a collection of mobile nodes or routers connected with an automatic system. There nodes does not user any wired media as a link. Sensor network is type of wireless network so it uses the wireless links. The combination of this structure makes the random graph having vertices and links. Here node can freely moves anywhere in the network so it also change the location of node in graph. This is a major cause by which the network can use without pre analysis [2].The attacks can be classified in many ways. Some of them has discussed below. In figure there is a basic classification of attacks happened in sensor network

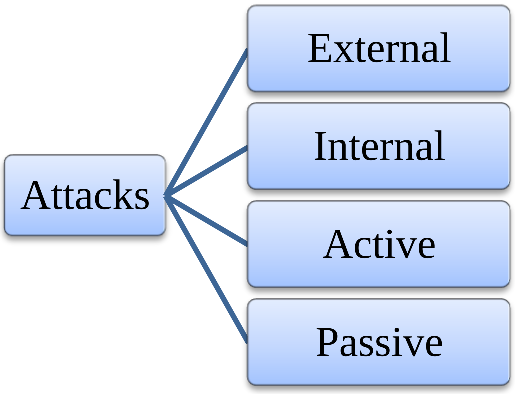

Figure 3 Attacks in WSN

- **External Vs Internal Attack**

The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks [6, 7]. Nodes that do not belong to the domain of the network carry out external attacks. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more harmful when compared with outside attacks since the insider knows valuable and secret information, and possesses confidential access rights.

- **Active Vs Passive Attack**

The attacks in sensor network can generally be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a sensor network, [7, and 8]. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

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.

V. CONGESTION CONTROL

Many wireless sensor network applications require readings or observations gathered by the sensors can be stored in a central location. Congestion can occur when collecting data and sending it to the area of the city center for the wireless sensor network. Congestion occurs mainly in the direction-sensors-sink when packages are shipped the highest number to one. Congestion in sensor networks has a negative impact on network performance and purpose of the request, namely the loss of blind packet, increased packet delay, waste of energy and the knot of the degradation of the severe fidelity. The goal of WSN congestion control to improve network performance, reduce the delay time of the data transmitted. Under these conditions, the energy node, a communication bandwidth, computing power and other network resources in general is limited. You can improve network performance by balancing protocol design, choose the path algorithm, integration and loading data, and so on.

There are two basic Congestion types in Wireless Sensor Networks as given below

- **Node-level congestion:**

The node-level congestion that is common in conventional networks. It is caused by buffer overflow in the node and can result in packet loss, and increased queuing delay [4].

- **Link-level congestion:**

In a particular vicinity, stern conflicts could crop up when manifold active sensor nodes within range of one another endeavor to pass on at the similar instance. Packets that leave the buffer might fail to reach the next hop as a result of collision. This sort of congestion reduces both link deployment and overall throughput, while increasing both packet delay and energy waste [5] [6].

VI. LITERATURE SURVEY

Wireless sensor network (WSN) [6] is an ad hoc network of sensor nodes with limited computing power equipped with a radio transceiver. The main limitation of the sensor node limits of its power source in the form of short battery life. Conserve battery power is very important in sensor device and battery life is often a crucial element in the extension of the life of the sensor network. Thus the energy conservation techniques must be analysis when the network has been design. The problem is how to reduce energy consumption to increase the battery life of the network has been studied extensively. But most of the curriculum focuses on choosing the shortest route or energy-saving guidance, and leaders often change based on the remaining energy contract, the optimum size of the box to lengthen the life of the network. Here the author has worked to control congestion and reduce collision package, however, to avoid congestion in the network of sensors did not receive serious consideration until recently. The document describes the topology of the network by avoiding congestion or catopology.

A PCR-based congestion avoidance [7] (CA) and built VPN suggests (VNT) restructure and progress (CA-VNTR) routing scheme and detailed CA-VNTR algorithm. Carried out a simulation of the proposed method compared with conventional guidance in terms of resources and prevent the possibility of a useful scheme. The results showed that the method of CA-VNTR of traditional routing blocking probability, especially in light of the heavy traffic load.

The congestion control in wireless sensor networks (WSN) [8] is always a big challenge as the struggle for storage medium and is limited in the contract leads to packet loss through collisions and buffer overflows. The problem of congestion is more difficult multi-hop networks, network necessary when a large display area compared with the communications group in the individual nodes and the network is ad hoc in nature. The goal is to design the guidance system that reduces congestion in these networks without increasing the communication overhead. Often these networks are used to access medium and Sense multi-carrier access control protocols with Collision Avoidance (CSMA / CA) that require a sensor to listen to the medium using a technique hearing. In this paper proposes blueprint directive energy efficiency multi-hop wireless networks of sensors and a network topology. Here, the sensor node is used to listen to predict the occurrence of congestion in the neighboring glands by estimating the buffer professions each (and lined up a number of messages in the buffer). This information is used directly in the directive. The benefit of this approach is a noteworthy diminution in the standard obstruction which leads to a decrease in the number of packages and thus reduces the average delay transmission along with no additional overhead communications to implement the plan. It demonstrates the effectiveness of simulation software.

