Analyse:- Secured and Reliable Data Transmission On Multi-Hop Wireless Sensor Network using Multi-Hop Based Congestion Avoidance Technique

Sujitha S
Assistant professor
Department of CSA and SS
Sri Krishna arts and science college

R.Surya Prabha
Assistant professor
Department of CSA and SS
Sri Krishna arts and science college

Abstract

In multi-hop wireless networks, route stability is very challenging task and major research problem. The routes in this network are frequently breaks presence of malicious nodes, faulty nodes, or due to lack of energy of intermediate nodes. Hence there should be the hybrid approach in which route stability should be achieved by considering all the causes of frequent routes failure. Wireless Sensor Network will be the future of communication and it plays the vital rule of super internet in the future were all data are powered by wireless communication for transmission. In this paper going to discussed about multi-hop based congestion avoidance technique, key challenges and routing protocol design.

Keywords: Efficiency, Energy, Multi-Hop, Fault Tolerance.

1. Introduction

Wireless Sensor Network is a set of sensor nodes which is used to monitor physical or environmental conditions and the data which is sensed is then processed, computed, aggregated and finally it is passed on to the main location called base station. The base station or sink node is the central location where the collected data from all other sensor nodes is stored and the data can be retrieved for future use. The main advantages of WSN are the sensor nodes can be place in non-reachable areas such as deep forests, there is no need for any fixed infrastructure for a network setup, rural areas, etc., avoids wiring, supports node mobility and heterogeneous nodes, low cost for implementation and able to withstand even in wild environmental conditions. The applications of WSN include tracking, environment monitoring, healthcare monitoring, landslide detection, traffic monitoring, forest fire detection, other natural disaster monitoring and etc. In WSN, the energy of nodes gets discharged based on the transmission and reception of both data and control packets. Since WSN is battery operated, in hostile environment the recharging of node's battery is not an easy task, so the energy consumption parameter is taken into account for most of the research for the improvement of the lifetime of the network. So, in order to prolong the lifetime of the network the

existing routing protocols should be selected efficiently for the type of network to be implemented. Since, routing protocols works optimally for certain network topologies. In multihop wireless networks, when a mobile node needs to communicate with a remote destination, it relies on the other nodes to relay the packets. This multihop packet transmission can extend the network coverage area using limited power and improve area spectral efficiency. The multihop wireless network implemented in many useful applications such as data sharing and multimedia data transmission. It can establish a network to communicate, distribute files, and share information. However, the assumption that the nodes are willing to spend their limited resources, such as battery energy and available network bandwidth. The applications like military and disaster-recovery, the nodes' behavior is highly predictable because the network is closed and the nodes are controlled by one authority. However, the nodes' behavior is unpredictable in civilian applications for different reasons. The nodes are typically autonomous and self-interested and may belong to different authorities. The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission. Multihop wireless network are frequently used in many real life applications. The communication in such networks is based on routing protocols in which the communication between two remote nodes is done by other intermediate nodes. Therefore this creates the chances security threats during the packet transmission from one node to another. All nodes in network are battery constraint hence the routes may break if the battery of any node expires. Similarly the malicious node also frequently breaks the current routes. Due to the uncertainty of nodes behaviour, random selection of intermediate nodes will resulted into routes stability degradation. It will also endanger the reliability of data transmission and degrade the network performance in terms of packet delivery ratio (PDR). Only one intermediate node can break a route, and a small number of incompetent or malicious nodes can repeatedly break routes. When a route is broken, the nodes have to rely on cycles of time-out and route discoveries to re-establish the route. These route discoveries may incur network-wide flooding. of routing requests that consume a substantial amount of the network's resources.

