Collision Avoidance Using WTRP-MAC Protocol for Clustered Wireless Sensor Network

S.Sathishkumar,
Research Scholar,
School Of Computer Science, Engineering and Applications,
Bharathidasan University, Trichy.
Sathish.galaxyboy@gmail.com.

Abstract-In a clustered wireless sensor network, multiple accesses at a time lead to collision. This could cause retransmit of lost packets. It increases power consumption, decreases sensor lifetime and delay in packet transmission. Basically sensors are not always need to send data. Suppose if an event occurs, then every sensor automatically accesses their base station simultaneously. It causes multiple communications at a single time and leads to collision. To overcome this problem in a wireless sensor network our proposed Collision Free MAC protocol is used. Passing token to the cluster head makes a single data transmission at the time. All the cluster heads in the Wireless Sensor Network starts transmitting data only when it receives token from the Base Station. After completion of transmitting the packets, the token will be passed to its successor cluster head. The Token passing depends on two states (i) THT, (ii) TRT. In every cluster head the desired 'Token Holding Time' gives stipulative time to sending data. Single 'Token Rotation Time' must provide token to all cluster head in the Sensor Network at a point of time. This process reduces collision during data transmission. The simulation result gives our Collision Free MAC protocol reduces collision at multiple accesses through given time of data transmission.

Keywords: Collision, Token, Collision free MAC, THT, and TRT

I. INTRODUCTION

Wireless sensor networks (WSNs) are battery driven and hence a major constrain in a WSN is its low energy. One of the factors that reduce the energy efficiency is collision. In WSNs, the density of transmission for packets through the medium is often very high and as a result the traffic flow would be increased These networks also experience a phenomenon which is very common known as congestion[1].Sensors do not regularly have much data to send. However, when an event occurs, every sensor in a given area will send its alert to the access point simultaneously. Hence, this network suffers a huge number of communications at the same time. In fact, at an instant, only one transmission is permitted among interfering nodes. If there are more than two transmissions at the same time, there will be a collision. Therefore, this variant communication of wireless sensor networks leads to an increase in collision and energy consumption [2].Clustering is a method of grouping sensor nodes, can meet the requirements of the TDMA-based MAC protocols and has been the focus of much research on sensor networks. In a clustered sensor network, all the sensor nodes are organized into a hierarchy based on some clustering algorithm. In each cluster, one sensor node is selected to act as the cluster head and perform a majority of functions, e.g., maintaining the collision-free schedule, collecting all the information sensed by the cluster, aggregating data and reporting to a base station, the cluster head role is usually periodically rotated among the nodes to balance the energy consumption. All the other sensor nodes only need to contact with their cluster head. Most of the cluster-based MAC protocols apply TDMA within a cluster. However, the existing cluster-based schemes do not dynamically change the frame size and slot assignment due to nodes failures or change of traffic load[3].CSMA/CA Carrier sensing prior to transmission is an effective approach to increase the throughput efficiency in shared-medium access environments. Although applicable in wireless environments, the scheme is susceptible to two problems, commonly referred to as the hidden- and exposed-node problems. CSMA is designed to avoid collision by sensing the signal in the vicinity of the transmitter give rise to the hidden- and exposed-node problems [4]. For a wireless sensor network, the WTRP protocol give nodes take turn for transmission, thus get fair share of the channel. It has been shown that WTRP provides guaranteed QoS in terms of high throughput and bounded transmission delay [5].

II. MOTIVATION OF TOKEN PASSING

The motivation of using token approach reduces the collision at multiple accesses also to provide reliable data transmission. This is because every sensor node that intends to transmit the data should have the token first before it senses the medium. This will reduce the probability of collision in a wireless sensor network.

Using of CSMA/CA protocol in a sensor network to transmit data packet from cluster head to Base station, there are two problems, commonly referred as hidden-exposed node problem. To avoid this problem using

RTS/CTS handshake. Through this method every cluster head need to send RTS/CTS handshake for data transmitting. This could be made delay in data packet processing. Because every cluster head wait for the acknowledgment for sending and receiving data transmission.

