ELIMINATION OF DUPLICATE PACKETS FROM THE NETWORK USING REDUNDANCY AWARE HIERARCHICAL TREE ALTERNATIVE PATH ALGORITHM

Chinnu.J.Thayyil[1] , P.J.Gladys Glory[2]
M.Phil Scholar Department of CS, SNMV CAS[1], HOD Department of IT, SNMV CAS[2]
chinnuelsa308@gmail.com[1], gladsjacob@yahoo.com[2]

ABSTRACT:

The wireless sensor network (WSN) is a grouping of sensing, computation, and communication into a particular tiny device. A sensor network consists of an array of many sensor networks of various types unified by a wireless communication network. This paper has largely described the feature and the substance of congestion control in WSN and survey the study related to the Congestion Control Protocols and Algorithms for WSNs. In this paper we applied Redundancy Aware Hierarchical Tree Alternative Path (RAHTAP) algorithm, this algorithm eliminates the duplicate packets from the network and attain reduction in network load as per packets basis which generate lively substitute path from source to sink.

Keywords: *WSN, RAHTAP, Eliminating duplicate packet in WSN.*

1. INTRODUCTION:

A Wireless Sensor Network (WSN) for a times called a wireless sensor and actor network (WSAN) are spatially scattered independent sensors to *monitor* objective or environmental conditions, such as temperature, sound, pressure, etc. and to politely pass their data throughout the network to a main location. The present networks are bi-directional, also enable the *control* of sensor activity.

A sensor node might vary in size and the cost of sensor nodes is equally variable, ranging from a few to hundreds of dollars, depending on the difficulty of the entity sensor nodes. The cost and size constraints on sensor nodes outcomes in equivalent constraints on property such as energy, memory, computational speed and infrastructure bandwidth. The topology of the WSNs can differ from a plain star network to an advanced multi-hop wireless mesh network.

2. RELIABLE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS DURING OVERLOAD SITUATION

2.1 Alternative Path Creation (APC)

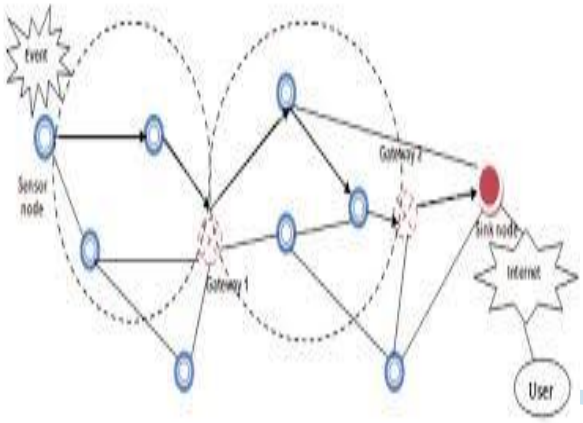

Fig. 1: Alternative Path Creation (APC)

The early design for the formation of this algorithm derived from a exacting concept of the theory of Dynamic Alternative Routing (DAR) which is widely used in public telephony. In this idea it is stated that if you have a high-quality route without troubles, stick to it, until incredible goes wrong. With some main changes in the execution, this concept is adopted by us in the crate of congestion control in WSNs. The main target of the APC algorithm is to take benefit of the nodes and use them for the formation of substitute paths from the source to the destination. The formation of these paths will unpack the highly opaque parts of the network and will lead the data packets securely to a sink though other routes. The main theory of this algorithm is a source node keeps transmitting data packets to a specific node in a level elevated than itself, upon it receives a control message starting this node that is not able to handle any more packets.

3. IMPLEMENTATION:

A. APC implementation

The APC execution philosophy of the algorithm follows the steps below:

• A very simple hierarchical flooding protocol is used for the pattern of the network's topology. During this process, every node discovers its neighbor nodes and updates its neighbor table. In accumulation during this protocol, sensor nodes are notionally located in levels from the source to the destination.

• At every packet transmission each node piggybacks its blocking state (buffer occupancy). The neighbor nodes listen in the packet transmission and inform their neighbor tables with this information.

• During the trigger of an event, the source node starts transmitting data packets by creating flows to the destination. If the sending data time is higher than the sending time that the getting node can transmit, the receiving nodes will quickly face a barrier congestion condition and the outcome would

perhaps be the arbitrary drop of data packets. To avoid this circumstance each candidate crammed receiver is sending a packet to the sender to inform it, and again if it continues to transmit packets with the same rate it will soon be congested.