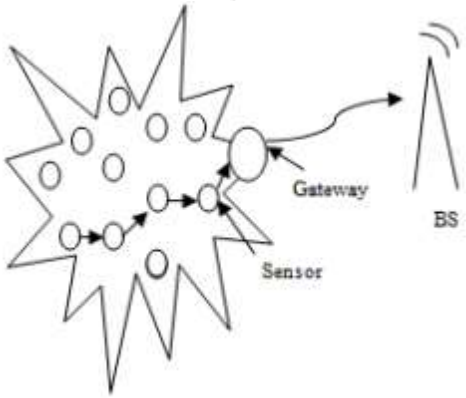

Figure 1: Wireless Sensor Network

Latency between the devices provides the best way on understanding connectivity security of wireless sensor network. All the latency approaches are possible avenue that can provide clarity on how we can determine the solution of securing the nodes between devices. Wireless Sensor network share the same connection property like computer network. The connectivity between computers to another computer is the simplest example of how network works. When typical network of computers connect with each other, they are govern by different rules and policy. On the other hand, the connection that appears and present between the two devices on how and why they are connected is empowered by occurrences of different factors. One of the main factors is nodes latency communication. Now on this research paper, the researchers going to discuss several security issues governing latency that govern networks. Sensor networks are expected to play an essential role in the upcoming age of pervasive computing. Interference on nodes between devices while in connection result to failure on latency configuration. Failure of stabilizing the configuration into normal state of connection latency when sending devices and receiving device transmits nodes. Inability of devices to develop latency security protocol during the devices attempts to re-connect. Establish an advance mechanism between connected devices when connection are attempted to be interfered through means of distance. Create minimum and maximum latency volume that will stabilized the connection latency of a devices which is connected to another device. Develop security protocol for latency security to devices that attempts to re-connect on other devices.

2. Literature Survey

Jilani Sayyad and Dr.N.K. Choudhari gave an overview about the types of congestion in WSN. There are two types of congestion in WSN which are node level congestion and link level congestion. The node level congestion arises when the input buffer or output buffer of node is overloaded which results in dropping the packets and increased queuing or processing delay. Because of the packet loss in node level congestion which leads to retransmission of packets thereby it consumes additional amount of energy. Link level congestion is caused when several active sensors in the network try to access the channel at the same time since wireless channels are shared by multiple nodes by using carrier sense multiple access (CSMA) protocol. This second type of congestion reduces both effective utilization of the link and overall throughput and also increases the packet service time. So this type of congestion also consumes additional energy. **K. Liu, J. Deng, and K. Balakrishnan** presented another reputation based method in order to eliminate using the channel overhearing technique based on two-hop ACK technique. NA accuses its neighbor NB of dropping a packet, if NA does not receive an ACK packet from the two hop-away nodes NC. Reputation-based schemes suffer from false accusations where some honest nodes are falsely identified as malicious. This is because the nodes that drop packets temporarily, e. g., due to congestion, may be falsely identified as malicious by its neighbors. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is

malicious. However, this increases the missed detections where some malicious nodes are not identified. Moreover, tolerant threshold enables the nodes with high packet dropping rate to participate in routes, and enables the malicious nodes to circumvent the scheme by dropping packets at a rate lower than the scheme's threshold. When a node's reputation value is above the threshold, it does not have incentive to relay packets because it does not bring more utility. **P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle** have proposed a human-based model which builds a trust relationship between nodes in ad hoc network. Without the need for global trust knowledge, they have presented a protocol that scales efficiently for large networks. **M. Yu and K. Leung** a secure routing protocol with quality of service support has been proposed. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes and the quality of service of the links along a route. There are many other methods proposed for security.

3. Multi-Hop Based Congestion Avoidance Technique

To avoid the congestion in wireless network for continuous data transmission and also for a large network topology, the multi-hop clustered topology is proposed. Moreover, compared to single wireless links, the proposed multi-hop wireless links have several benefits such as network coverage is extended, availability of several paths which improves the robustness of the network and also the requirement of the transmission power for several short links is less than the single long link. Figure 2 shows the clustered topology as multi-hop routing. For a multi-hop connectivity, there are one or more intermediate nodes along the path from source to destination which receive data and forward through wireless links. Here routing protocol is used to find the efficient path from source to destination. So, in order to select a good routing protocol for a multi-hop network, initially the performance analysis of proactive and reactive routing protocols has been performed for the parameters such as energy consumption, packet delivery, delay and total number of hops.

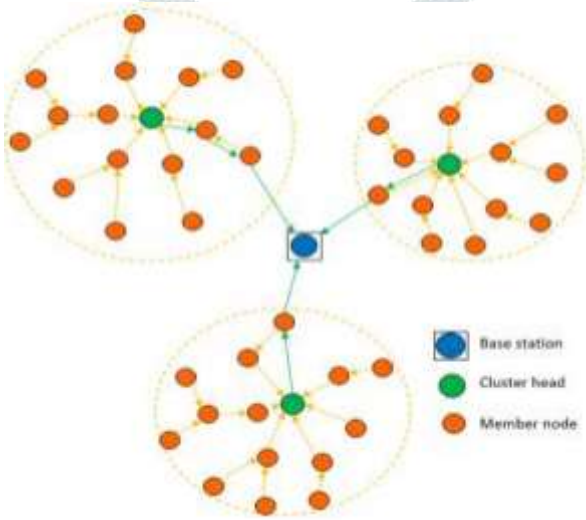

Figure 2: Multi-Hop Topology

Assumption model

- Static clustering topology as multi-hop routing is used
- In static clustering, initially nodes are placed in the clustered form
- All the nodes have fixed position, so it has fixed x and y coordinates
- In each cluster, the cluster head (CH) is selected.
- The node which has the maximum energy and also minimum distance to all other nodes in the cluster is selected as the cluster head (CH)
- CH collects the data from its member nodes and the aggregated data is forwarded to the base station
- For a multi-hop clustering topology, the member nodes in the cluster chooses an optimal path to reach its CH and also the aggregated data is transmitted through an optimal path from CH to the base station.

