INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

MANAGING PACKET DROPPING USING REACTIVE TIME BUFFER TECHNIQUE IN WIRELESS SENSOR NETWORK

R.Vijayakumar[#1], M.Boopalan[#2], S.Prabakaran[#3], T.Sathyamoorthi[*4]
[#]PG Student, Department of Computer Science and Engineering, Muthayammal Engineering College, Namakkal
[*]PG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur
[1]r.vijay155@gmail.com
[2]wakeupboopalan@gmail.com
[3]sprabu38@gmail.com
[4]sathyame11@gmail.com

Abstract- In wireless sensor network, the important one is to manage the collection of mobile nodes to improve the performances of the network. The main issue is packet dropping that occurs due to malicious attackers, CPU overload, Software fault, network error, low bandwidth, etc., so it interrupts the communication. In order to manage this problem, we propose an efficient technique, called Reactive Time Buffer (RTB), which can identify which node is drop the packets, by getting acknowledgment from nodes.

Keywords- Wireless Sensor Networks (WNS), Reactive Time Buffer (RTB), Packet Dropping.

I. INTRODUCTION

Wireless Sensor Networks (WSN) is unruffled of a large number of small nodes among computation, sensing, and wireless communication capabilities. In wireless sensor networks, sensor nodes are typically placed and scattered of sensor nodes needs not be prearranged. It means that sensor network algorithms and protocols are being required to gives self-configuring ability and self-organizing capabilities [1].

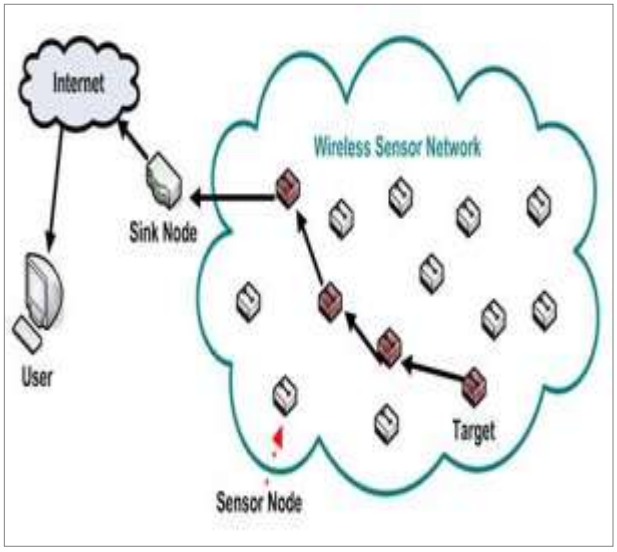

Fig 1.1 Wireless Sensor Networks (WNS)

One more feature of sensor networks is the synchronization of sensor nodes to generate high-quality information about the sensing environment. That is WSN is used to collect and utilize the information from physical environments.

Although many protocols and algorithms have been proposed for traditional wireless ad-hoc networks, they are not well suited to the unique features and application requirements of sensor networks. Therefore, many routing and data dissemination protocols should be designed for sensor networks where the following issues should be considered [2]:

A. Energy Awareness
B. MAC for Wireless Sensor Networks
C. Time Synchronization
D. Power-saving Mode of Operation
E. Routing

The wireless sensor networks provide a wide range of applications such as health, military, and home. The realization of these and other sensor network applications require wireless ad-hoc networking techniques. This contains two network methods called single-hop and multi-hop [3]. In single-hop network within communication range the sender and receiver can directly communicate through message passing.

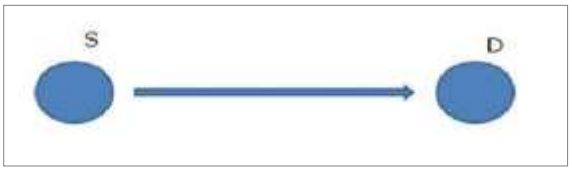

Fig 1.2 Single-hop Network

Otherwise its communicate using forward packets through intermediate nodes. This is called multi-hop network. MULTIHOP data routing over wireless sensor networks (WSNs) has attracted extensive attention in the recent years.

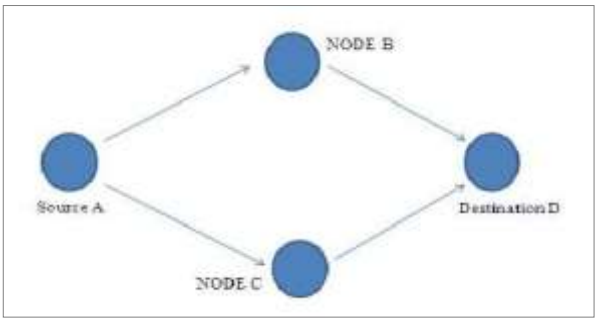

Fig 1.3 Multi-hop Network

Advantages of Sensor Networks

Wireless sensor network provides lot of unique advantages over traditional centralized approaches. There are given below:

- *Flexibility*- Able to adapt dynamically to changes in node density and topology
- *Self healing minefields*- Able to self-heal to control the process of the nodes
- *Data Collection*- Data is collected based on the network coverage
- *Time synchronization [4]*- It is used for security-related interaction
- *Maintenance*- Based on entire or partial update of the program

The rest of the paper is organized as follows. Problem statement is given in Section II. In Section III describe overview of proposed system with two different schemes in detail. Finally, the conclusion and future works of the proposed system is presented in Section IV.