Besides, through the Token approach, no hidden terminal problem will occur. For example, as shown in Fig 1, cluster head c1 and cluster head c2 can hear communication that occurs within Base station B's range, but node c1 and node c2 cannot hear each other's data packet. Without token approach, in CSMA protocol, each sensor node sense the channel and transmit the data, if found that the ratio channel is idle. Hence, sensor node c1 and node c2 might sense and transmit data packet at the same time and cause a collision. However, the token approach, only one cluster head that has the token can transmit the data packet. Node c2 holds the token and can transmit the data without collision because node c1 will wait for the token before it sends the data.

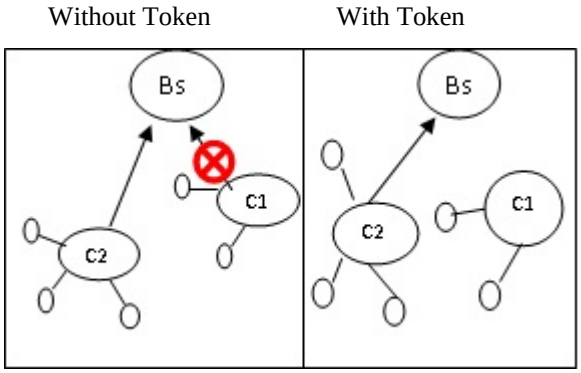


Figure 1: Token work with partial connectivity

In token approach can offer dynamic frame length with time holding token (THT). A cluster head that needs less time than THT will hand over the token when packet transmission is finished. Through this method, packet delivery will be increased and delay can be decreased in the network. The main advantage of using token approach is in terms of synchronization. The wireless network must be synchronized in order to transmit the data packet. In a real implementation of WSN it is difficult to achieve synchronization, since sensor nodes are low power devices. This will lead to high overhead and increase the energy consumption.

III. LITERATURE REVIEW

CSMA/CA Carrier sensing prior to transmission is an effective approach to increase the throughput efficiency in shared-medium access environments. Although applicable in wireless environments, the scheme is susceptible to two problems, commonly referred to as the hidden- and exposed-node problems. CSMA is designed to avoid collision by sensing the signal in the vicinity of the transmitter give rise to the hidden- and exposed-node problems [4].A hidden node is defined as a node that is within the range of the destination node but out of range of the transmitting node. An exposed node is a node that is within the range of the sender but out of the range of the destination. Several approaches have been proposed to eliminate, or at least reduce, the impact of the hidden- and exposed-node problems on the network throughput. The first approach is based on the use of a busy tone. The basic idea of the busy-tone approach stems from the observation that collisions occur at the receiving node whereas CSMA is performed at the transmission node.

The major drawback of the approach, however, is a node's need to operate in duplex mode, to be able to transmit and receive simultaneously. This requirement increases the design complexity of a node significantly, thereby increasing its cost and power consumption.

The second approach to deal with the hidden-node problem is based on collision avoidance. This is achieved using a procedure referred to as the ready-to- send (RTS), clear-to-send (CTS) handshake. Using this handshake procedure, the CSMA/CA scheme requires that nodes apply a standard mechanism to avoid collision of wireless packet transmission. Since a node cannot detect if a collision has occurred, it attempts to avoid collisions by waiting for the wireless medium to be clear for the amount of time it takes for a packet to propagate through the entire medium: the time required to send a packet between the most distant nodes in the network. When a node intends to transmit a data packet, it first senses the carrier to determine if another node is already transmitting. If no other transmissions are sensed, the node sends a short RTS packet to the intended recipient of the data packet. If the recipient is, in fact, idle and senses that the medium is clear, it sends a short CTS packet in reply. Upon receiving the CTS packet, the transmitting node sends the actual data packet to its intended recipient. If after a predetermined period of time, the transmitting node does not receive a CTS packet in reply to its RTS packet, it waits a random period of time before repeating the RTS/CTS handshake procedure [4].Collision avoidance multiple access plays an important role in wireless sensor networks, especially for those composed of nodes having simple access protocol functionality. Numerous protocols have been proposed for wireless sensor networks during the past decades. However, the majority of these proposals require too many

actions to be taken by sensor nodes, which makes the sensor nodes too complex. Here novel collision avoidance multiple access algorithms are used to reduce collision in sensor network. [6].

