ISSN 2063-5346

AN DYNAMIC APPROACH FOR PACKET RECOVERY FROM LOSS AT BUFFER OF ROUTER SYSTEM IN WIRELESS SENSOR NETWORK

John J P[1], C K Narayanappa[2]

[1]Research Scholar, Dept of CSE, MSRIT, Bengaluru, Karnataka, India

johnypaul10@gmail.com

[2]Prof & Head, Dept of Medical Electronics, MSRIT, Bengaluru, Karnataka, India

c_k_narayanappa@msrit.edu

Article History: Received: 03.04.2023 **Revised:** 25.04.2023 **Accepted:** 15.05.2023

Abstract

Today's WSN(Wireless Sensor Network) is a network of spatially dispersed sensors that communicate with one another. Enterprise applications including email, security, backup/DR, and servers are all provided by WSN and are distributed over the Internet. The main issues that streaming media applications in WSN experience are congestion and packet loss. This issue happens when the sensor receives traffic that is greater than it can handle in terms of packet loss, delay, and overall quality. One technique for gathering lost packets and retransmitting them to the destination in order to improve network performance and reliability is buffering at the routers. Dynamic content, whose creation is altered dynamically in response to a user's request, has recently become widely used throughout the across the sensor nodes. By using buffering at the routers between the server and the user, this article presents a technique for rapidly reacting to the dynamic information of numerous sensor nodes. The proposed approach makes use of the router's buffering strategy to retransmit data that was lost on the network and to recover from packet loss.

Keywords:WSN, Packet Loss, Loss Recovery, Dynamic Contents, Buffer, i-Leach, M-Leach, M-Gear.

1. Introduction

Today, the field with the fastest growth is wireless sensor networks. Even yet, many applications of Sensor Nodes are not safe and introduce unnecessary delays to the delivery of data. The challenge of making dynamic content more responsive in WSN is compounded by the fact that it is transported from the source to the destination. A router that is near to the users can buffer dynamic network content. Data loss occurs during data transfers from source to destination for a number of network-related reasons. Data packet loss recovery in a WSN involves

retransmitting a previously lost packet to its intended recipient by using a number of recovery methods. Every packet is significant if an application is time-sensitive. We can retrieve the missing packet using a variety of methods. A variety of factors can cause data loss.

A network of Senor Nodes interacting with one another is a WSN. Through the router, they are exchanging data with one another. Every router maintains a buffer to manage the dynamic contents that are transferred over the network. Any network should be dependable and environmentally friendly. When a sensor node communicates, a data travel through a number of routers, but not all of it reaches its destination. There may be occasions when the data rate is really high. Data loss is a concern in WSNs because traffic is not distributed uniformly across the nodes. A loss recovery system must improve reliability and packet delivery ratio while reducing packet loss ratio and managing memory. By utilizing various approaches, such as dynamic buffering at the router node, data packet loss recovery can be accomplished and reliability can be preserved.

The WSN offers dynamic information that is available instantly, adaptable, expandable, and cost-effective for businesses to use. It offers others on-demand access to shared virtualized IT resources. WSN is no longer as safe and secure as it once was in recent years. However, nowadays, cybercriminals can more easily access WSN data by infecting the Sensor Nodes with malicious software. Data loss results from this. They have access to all confidential files and papers. Websites are taken down. The suggested method makes use of a dynamic buffer at routers to get over the aforementioned issue. To prevent data loss, the buffer saves frequently used dynamic material and retransmits it in the event of a packet transmission failure.

2. Related Work

The rate control method for wireless networks that stream data is a crucial subject for research. Many strategies are used to keep the transmitting rate consistent. The cross-layer method described in [5] employed the physical layer ARQ ACK information to distinguish between congestion loss and wireless loss. It was possible to adapt the congestion management approach for usage in wireless networks by distinguishing between packet loss caused by signal fading and congestion-related packet loss [4].