II. PROBLEM STATEMENT

Packet Dropping Problem

The data transmission takes place using special hardware for router. This hardware normally works with not introducing transmission errors. In software side, it is established enough means, it will not drop packets, so if a packet on its way from a sender to a receiver is lost in a fixed network, it is not because of hardware or software errors. The probable reason for a packet loss in a fixed network is a temporary overload some point in the transmission path, i.e., a state of congestion at a node. Congestion may appear from time to time even in carefully designed networks.

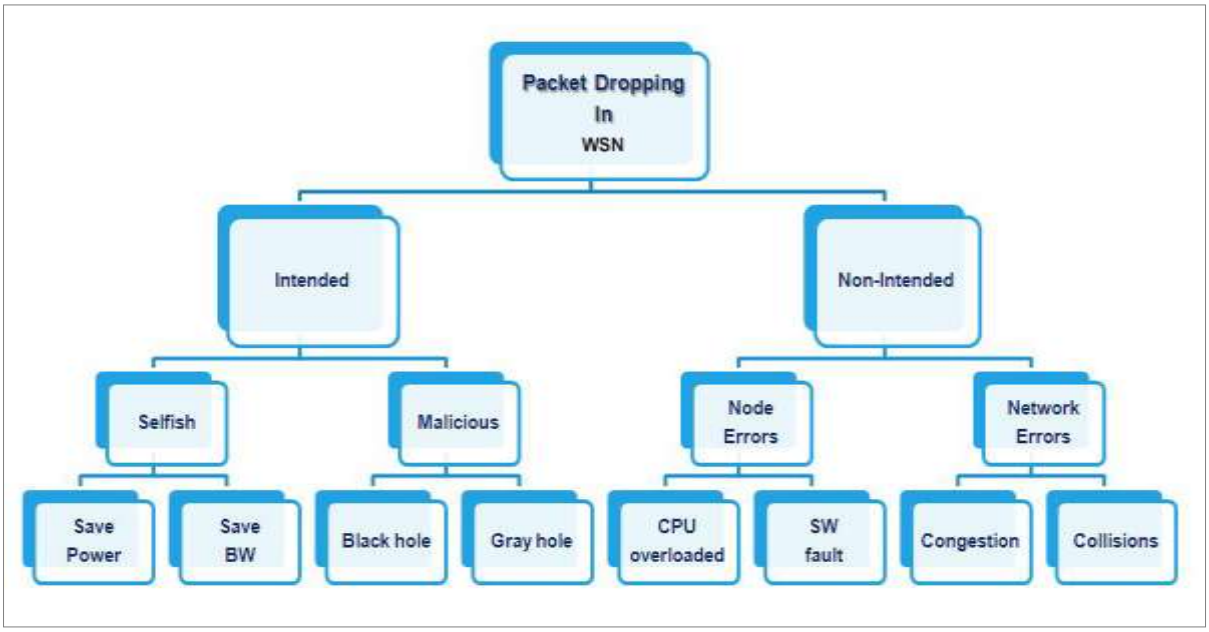

Fig 2.1 Partial Dropping: Occurs due to malicious node, CPU overloaded, Software fault, network error, low bandwidth, etc.

The packet buffers of a router are filled and the router cannot forward the packets fast enough because the sum of the input rates of packets destined for one output link is higher than the capacity of the output link. The only thing a router can do in this situation is to drop packets.

Since there is no infrastructure in mobile ad hoc networks, each node must rely on other nodes for cooperation in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. The packet dropping is occurs due to lot of reasons. These are shows in above figure 2.1.

III. PROPOSED SYSTEM

The absence of a physical link among nodes makes the wireless links vulnerable to eavesdropping and information theft [5]. To provide a certain level of security, we defined a new technique called, Reactive Time Buffer (RTB). This technique contains two types of solution scheme namely, Buffering & ACK scheme and Routing scheme.

Buffering & ACK scheme

The first solution is Buffering and ACK scheme shows in figure 3.1. It contains six nodes, the nodes S and D are source and destination nodes. And m, n, o and p are the intermediate nodes. These intermediate nodes having individual buffers that contain source and destination address with details and also having transmission packet. The source node S sends the packets to destination node D through intermediate nodes m, n, o and p. If any one of intermediate nodes drop the packet due to network errors or low bandwidth.

The Buffering and ACK scheme can solves this type of dropping. In below figure 3.1, the node S forward the packet to intermediate node m means, that node m stores that packet to the own buffer B1 and forward the packet to next node n and so on. The node n receive the packet successfully means its send back the ACK acknowledgement to node m. If node m receives ACK means that delete the packet from the buffer B1. If any one of the node cannot receive ACK due to network error means it cannot delete the packet in the buffer and it can send the dummy packet. This time it gets the ACK acknowledgement means, now it takes the original packet from the buffer and forward to that node. The node cannot receive the ACK

acknowledgement for that dummy packet means that node is reported as malicious node and this is switched to Routing scheme. In following figure, the node p cannot send the ACK acknowledgement signal to node 'o'. So the node o takes the stored packet from buffer B3 and forward (ie., resend) to node p.