TABLE 1: SUMMARY OF TOKEN APPROACH PROTOCOL

Ref	Advantage	Disadvantage
7	• Better coverage, • Sleeping improved power efficiency, • Dynamic token holding time	not suitable for scenarios with rapid topology
8	bounded latency and robustness against multiple node failures	Token lost
9	It's a centralized approach, and its robust against single node failure	In the centralized approach, the network is managed centrally from a central station

IV. METHODOLOGY

A. Problem & Definition

In a wireless sensor network, multiple accesses to the base station at same time increase the occurrence of collision. This could cause retransmit of lost packets. It decreases sensor lifetime and increase delay in packet transmission. Basically sensors are not always need to send data. Suppose if an event occurs, then every sensor automatically accesses their base station simultaneously. It causes multiple communications at a single time and leads to collision.

B. The Proposed Technique

In this proposed system, avoiding collision at data transmission is mandatory and is demanded in many such practical WSN. So I propose Collision Free MAC protocol called WTRP (Wireless Token Ring Protocol). In a clustered wireless sensor network, every cluster head should defer its transmission until they get the token. At a point of time only one cluster head holds the token and it can transmit for a period of time that cluster head has the token. After that the head sends the token to its successor in the ring. In this way the transmissions in the network is collision-free.

C. Proposed Protocol

WTRP is efficient in the sense that it reduces the number of retransmissions due to collisions. It is fair in the sense that each cluster head takes a turn to transmit and is forced to give up the right to transmit after transmitting for a specified amount of time. It can be used with an admission control agent for bandwidth or latency reservations. WTRP is robust against single node failure. WTRP is designed to recover gracefully from multiple simultaneous faults. The Wireless Token Ring Protocol discussed in this research is a distributed medium access control protocol for clustered wireless sensor network. The advantages of a distributed medium access control protocol are its robustness against single node failure, and its support for flexible topologies, in which sensor nodes can be partially connected and not all nodes need to have a connection with a Base station.

WTRP is to be deployed initially in the University of California at Berkeley PATH Advanced Vehicle Safety Systems Program, the CALTRANSPATH Demonstration 2002, and the Berkeley Aerobat project. These projects impose stringent bandwidth, latency, and speed of failure recovery requirements on the medium access protocol. As in the IEEE 802.4 standards, WTRP is designed to recover from multiple simultaneous failures. One of the biggest challenges that the WTRP overcomes is partial connectivity. To overcome the problem of partial connectivity, special tokens, additional fields in the tokens are added to the protocol.

When a sensor node joins a ring, it is required that the joining node be connected to the prospective predecessor and the successor. When a sensor node leaves a ring, the predecessor of the leaving sensor node finds the next available node to close the ring. Partial connectivity also affects the multiple token resolution protocol (deleting all multiple tokens but one)

In a partially connected sensor network, simply dropping the token whenever a sensor node hears another transmission is not sufficient. To delete tokens that a sensor node is unable to hear, we have designed a unique priority assignment scheme for tokens. Sensor node only accepts a token that has greater priority than the token the sensor node last accepted. The WTRP also has algorithms for keeping each ring address unique, to enable the operation of multiple rings in proximity.

The WTRP protocol avoids collision in clustered wireless sensor network in the following phase.

1. Basic Process
2. Maintaining Token
3. New node join and relieve from ring

1) Basic Process:

Operations in a token ring network rely on a special packet called token. Fig.4 illustrates the token frame format. The token has a length of 29 bytes.