Congestion control of TCP [9] Vegas is more stable and brighter than the other versions of TCP Westwood plus as a result of congestion control before the collision in an ad hoc network with frequent topology changes. However, Las are less competitive ability when the data flow coexists with other protocols. Also, you cannot make the most of the available packages for the transfer bandwidth. The research aims to propose TCP Vegas, ICATCP, which includes three stages of the improvement in the aspects of improving avoid congestion. And it will take the first lower layers parameters "into account in the performance model to improve the accuracy of the theoretical yield. II. Uses an indicator to the front of the review based performance to predict gray to enhance the line of control cwnd. III. Explore the optimal mechanism to Q- learning basis find more reasonable change is implemented the size of the congestion window. The simulation results show that ICATCP has a higher throughput, delay and shorter and more equitable distribution of bandwidth Las Westwood plus customized scenarios multihop.

Dragonfly networks [10] are built on the scope of the data center and HPC attractive networks, which provide high performance with low Qatar at moderate cost. However, they are prone to congestion in certain types of frequent traffic cluttering links specific network. Is minimal steering adjustment can be used to avoid such congestion. This type of guidance is used longer paths to avoid the crowded local or global bonds however, if the use of a mechanism to avoid the deadlock on the basis of the distance, and ask for more virtual channels (VC), which increases the design complexity and cost. Ofer (on-the-fly routing adjustment) is proposed previously that the road to separation and VC to avoid a recession, making misrouting local and global prices are reasonable. However, the severity of congestion with Ofer goes greater because it is based on the exhaust subnet low bandwidth half-life. In addition, Ofer misrouting allows unlimited secondary network of exhaustion, leading to endless road network and long latencies. We propose and evaluate Aovr- CM, a variant of Ofer along with a simple congestion management and is based on (CM) only on local information mechanism, specifically credit account O ports on the local router. Subnets with simple exhaust Hamilton as a ring or tree, exceeding the previous Ofer proposals to avoid deadlock at the distance. Moreover, despite allowing a long ways in theory, in practice the packets arrive at their destination in a few jumps. In total, Aovr- CM is the earliest possible date for the misrouting supports both local and global networks mechanism dragonfly.

VII. CONCLUSION

Wireless sensor networks, an emerging technology, is expected to change our lives in the near future. Wireless sensor networks (WSN) are used in numerous applications like ecological monitoring, infrastructure defense, healthcare applications, and traffic control. The blueprint concerns of such applications must speak to related challenges around WSN uniqueness on one hand and the applications on the other. This Paper gives a birds' eye on design principles, scalability, security and power saving issues with QoS. And conclude most of its issues by tradeoffs with QoS, there is a lot of research yet to be carried out before a perfect middleware for WSN can be built and tested.

VIII. REFERENCES

[1] Gaddam, A.; Mukhopadhyay, S.C.; Sen Gupta, G.; Guesgen, H., "Wireless Sensors Networks based monitoring: Review, challenges and implementation issues," in *Sensing Technology, 2008. ICST 2008. 3rd International Conference on* , vol., no., pp.533-538, Nov. 30 2008-Dec. 3 2008

[2] Popovici, E.; Magno, M.; Marinkovic, S., "Power management techniques for Wireless Sensor Networks: A review," in *Advances in Sensors and Interfaces (IWASI), 2013 5th IEEE International Workshop on* , vol., no., pp.194-198, 13-14 June 2013

[3] Singh, J.; Kumar, R.; Mishra, A.K., "Clustering algorithms for wireless sensor networks: A review," in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* , vol., no., pp.637-642, 11-13 March 2015

[4] Soumyasri, S.M.; Ballal, R., "A review: Preserving privacy in wireless sensor networks," in *Research & Technology in the Coming Decades (CRT 2013), National Conference on Challenges in* , vol., no., pp.1-7, 27-28 Sept. 2013

[5] Kalore, S.V.; Rewagad, P., "A review on efficient routing techniques in wireless sensor networks," in *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in* , vol., no., pp.803-807, 19-20 March 2015

[6] Dasgupta, R.; Mukherjee, R.; Gupta, A., "Congestion avoidance topology in wireless sensor network using Karnaugh map," in Applications and Innovations in Mobile Computing (AIMoC), 2015 , vol., no., pp.89-96, 12-14 Feb. 2015

[7] Hui Ding; Min Zhang; Jiuyu Xie; Lifang Zhang; Jie Zhang; Xue Chen, "PCE-based Virtual Network Topologies reconfiguration and congestion avoidance routing scheme for optical networks," in IEEE International Conference vol., no., pp.1-4, 21-23 Oct. 2011

[8] Sett, R.; Banerjee, I., "An overhearing based routing scheme for Wireless Sensor Networks," in Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on , vol., no., pp.2076-2082, 10-13 Aug. 2015

[9] Ying Luo; Minyong Yin; Hong Jiang; Shaoliang Ma, "An improved congestion avoidance control model for TCP Vegas based on Ad Hoc networks," in Control and Decision Conference (2014 CCDC), The 26th Chinese , vol., no., pp.2310-2314, May 31 2014-June 2 2014

[10] Garcia, M.; Vallejo, E.; Beivide, R.; Valero, M.; Rodriguez, G., "OFAR-CM: Efficient Dragonfly Networks with Simple Congestion Management," in High-Performance Interconnects (HOTI), 2013 IEEE 21st Annual Symposium on , vol., no., pp.55-62, 21-23 Aug. 2013