LEACH adopts an idealistic perspective by treating each node's energy as though it were uniform across the board. Because spherical uneven nodes are particularly attached to numerous cluster heads, a cluster head with a large number of member nodes will expend more energy in this case than a cluster head with a smaller number of linked member nodes. Mobility support is another issue with the LEACH routing protocol; M-LEACH is recommended in[3] as a solution.

Both non-cluster-head and cluster-head nodes are mobile during M-setup LEACH's and steady-state phases. Based on the node's remaining energy, M-LEACH selects the cluster head. Like other clustering routing systems, the M-LEACH routing protocol has a number of presumptions.

In terms of antenna gain, all nodes are initially homogeneous. In M-LEACH, the base station is treated as fixed, and all nodes have GPS to identify their locations. To select the proper cluster head, M-LEACH modifies LEACH's distributed setup process. In M-LEACH, cluster heads are selected using an attenuation model [7]. The best cluster heads are selected to lessen the strength of attenuation. Other selection factors for cluster heads include mobility and speed. M-LEACH is chosen as the cluster head because it has the lowest mobility and attenuation power. The chosen cluster heads then sent out a broadcast to all nodes within transmission range with their status. Non-cluster-head nodes compute their willingness across many cluster heads in order to select the cluster head with the greatest leftover energy.

Each routing protocol aims to enhance the well-known clustered routing protocol LEACH by concentrating on a specific problem. Each routing protocol has a few characteristics and advantages. These routing protocols struggle with a number of challenges, including the cost of clustering, the selection of cluster-heads and clusters, synchronisation, data aggregation, repair mechanisms, scalability, mobility, and the initial energy level of all nodes[5]. We contrast the aforementioned routing in light of some critical wireless sensor network performance indicators. These requirements are listed below. It might be flat, location-based, or hierarchical, according to routing protocol classifications [6].

Motion: This explains how both fixed and mobile nodes are taken into account while designing the routing protocol. Scalability is the ability of a routing technology to expand while maintaining high performance as network concentrations increase.

Self-organization: The ability of the routing protocol to change as the network does is essential. The routing protocol should automatically carry out node configuration and re-configuration as nodes enter or leave the network [6].

Randomized Cluster-head Rotation: The cluster head must be rotated in order to evenly drain the batteries of all nodes [1]. In the distributed clustering process, cluster heads self-select, and nodes share the choice of their cluster head.

Algorithm for centralised clustering: The cluster leaders are selected by the base station using a central control algorithm [3].

Another essential element of the routing protocol is the choice between single-hop and multi-hop. Single-hop networks use less energy than multi-hop networks if the network is smaller [7].

Energy Efficiency: An energy-efficient routing strategy seeks to maximise network longevity [1], [2], [4], and [8].

Resources awareness: The routing protocol must be mindful of the limited resources, such as batteries, available in sensor networks [8].

Data Aggregation: The cluster head performs data-aggregation [1], [2] to reduce the quantity of data that needs to be broadcast to the base station.

All routing protocols take into account the homogeneity of each node, which means that each one has a similar initial state of energy.

3. Modeling and Simulation Results

Using the simulator NS-3 version 3.21 and the OMNet++ library for WSN framework buildings, the analysis of WSNs using various existing routing protocols against proposed protocols and models with various performance parameters in terms of end-to-end delay, packet overhead, packet delivery ratio or throughput, energy consumption and lifetime of network have been carried out.

3.1 E2E Latency

The suggested protocol's average E2E latency is lower than that of the i-Leach, M-Leach, M-Gear, and Leach protocols.

“Fig 1. : Average E2E” Latency 30 nodes (Sec)

having the option of alternate paths. Nevertheless, the selection procedure must start again from scratch if the network needs to choose a new cluster head, adding extra latency. The proposed protocol's latency is also found to decrease as the network's nodes increase in size in such a case, but the M-Gear protocol's performance also increases and its latency decreases as a result of fewer alternative paths and decreased cluster head selectivity, as shown in the figures 1, 2, and 3 below.