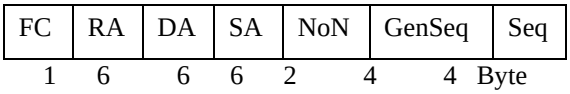


Figure 2: Token Frame Format

Table 2 demonstrates the usage of every field in the token. Seq is reset to zero by the ring in clustered wireless sensor network. The ring is incremented by every sensor node when forwarding the token. GenSeq is initialized to zero when the token ring is first created and incremented by the ring at every rotation of the token. Sensor Nodes in the token ring take turn to transmit.

TABLE 2: FIELDS IN THE TOKEN FRAME

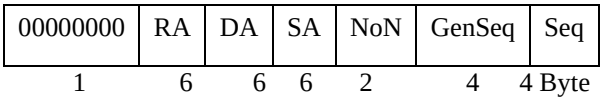
Abbreviation	Name of the field	Usage
FC	Frame Control	Packet Type
RA	Ring Address	Ring owner Address
DA	Destination Address	Receiver of the token
SA	Source Address	Sender of the token
NoN	Number of Nodes	Number of nodes
Gen Seq	Generation Seq	Token rotation sequence
Seq	Sequence	Transmission order

FC referred as Frame Control and it identify the type of packet, such as Token, Solicit Successor, Set Predecessor. Additionally, the source address (SA), destination addresses (DA), ring address (RA), sequence number (Seq) and generation sequence (GenSeq) number are added in the token frame. The ring address belongs to the ring to which the token belongs.

Every sensor node knows its predecessor and successor in the ring. On grasp of the token cluster head starts its transmission for a specified amount of time called token holding time (THT). One or more packets can be sent during a token holding time. After that it must stop to forward the token to its successor. When one cluster head in the ring finish sending a packet, it doesn't need to wait for the ACK from the receiver. Instead of they employ a mechanism called implicit acknowledgement. After transmission, the cluster head listens to the channel to see if any packet with the same ring address exists. The successful reception of the packet acts as implicit acknowledgement to the sender of ACK.

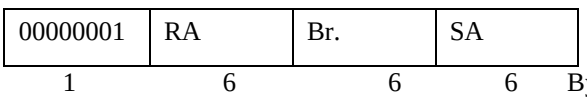
Frame types:

a) Token



The token is used to transfer the right to transmit data packet.

b) Claim Token



The Claim Token is Broadcast (Br).When the Base station generates the token in that case where a cluster head creates the ring. It is also used when a station regains the token in the case of lost token.

c) Solicit Successor Token

00000010	RA	Br	SA	NoN	NS
1	6	6	6	6	6 Byte

The solicit successor token updates the successor field of a Base station. It is broadcast for inviting another node to join the ring. NS field is to inform the joining sensor node about its successor.

d) Solicit Predecessor Token

00000011	RA	DA	SA	NoN	GenSeq	Seq
1	6	6	6	2	4	4 Byte

The set predecessor token updates the predecessor field of a Base station. It is used for both joining and exiting the ring.

2) Maintaining token:

Every token ring network has an owner who is Base station. It is responsible for the generation of the token. The token rotates in the ring, acting as an arbitrator for collision-free transmissions. The token rotation time is bounded by Maximum Token Rotation Time (MTRT). If a cluster head doesn't receive a token within MTRT, it infers that the token has been lost. At that time it send ACK to Base station and it generates a new token, sets its MAC address as the token's RA field.

Duplicate tokens to be eliminated by checking the GenSeq and RA fields. When a cluster head receives a token with the GenSeq field lower than what it has seen before, it discards the token and notifies its predecessor without accepting the token. When the generation sequence numbers of tokens are the same, ring addresses of each token are used to break the tie.

3) New node joins and relieve from ring:

Every time to time, cluster head in the ring broadcasts solicit successor- to invite others to join the ring, provided that the token rotation time does not exceed MTRT. On receipt of the solicitation cluster head outside the ring can join the network through contentions, one at a time. At the time cluster head wants to leave the ring, it waits for the token and then sends set-successor to connect its predecessor with its successor. When the cluster head leaves, its successor becomes the new owner. If the sensor node leaves the ring without notification, other sensor nodes in the ring could still detect this event through implicit acknowledgement or timeout. Corresponding actions will be taken to restore the ring.