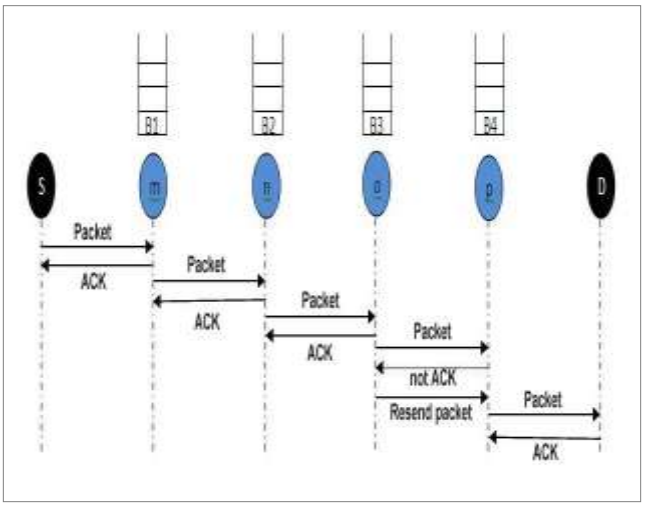

Fig 3.1 Buffering and ACK scheme

Routing scheme

The second solution is Routing scheme that shows in figure 3.2. In this figure S and D are source and destination nodes. The source node S finds the route to destination node D using any one of the routing algorithm. Here n1, n2, n3 and n4 are the intermediate nodes that are selected for the routing path.

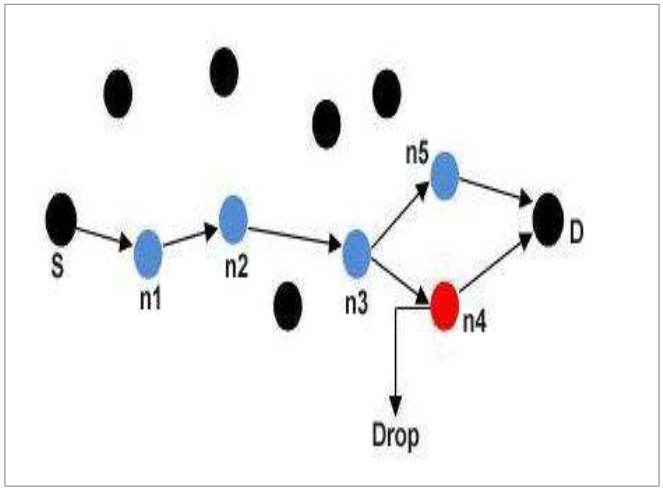

Fig 3.2 Routing scheme

Any one of the intermediate node will drop the packet due to occurrences of the different types of misbehaviors or attacks. In this case the router is activated and router is check another nearest route to destination then forward the packet to that selected route and finally the original packet reached to the destination.

In the figure 3.2, the node n4 is cannot send back the ACK to node n3 for long time so it is reported as malicious. The Malicious nodes simply drop all the packets that they receive. This situation the router can find another route n1, n2, n3 and n5 then forward the packet to this path. Finally the packet is received successfully by destination node D.

IV. CONCLUSION AND FUTURE WORK

Wireless Sensor Networks are one of the largest important parts in wireless technologies [6]. It contains lot of security issues like power consumption, packet dropping, collision, congestion, etc., The technique proposed in this paper aims to improve and manage the packet dropping in wireless sensor networks. The main effort of this proposal has been to improve the performance of the data transmission in terms of data rate.

To enhance the qualities of our research work, we plan to examine the following issues in our future research:

1. In this technique we continuously use the buffers, so the time will be increased. So we research new technique for time management for handling packet dropping.

2. To analysis the new mechanism to control the power consumption.

REFERENCES

[1] M. Vieira, D. da Silva Jr., C.C. Jr., and J. da Mata, "Survey on wireless sensor network devices," in Proceedings of the 9th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'03), Lisbon, Portugal, Sept. 2003.

[2] Mokhtar Beldjehem, "Toward a Multi-Hop, Multi-Path Fault-Tolerant and Load Balancing Hierarchical Routing Protocol for Wireless Sensor Network," in scientific research journal, pp. 215-222, March 2003.

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs," Transactions on Industrial Electronics, vol.60, no.3 pp. 1089– 1098, 2013.

[4] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: A survey," IEEE Network, vol. 18, pp. 45–50, July–Aug. 2004.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad hoc Networks, Proc. 6th Annual Intl. Conf. on Mobile Computing and networking(MobiCom00), Boston, Massachusetts, pp. 255-265, August 2000.

[6] A.S.K. Pathan, L. Hyunh-Woo and H. Choong-Seon, Security in wireless sensor networks: issues and challenges, Advanced Communication Technology, 2006. The 8th International Conference, Vol. 2, p. 6, February, 2006.