• The node begins transmitting the data to the alter node. The same phenomenon can happen in each level (between the neighbor nodes). The wavering of receiver can leads to the creation of alternative paths.

B. Hierarchical Tree Creation (HTC)

The Hierarchical Tree Creation algorithm consists of two main steps:

• **Route Creation:**

In this step each node is assigned a level according to the hierarchical tree. Each source node is assigned a level 0 to a node and broadcasts a *level_discovery* packet in the network. The sensors which receive the packet are handed as offspring to the transmitter and are set to level 1. All these nodes broadcast a *level_discovery* packet, and the patterns continue with the level 2 nodes in the network. The source node when it receives the *level_discovery* packet updates its neighbor table.

• **Flow Creation:**

In Flow Creation the connection is established between each transmitter and receiver using a 2-way handshake. Packets are exchanged between every transmitter and receiver in the network. During this packet swap, the congestion position of each receiver is communicated to the transmitter. The association is performed using a 2-way handshake. In a source node A and a receiver B, node A sends a first packet to B. When node B receives this packet, it sends an acknowledgment packet back to A. In this acknowledgement packet the node B piggybacks the congestion state at the moment.

C. RAHTAP Algorithm for Congestion Control in Wireless Sensor Network

There are two technology by which congestion can be condensed which are: either by dropping the data sending rate of source or by given that extra resources.

Congestion in WSNs is elevated if load in the system is very high. So network load is concentrated upon exclusion of redundant number of packets in WSNs. In this paper we executed an algorithm called Redundancy Aware Hierarchical Tree Alternative Path (RAHTAP), which destroy the duplicate packets from the network and attain reduction in network load as per packets base which create dynamic substitute path from source to destination when congestion on a particular node in the network. The RAHTAP algorithm works

above the thought of existing congestion control algorithm HTAP.

In wireless sensor network, there are so many challenges. The main challenge is to provide greatest lifetime to network and how to present a network totally rely on battery power. The main goal for enlarging lifetime energy efficient, load balancing packet relocate from source to destination to network as a sensor of network is to protect battery power or force with the help of falling of the reproduction data packets in to the networks.

Flow Establishment

An association is created between every transmitter and recipient pair utilizing a two-way handshake. Through this parcel trade, the clogging state of every collector is conveyed to the transmitter. In the event that we think about, where hub 1 is the source and hubs 2, 3, and 4 are collectors. Firstly, hub 1 sends a parcel to hub 2.When hub 2 accepts this bundle, it sends an ack bundle once again to 1.In this ack bundle hub 2 piggybacks its current blockage state. This trade makes the source hub mindful of the blockage state of all its next jump neighbors that can catch. When the clogging state of a kid (downstream neighbor) achieves a prespecified farthest point, the hub upgrades its upstream hubs of the blockage state utilizing a devoted control bundle.

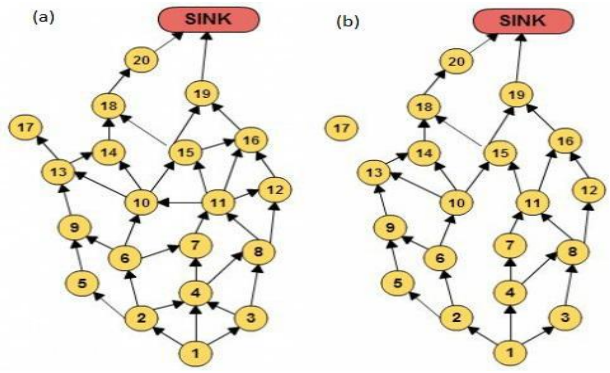

Fig.2: (a) network connectivity after topology control, (b) level placement procedure

4. CONCLUSION:

In recent times there has been a increasing interest in Wireless Sensor Networks (WSN). Sensor Networks hold a lot of guarantee in applications where assembly sensing information in remote locations is needed. It is an evolving field, which offers scope for a lot of study. Their power-constrained nature necessitates us to look at more energy resourceful design and operation.

The impact of wireless sensor networks on our everyday life can be preferably compared to what Internet has done to us. Both the factors of congestion control and reliability helps in reducing packet loss, which results in an energy efficient operation of the network, which is a key

factor in increasing the lifetime of the sensor in the network. While these congestion manage techniques are promising there are still there are many challenges to solve in wireless sensor network to hold congestion organize efficiently. And more research efforts are needed to continue to improve congestion control in WSNs.