V. PERFORMANCE ANALYSIS

Simulation studies of the proposed WTRP-MAC which is carried out using NS-2 simulation tool. The performance of WTRP-MAC is compare with existing Mac protocol CSMA/CA. Implement WTRP protocol for 29 nodes, sending CBR packets with constant interval. First the CBR files and scenario files are generated and to be WTRP protocol. Simulation is done it produces the NAM file and trace file. The following figures are the execution of the NAM files instances created. The network performance is also evaluated by calculating packet delivery ratio, collision ratio and end to end delay and compared the previous result with proposed work done.

A. Simulation Parameters

TABLE 3.A REVIEW OF SIMULATION PARAMETERS IS GIVEN IN TABLE

Channel Type	Channel/Wireless channel
Radio-propagation	Propagation /Two way ground
MAC type	MAC/802_11
Interface Queue	Queue / Drop Tail / Pri Queue
Antenna Model	Antenna/Omni antenna
r-agent	WTRP
Simulation time	30
Traffic type	UDP/CBR
Packet size	512
Number of nodes	29
Total area	500*500

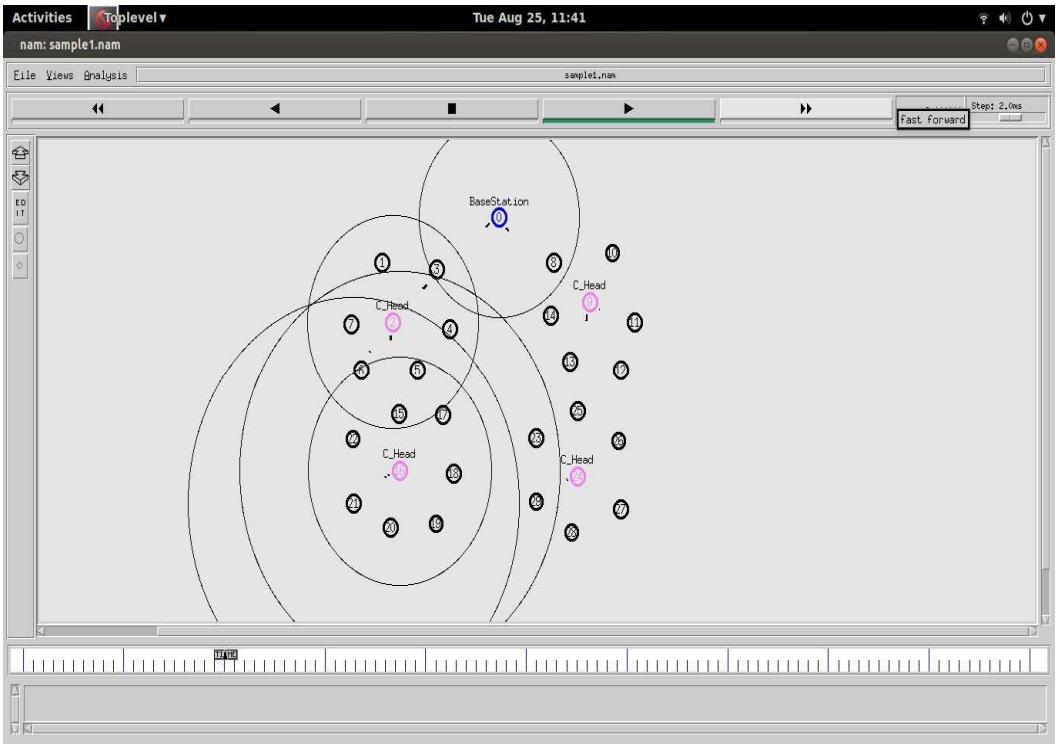


Figure 3: Data Packet Transmission

In this Fig.3, sensor nodes in the every group send the data packet to the cluster head. These cluster head organize and forward those data packet to Base station. The cluster head which are in long distance pass packet to nearest cluster head thereafter it could be reach its Base station.

