Improving Transport Protocol for Reliable Data Transfer in Wireless Sensor Network

Andualem W/giorgis[1], Dr. Ing. Tofik Jemal[2], Salahdin Seid[3]

[1]Samara University College of Engineering and Technology Department of Information Technology, Semera, Ethiopia

[2]Jimma University Institute of Technology, School of Electrical and computer Engineering, Jimma, Ethiopia

[3]Jimma University Institute of Technology, School of computing, Jimma, Ethiopia

Abstract: ***In the current world of Technology, wireless sensor communication technology places the major role that led us the innovative idea of using new technology for many applications. This network is applied in many application areas such as in military, agricultural, health care, environmental monitoring, industry, natural disaster prevention, wildlife tracking system, building monitoring, space exploration ,security, entertainment, seismic detection, care of the dependent people, and emergency management, dam monitoring, traffic management, and many other areas. There are challenges in providing a reliable data delivery in these applications, such as unique network topology, diverse applications, small message size, resource constraints frequent node failure and congestion. The main objective of this thesis is to improve reliable data transport protocol for wireless sensor network. In order to achieve reliability of data by detecting and recovering lost packet, by making survey on existing reliable data transport protocols, approaches and identified RMST (Reliable Multi-Segment Transport protocol) as best protocol for reliability and lastly make a survey on queue theory. The novel approach, which is named as EERMST (Energy Efferent Reliable Multi-Segment Transport protocol) has developed by hybrid (EACK and NACK), based loss detection, and recovery mechanism to grant reliability. In addition, a novel queue approach has introduced to avoid congestion in multi hop communication. Finally, new approach was tested, and evaluated with different metrics on Tinyos 2.1.x, with Five, Ten Micaz mote, meyer-heavy.txt full noisy file, in 50, 100 ms, and TOSSIM simulator on system application. From the analysis result, the end-to-end delay of EERMST was closer to NACK not more than 0.00046ms but ACK has more delay, which is 0.00231 ms. The delivery ratio of ACK is more and somewhat closer with EERMST but has more packet delay. Generally, the EERMST has less packet delay and more packet delivery ratio than the other protocols.***

Keywords: Communication; hybrid; packet; protocol; technology; topology; wireless sensor network

1. Introduction

In the current world of Technology, wireless communication technology places the major role that led us the innovative idea of using new technology for many applications. A Wireless Sensor Network is a wireless network technology consisting of spatially distributed autonomous devices using sensors. These network has the potential to change the way of living in many applications areas such as military, health care, agriculture, environmental monitoring, industry, natural disaster prevention, wildlife tracking system, building monitoring, space exploration, security, entertainment, seismic detection, care of the dependent people, emergency management, dam monitoring, traffic management , and many other areas[1,2,3].

In wireless sensor network, a large number of sensor nodes continually sense data from the environment and the critical event data need to be reliably delivered to the sink. The sink receives all the information from these sensor nodes, processes it, and sends them to the end user. Therefore, given the nature of error prone wireless links, presence of moving nodes, frequent node failure, unique network topology, diverse applications, small message size, resource constraints, and congestion affects reliable transfer of data from resource constrained sensor nodes to the sink are the major challenges in wireless sensor networks. Therefore, the design of sensor network is application specific and different applications have different reliability requirements. Applications like habitat monitoring [4], periodic collection of environmental parameters like temperature, humidity etc. can tolerate a loss in data packets.

However, in event detection sensor networks critical information pertaining to the event has to be reliably transported to the central base station. Examples of event detection applications includes tsunami monitoring for detecting tsunamis in advance and issue warnings to prevent loss of life and damage. Border surveillance monitoring for detecting the attack of enemy forces, Health care monitoring to detect abnormal patient behavior, forest fire monitoring to detect and set an alarm if a fire starts somewhere in the monitored area. In addition, tracking and inventory management using sensors with RFID readers mounted on them to detect presence and location of objects, provides information regarding the condition of the object carrying the sensors [5]. Wireless sensor network has many unique characteristics such as unique network topology, diverse applications [6], small message size, traffic characteristics, and resource constraints usually having limited resources, including low computation capability, small memory size, low communication bandwidth, and finite, and un rechargeable battery [7]. Because of this resource constraint, using traditional transport protocols, which is TCP/UDP, is not implemented on wireless sensor network. The main objective of this research was to improve transport protocol for reliable data transfer. (a) to explore Wireless sensor network, architecture and its unique characteristics (b) to study and analyze the problem of reliable data communication in wireless sensor networks, (c) To compare and contrast different reliable transport protocols in wireless sensor network in order to select the one that fits with our scenario, (d) to study queue theory in wireless sensor network, analyze the problem and develop an new de-queue algorithm, (e) to Simulate, analyze, and evaluate the performance.