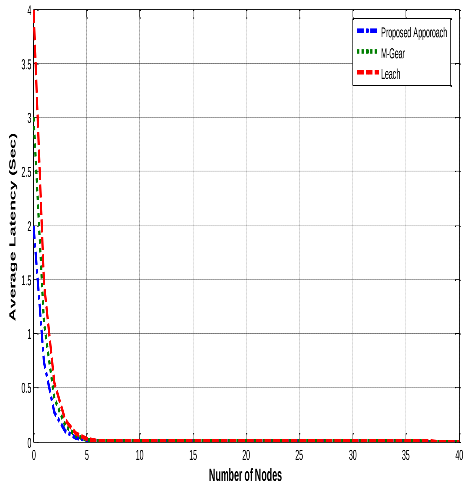
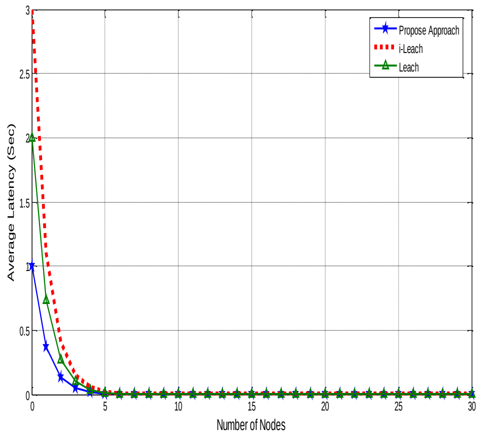
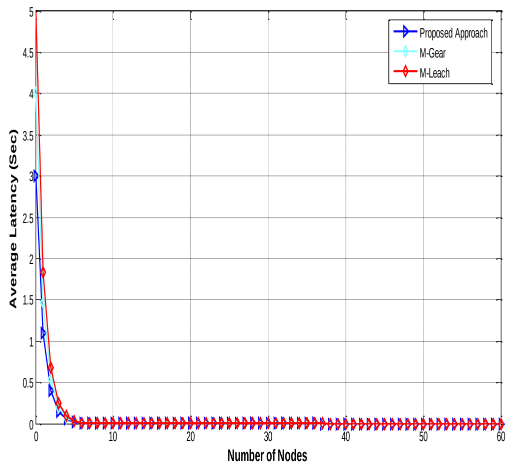


Fig 2. : Average E2E Latency 40 nodes (Sec)





"Fig 3. : Average E2E" Latency 60 nodes (Sec)

This study concludes that the recommended procedure is successful in maintaining

3.2 Ratio of Delivered Packets

According to Fig.. below, LEACH protocol allocates the available track's importance among the various data rates. If a connection fails, traffic is rerouted around the downed one and over the remaining ones. This ensures that the network's throughput remains unchanged. Additionally, M-Leach only uses one route at a time to transmit data packets. If one route is blocked, it will try another.

One main path and many other paths are included in the proposed......protocol. A single path is taken at a time, while the remaining node energy is monitored. If the leftover energy at any node along the active path fell below a certain level, the path would switch to a different one. As a result, the possibility of a data packet being lost is very low.

However, as the number of nodes grows, the suggested method's improvement in results will begin to deteriorate. Also, the proposed method when compared with M-Gear protocol and i-Leach protocol the packet delivery ratio is also efficient and increases up to 99% with different simulation time and by varying number of nodes in a network.