B. Analysis of Our Approach

In this paper to reduce collision of packet by using WTRP protocol in the clustered wireless sensor network. In this approach we show that passing token to the cluster head which brings one sensor node can pass data at a given timing. The experiment results shows, using the WTRP protocol, reduces collision over the multiple access in the wireless sensor network gives satisfying result.

1) Experimental Results

In this paper, an analysis is done for Packet delivery ratio, collision ratio and end-to-delay. The simulation result shows the effectiveness of the proposed technique. We are viewing results of our proposed system by using some different performance parameters.

For finding the collision ratio in WTRP protocol from the simulation result, it has to compare with existing pre defined protocol CSMA/CA always available on "NS2.35" directory, taking of manual values from the literature papers.

A variety of parameters used for analysis are described below:

Packet Delivery Ratio:

It is also known as packet Delivery ratio of the amount of data packets delivered to the destination and total number of data packets sent by source. Calculated as,

PDR= (Received Packets / Packets Sent)*100

Collision Ratio:

This ratio is used to find collision of packet, the number of packet dropped by destination and total number of data packet generated by source. Calculated as,

Collision ratio = (Dropped packet / Generated packet)*100

End to End Delay Time:

The interval time between sending and receiving sensor node, which includes the processing time and queuing time. Calculated as,

EED = (Time packet received-Time packet sent) / (Total number of packets received)

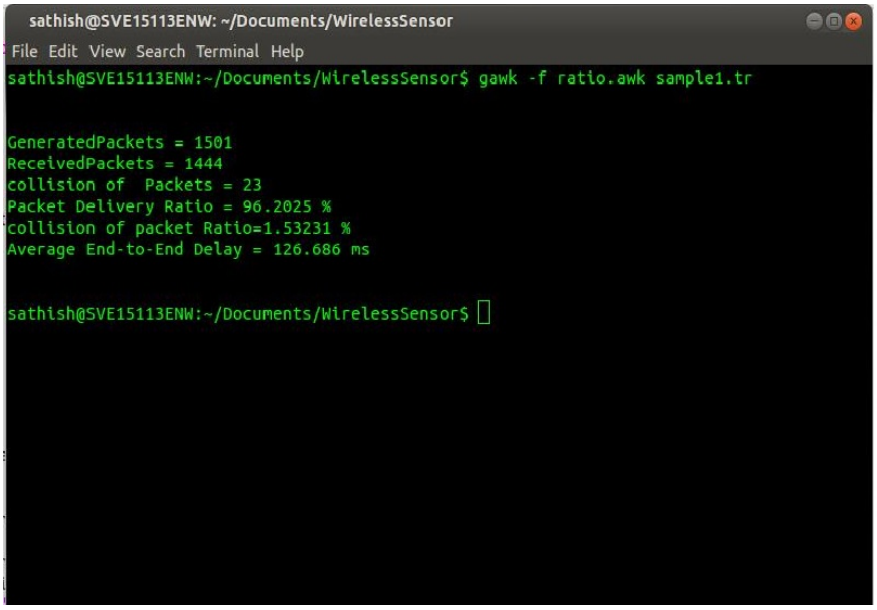


Figure 4: Ratio Calculation

This Fig.4 represents packet delivery ratio, collision ratio, Average end-to-end delay are calculated from the above formula. The values that are taken from "trace file" called sample1.tr. This processed values of the corresponding "NAM file" for the flow of packet from source to destination.