RAHTAP algorithm manages to control congestion in WSNs using Redundancy Detection and elimination when congestion appears in the network. The main advantage of RAHTAP is redundancy detection and elimination process it uses on sensor node to eliminate the copy of packets in each sensor nodes, as a result of which network throughput and efficiency increases. It also reduces the overhead to already heavy loaded networks. Further this algorithm is an algorithm for energy constraints in WSNs. RAHTAP has been assessed and its execution was contrasted with an alternate existing asset control calculation HTAP.

5. REFERENCES:

1. A. Perrig, L. van Doorn, and P. Khosla, "SWATT: Software-Based Attestation for Embedded Devices," Proc. 2004 IEEE Symp. Security and Privacy, 2004.
2. A. Woo and D. E. Culler, "A Transmission Control Scheme Sensor Networks", *Seventh Annual International Conference on Mobile Computing and Networking, pp 221-235,* July 2001
3. B. Hull, K. Jamieson, H. Balakrishnan, "Mitigating Congestion in Wireless Sensor Networks", *Proceedings of the 2nd international conference on Embedded networked sensor systems,* November 03-05, 2004, Baltimore, MD, USA
4. Chris Wright and Crispin Cowan, James Morris, Stephen Smalley and Greg Kroah-Hartman "Linux Security Modules: General Security Support for the Linux Kernel" August 17, 2002
5. C.E. Perkins and E.M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proc. Second IEEE Workshop, Mobile Computing Systems and Applications, 1999.
6. C. Lu, B. M. Blum, and T. He, "RAP: A Real-Time Communication Architecture for Large- Scale Wireless Sensor Networks", *Proceedings of the Eighth IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'02), p.55,* September 25-27, 2002.
7. C. Tien Ee,, "Congestion Control and Fairness for many-to-one Routing in Sensor Networks", *Proceedings of the 2nd international conference on*

Embedded systems, November 03-05, 2004, Baltimore, MD, USA

8. C. Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion Detection and Avoidance in Sensor Networks". In *Proc. ACM SenSys*, 2003
9. E. Shi, A. Perrig, and L. van Doorn, "Bind: A Time-of-Use Attestation for Secure System," Proc. IEEE Symp. Security and Privacy, pp. 154-168, 2005.
10. F. Ye, G. Zhong, S. Lu, and L. Zhang. PEAS: A Robust Energy Conserving Protocol for Long-lived Sensor Networks. *In Proceedings of the 23rd International Conference on Distributed Computing Systems*, May 2003.
11. Gang Xu, C.Borcea and L.Iftode, " A Policy Enforcing Mechanism for Trusted Ad Hoc Networks", IEEE Transcation on Dependable and Secure Computing, Vol. 8, No.3, May/June 2011.
12. G. Xu, C. Borcea, and L. Iftode, "Satem: A Service-Aware Attestation Method toward Trusted Service Transaction," Proc. IEEE Symp. Reliable Distributed Systems (SRDS), pp. 321-336, Oct. 2006.
13. G. Xu, C. Borcea, and L. Iftode, "Trusted Application-Centric Ad Hoc Networks," Proc. Fourth IEEE Int'l Conf. Mobile Ad-Hoc Networks and Sensor Systems (MASS '07), 2007.
14. G. Karjoth, "The Authorization Service of Tivoli Policy Director," Proc. 17th Computer Security Applications Conf. (ACSAC), p. 319, Dec. 2001.
15. K. Römer and F. Mattern, "The Design Space of Wireless Sensor Networks". *IEEE Wireless Communications* 11 (6): 54-61,December 2004
16. L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Networks, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.
17. T. Woo and S. Lam, "A Framework for Distributed Authorization," Proc. First ACM Conf. Computer and Comm. Security, pp. 112- 118, Nov. 1993.
18. T. Phan, Z. He, and T.D. Nguyen, "Using Firewalls to Enforce Enterprise-Wide Policies over Standard Client-Server Interactions," J. Computers, vol. 1, no. 1, pp. 1-12, Apr. 2006.
19. T. Yan, T. He, and J. A. Stankovic. Differentiated Surveillance Service for Sensor Networks. In *Proceedings of theACM SenSys 2003*, 2003.
20. "The Network Simulator—NS2," http://www.isi.edu/nsnam/ns, 2010.