4. Key Challenges in Multi- Sensor Network

Some of the issues that must be taken into consideration when designing protocols for use in multi sensor networks.

A. Data gathering:

Each sensor transmits and receives one data packet per unit time to the sensor or base station. It consumes a lot of energy when it transmits or receives a data. Because a sensor having a small battery, limited amount of energy available in one or more sensor node.

B. Energy enhancement efficiency:

Sensor nodes are considered that having of very less energy When the energy of a node depreciates, the node will die and this may cause the network to become partitioned – a situation whereby communication gaps exist in the Sensor network protocols must therefore be energy-efficient so as to extend the network lifetime and usefulness of the network.

C. Hardware constraints:

As Sensor node consists of sensor, processor and radio unit and its stringent, this hardware is available at all times according to need of the prospect.

D. Communication media:

Sensor nodes generally communicate over a shared wireless transmission medium because the environment in which they are deployed in does not allow for infrastructure (such as centralized base

stations or wires) to be setup easily. Depending on the environment that the sensor nodes operate in, different transmission media may be used.

E. Security:

A WSN are deployed in unattended area where every time quick eye is not there so security and privacy is the prime concern in WSN, some integrity keys are ascertained in order to provide security measures in WSN.

F. Data Quality:

The data quality is mean which type of data is require in network to increases the network life time and consume less energy. The data quality is based on the data consistency, data accuracy, timeliness and completeness. The data Consistency means which data stream is satisfy the user-defined model. This model is based on specific application. Data accuracy means intermediate processing such as difference between the sample value and the true value numerical measured. Timeliness means how much time is required for receiving a data to sink. It is based on network latency and reliability. Completeness is a property of a stream, it reflects if a node has taken a sufficient number of samples to reconstruct the measured.

5. Routing Protocols Design

The routing protocols designed for WSN should consider the goal, application area, and architecture of the network. The design of routing protocols is influenced by many challenging factors caused by the nature of the WSNs are:-

1. Node Deployment: Node deployment can be random, deterministic or self organizing. For deterministic deployed networks the routes are pre-determined, however for random deployed networks and self-organizing networks route designation have been a challenging subject.

2. Energy consideration: Since the life-time of the WSN depends on energy resources and their consumption by sensors, the energy consideration has a great influence on route design. The power consumed during transmission is the greatest portion of energy consumption of any node. Direct communication consumes more power than multi-hop communication; however the multi-hop communication introduces extra topology management and medium access control.

3. Data Delivery Models: Data delivery model depends on the application and can be continuous, event-driven, query-driven, or hybrid. In continuous model of delivery, each sensor sends the data periodically.

4**. Data Aggregation:** Since the sensors are densely deployed by definition, the data gathered from each node are correlated. Therefore data aggregation or in other words data fusion decreases the size of the data transmitted.

5. Fault Tolerance: WSNs are prone to failures; some of the nodes may fail or be blocked by physical interference, physical damage, or lack of power. The routing protocol has to be dynamic; failures of specific nodes should not affect network operation.