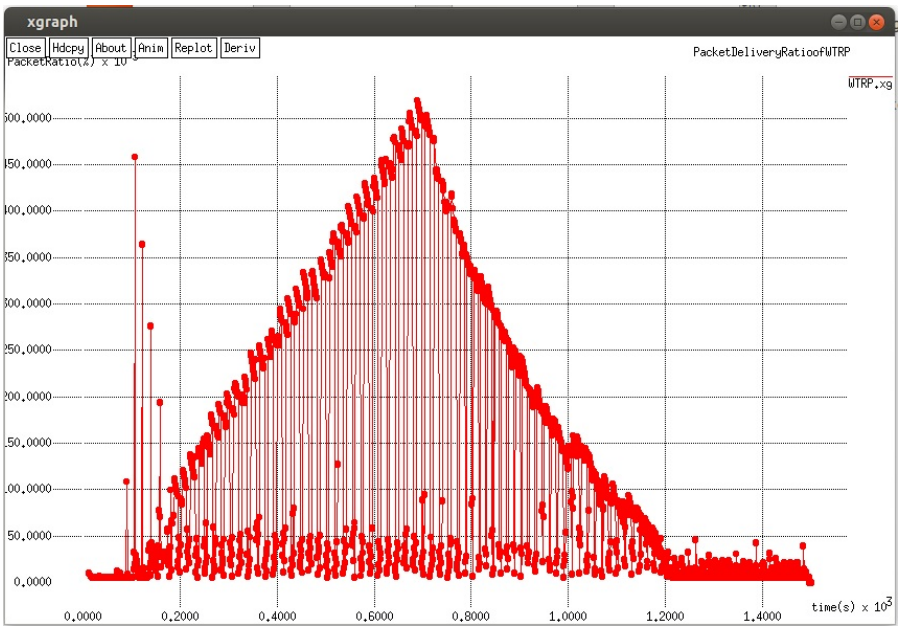


Figure 5: Packets Generation

In this Fig.5 shows the single graph generated automatically, depend on packet generated by source and received by destination which means total packet delivered.

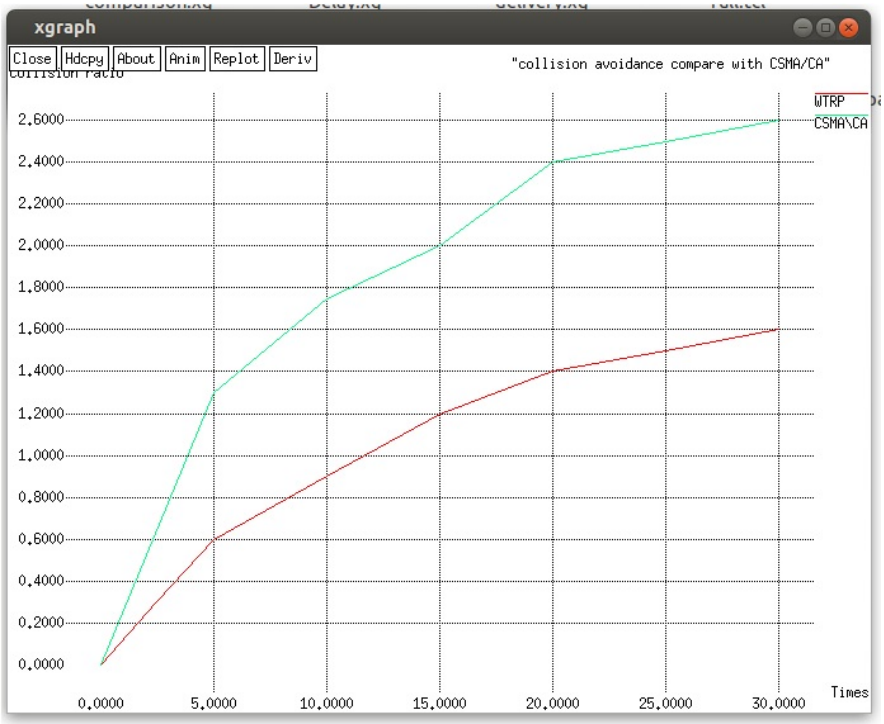


Figure6: Comparison of Collision

The Fig.6 shows that comparison of collision ratio of WTRP and CSMA/CA

CONCLUSION

In Clustered WSN, multiple access leads to huge packet loss and delay in data transmission caused by retransmitting packets. Using the Wireless Token Ring Protocol, this problem is avoided thereby ensuring an enhanced delivery of packets to the sink nodes. Passing of token through the cluster head makes reducing of collision occurring. The 'Token Holding Time' of sensor node brings every cluster head have a equal amount of time to transmit their data and 'Token Rotation Time' gives token simultaneously forwarded to every cluster head through the Maximum Token Rotation Time of the sensor network. Therefore the proposed Collision Free MAC protocol to effectively minimize collision. This would optimize the energy consumption in the wireless network thereby increasing the lifetime of the network.