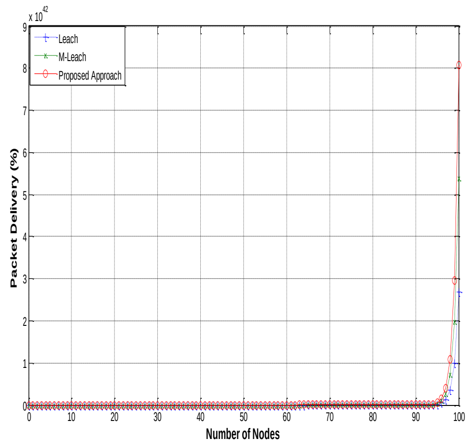


Fig 4. Ratio of Delivered Packets (Against Leach & M-Leach)

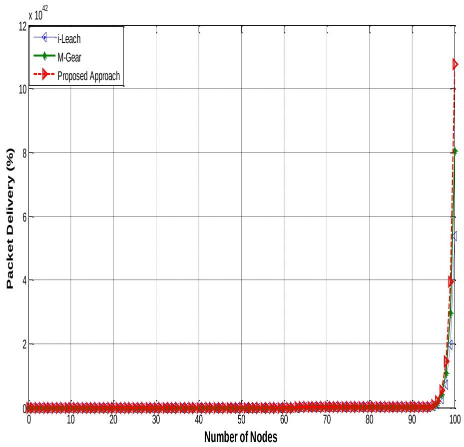


Fig 5. Ratio of Delivered Packets (Against I-Leach & M-Gear)

The simulation outcomes demonstrates that the suggested protocol is able for keeping the efficient packet delivery ratio stable.

4. Conclusion

Data packet loss recovery in WSNs is addressed by the method described above. With a dynamic buffer at the router, the packet loss ratio reduced. Additionally, the packet delivery ratio has improved, and this feat was made while using the same amount of energy to extend system life. Since the data loss ratio is reduced by increasing all QoS parameters, the network'soverall reliability is enhanced, which is especially useful in highly sensitive WSN where the density of events is high as well as burst data produced by the event raises the risk of data loss because of buffer overflow and thus significant data loss. In the future, the emphasis will be placed on high priority packets, and efforts will be made to increase the selective dependability of WSN.

References

[1] S. Suryawanshi and S.R. Hiray, “Congestion Control Protocol for Traffic Control in Multimedia Applications Using WSN,” Trends inNetwork and Communications, Springer Berlin Heidelberg, pp. 242-251, 2011.

[2] C. Sergiou, P. Antoniou, and V. Vassiliou, Congestion Control Protocols in Wireless SensorNetworks: A Survey,” IEEE Communications Surveys & Tutorials, Vol. 16, No. 3, pp. 1369-1390, 2014.

[3] S. Nosheen, S. A. Malik, Y. Bin Zikria and M. K. Afzal, “Performance Evaluation of DCCP and SCTP for MPEG4 Video over Wireless Networks,” in IEEE International Multitopic Conference, INMIC 2007, pp. 1-6, 2007.

[4] C. M. Huang, Y.T. Yu, Y. J. Huang, “A Cross-Layer Loss Discrimination Scheme for DCCP over The Wireless Network,” in 5th International Conference on Ambient Systems, Networks and Technologies, Procedia Computer Science, pp. 77-84, 2014.

[5] B. Görkemli, M.O. Sunay and A.M. Tekalp , "Video streaming over wireless DCCP," in 15th IEEE International Conference on ImageProcessing, ICIP 2008, pp.2028-2031, 2008.

[6] S. A. Nor, S. Hassan, O. Ghazali, M. M. Kadhum, and M. H. Omar,“Performance Enhancement of DCCP TCP-like over Long Delay LinkNetworks,” International Journal of Modeling and Optimization, Vol. 2,No. 3, June 2012.

[7]. ShilpaKatikar, Vivek Deshpande. "Reliability enhancement in WSN using loss recoverymodel", 2015 International Conference on Information Processing (ICIP), 2015.

[8]. S. V. Todkari, Vivek S. Deshpande, A. B.Bagwan. "Loss recovery scheme using adaptivedata collector node (ADCN) in wireless sensor network", 2016Thirteenth International Conference on Wireless and OpticalCommunications Networks (WOCN), 2016.