Latency Ratio

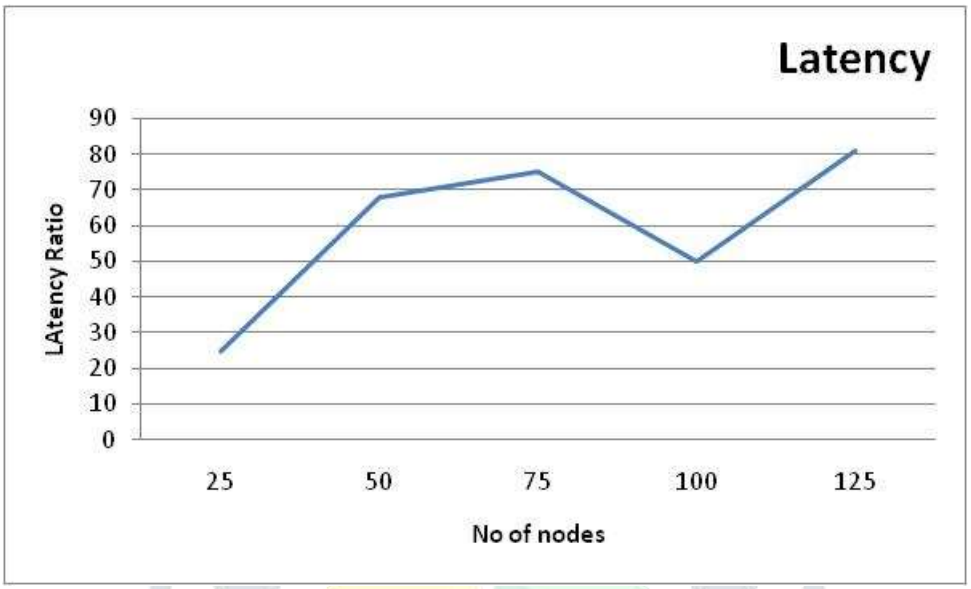

Figure 3: Latency Ratio

Figure 3 represents latency ratio refers to the time required by the network to operate until the first sensor node or the group of nodes in the network runs out of energy. The simple definition can be given as the overall network lifetime as determined by the remaining energy in the network.

Traffic Ratio

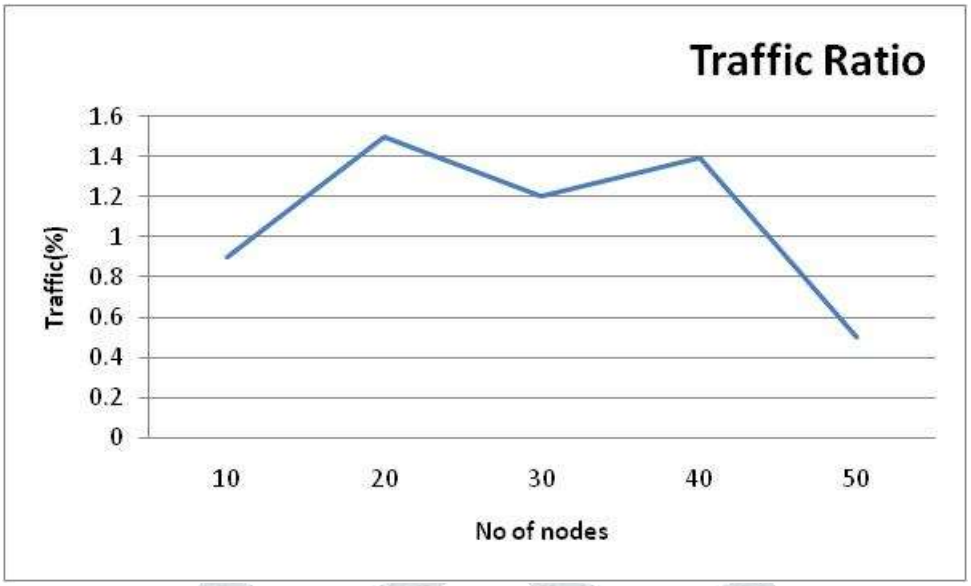

Figure 4: Traffic Ratio

Figure 4 represents denotes the time taken for transmitting the packet from source to destination across a network. The transmission is generally caused due to queuing and retransmission owing to collision.