REFERENCES

[1] G.Rajsekar, MichaelK.Mathew, N.Dineshrajl, S.RajBarathl, M.NesaSudhal, Dr.M.LValarmathi, "Collision Avoidance Scheme in Energy Constrained Wireless Sensor Networks Using MAC Protocol, International Conference on Computing, Communication and Networking (ICCCN 2008"), IEEE, 2008

[2] H-C. Le, H. Guyenne, N. Zerhouni, "New Contention Access Method for Collision Avoidance in Wireless Sensor Network's, International Conference on Networking (ICN'07), IEEE. 2007

[3] Abhishek Samantha, Drip to Bakshiy, Amitava Mukherjeez, Mita Nasipuri, ," Energy Efficient Wireless Sensor MAC protocol for collision avoidance", International Conference on Networks & Communications, IEEE, 2009

[4] KAZEM SOHRABY, DANIEL MINOLI, TAIEB ZNATI, "Wireless Sensor Networks Technology, Protocols, and Applications"

[5] Mustafa Ergen, Duke Lee, Raja Sengupta, Pravin Varaiya, "WTRP—Wireless Token Ring Protocol", IEEE Transactions on vehicular technology, vol.53, No.6, November. 2004

[6] Jianwei Wang, Yuping Zhao, Dong Wang, Timo Korhonen, , " Collision Avoidance Multiple Access in Wireless Sensor Networks" , IFIP International Conference on Network and Parallel Computing - Workshops, IEEE, 2007

[7] "A modified wireless token ring protocol for wireless sensor network", 2012, IEEE

[8] Duke Lee, Roberto Attias, Anuj Puri, Raja Sengupta, Stavros Tripakis, Pravin Varian," A Wireless Token Ring Protocol for Intelligent Transportation Systems" , 2001 IEEE Intelligent Transportation Systems Conference Proceedings - Oakland (CA) USA = August 25-29

[9] Duke Lee, Roberto Attias, Anuj Puri, Raja Sengupta, Stavros Tripakis, Pravin Varaiya, " A Wireless Token Ring Protocol for Ad-Hoc Networks ", IEEE. 2002

[10] In Taek Leemt , Mary Wu, Chonggun Kim, " A MAC scheme for avoiding inter-cluster collisions in wireless sensor networks", ICACT, 2010

[11] Shaiful Alam Chowdhury, Mohamamd Tauhldul lslam, Fariha Tasmin Jaigirdar, Md. Rokan Uddin Faruqui, Shahid AI Noor, " Performance study and simulation analysis of CSMA and IEEE 802.11 in Wireless Sensor Networks and limitations of IEEE 802.11", International Conference on Computer and Information Technology (ICCIT 2009), IEEE,. 2009

[12] Maotao Xie1, Xiaoli Wang, "An Energy-Efficient TDMA Protocol for Clustered Wireless Sensor Networks ", ISECS International Colloquium on Computing, Communication, Control, and Management, IEEE, 2008

[13] http://www.isi.edu/nsnam/ns/ns-documentation.html

[14] www.isi.edu/nsnam/ns/tutorial by Marc Greis tutorial on ns2.

[15] The ns Manual (formerly ns Notes and Documentation), May 9, 2010

[16] Ming zhang, Suoping Wang, ," An Novel Energy-Efficient MAC Protocol based on Collision Avoidance for Wireless Sensor Networks" , IEEE, 2009
[17] Nor-Syahidatul N.Ismail, Sharifah H. S. Ariffin,N. M. Abdul Latiff,Farizah Yunus," Medium Access Control with Token Approach in Wireless Sensor Network" , International Journal of Computer Applications.
[18] C. Jandaeng and W. Suntiamontut, Nittida Elz, "Throughput Improvement of Collision Avoidance in Wireless Sensor Networks", IEEE, 2010