Scalability

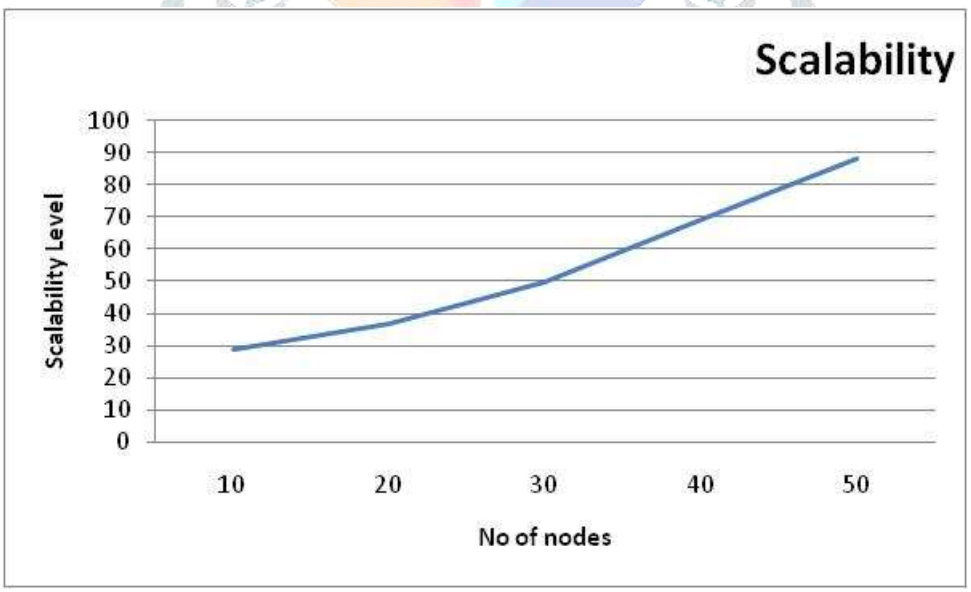

Figure 5: Scalability

Figure 5 represents scalability values of multi-hop based congestion avoidance technique. Their graph values are displayed into low to higher so that scalability values are increased into their process.

Throughput

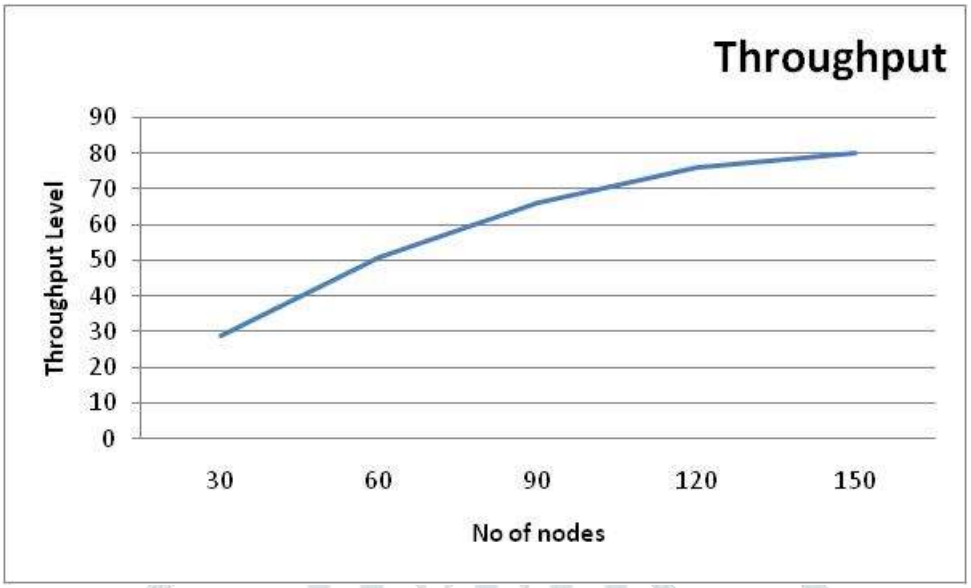

Figure 6: Throughput

Figure 6 represents Network throughput denotes the typical ratio of successful packet delivery over a message channel. The network throughput is measured in bits per second (bit/s or bps) and the higher throughput signifies the better performance.

Conclusion

Spatial reusability aware routing can efficiently improve the source to destination communication with high end throughput in multi-hop wireless networks, by carefully considering spatial reusability of the wireless communication media. In this paper analysed and some techniques, methods algorithms, protocols design, key challenges for enhance the multihop data transmission. Each one method or algorithm have some performance ratio not only the advantages and also have some drawbacks within that. In future work will choose any one algorithm which is most secure and suitable to do better accuracy for network security process and then apply some enhancement within that to proof much better than the old performance.

References:

[1] Jilani Sayyad and Dr.N.K. Choudhari, "Congestion Control Techniques in WSN and Their Performance Comparisons", International Journal of Multidisciplinary and Current Research, vol.3, February 2015.

[2] K. Liu, J. Deng, and K. Balakrishnan, "An AcknowledgementBased Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536- 550, May 2007.

[3] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model," IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[4] M. Yu and K. Leung, "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1888-1898, Apr. 2009.

[5] Jasleen Kaur, Kamaljit Singh Saini, Rubal Grewal, "Priority Based Congestion Avoidance Hybrid Scheme for Wireless Sensor Network", 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5, September 2015.

[6] Anu Arya, Jagtar Singh,"Comparative Study of AODV, DSDV and DSR Routing Protocols in Wireless Sensor Network Using NS-2 Simulator", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 4 , 2014.

[7] B.N. Jagdale, Pragati Patil, P. Lahane, D. Javale, "Analysis and Comparison of Diatance Vector, DSDV and AODV Protocol of MANET", International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 2, March 2012.

[8] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[9] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011

[10] Maryam M. Alotaibi and Hussein T. Mouftah, " Data Dissemination for Heterogeneous Transmission Ranges in Vanets", IEEE Conference on Local Computer Networks, pp.818-825, 2015.