2. Proposed Solution

Wireless sensor networks should be designed with an eye to energy conservation, congestion control, and reliability in data dissemination, security, and management, which often involve in one or several layers of the hierarchical protocol. Providing reliable data delivery and congestion control takes place on transport layer. Due to unique network topology, diverse applications, small message size, unique characteristics, frequent node failure and resource constraints. The proposed transport protocol should require the following:

1) The protocol should be able to provide robustness to the network and be able to adapt to different scenarios, such as node failure and route changes.
2) Fairness: In wireless sensor network, most of the data flows are transmitted from many sensor nodes that deployed in physical environment to a sink node. In such a multi-hop many-to-one, routing structure nodes deployed far from the sink are not equal in message delivery, which can often result in unfairness. The packets deliveries of nodes far away from the sink have a higher possibility to get lost during transmission than packets from closer sink nodes.
3) Energy Efficiency: a sensor node usually has limited energy. For this reason, it is most important to be considered here for designing a transport protocol to keep high-energy efficiency in order to prolong the network lifetime.
4) The proposed protocol is applicable in multi-hop network architecture, in which a sensor node transmits its sensed data toward the sink via one or more intermediate nodes, in order to maximize the packet delivery and reduce the energy consumption for communication.

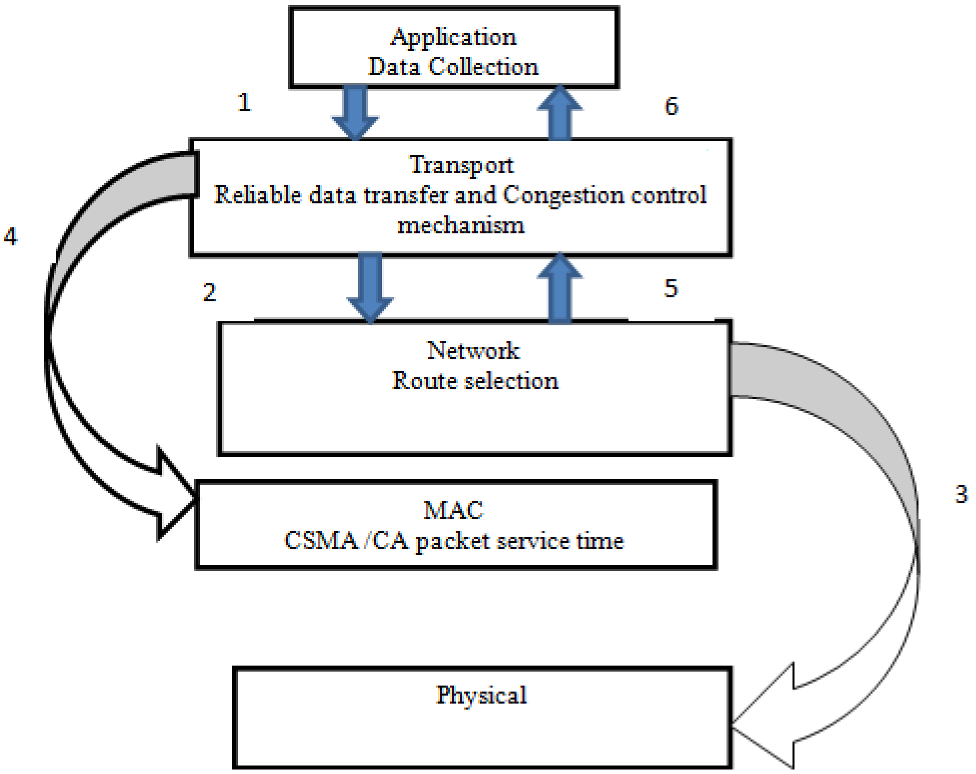

Figure 2.1: The architecture of reliable proposed protocol

The improved protocol, which named as EERMST (energy-efficient reliable multi-segment transport protocol). Beside this, the novel method that uses hybrid (Explicit Acknowledgement and Negative acknowledgement) lost packet recovery mechanism is introduced. The Explicit Acknowledgment cheeks the last/single packet in the transmission is successfully delivered or not. If the packet is lost within predetermined period the sender retransmits the lost packet. These mechanisms to handle single or last packet lost problem and to solve all packet in the communication lost which provides highest reliability guarantee in addition to Negative acknowledgement. In addition, a novel new queue management approach is introduced to solve the accumulated delay at each hop and to limit the congestion due to sudden happening of an event. This queue management approach is by giving higher priority for retransmission packet rather than new incoming data or old data (routed data) in the queue. Thus, it improves the energy consumption, improves network performance, higher reliability guaranty, increase the network lifetime, and reduces congestion. The state diagram as illustrated in Figure 2.2, describes how proposed hop-hop reliable data delivery protocol works and the following steps shows how protocol proceeds.

1) Sense and send physical phenomenon
2) For new packets set EACK=NACK=0
3) Intermediate nodes stores packet and process data aggregation

4) On successful reception, sink (intermediate) sends EACK=1, NACK=0 towards in reverse direction to sender and the sender deletes packet from its buffer
5) On unsuccessful reception, sink (intermediate) sends EACK=0, NACK=1 towards in reverse direction to sender with lost packet_id, sequence number. The sender resends the lost packet from its buffer.

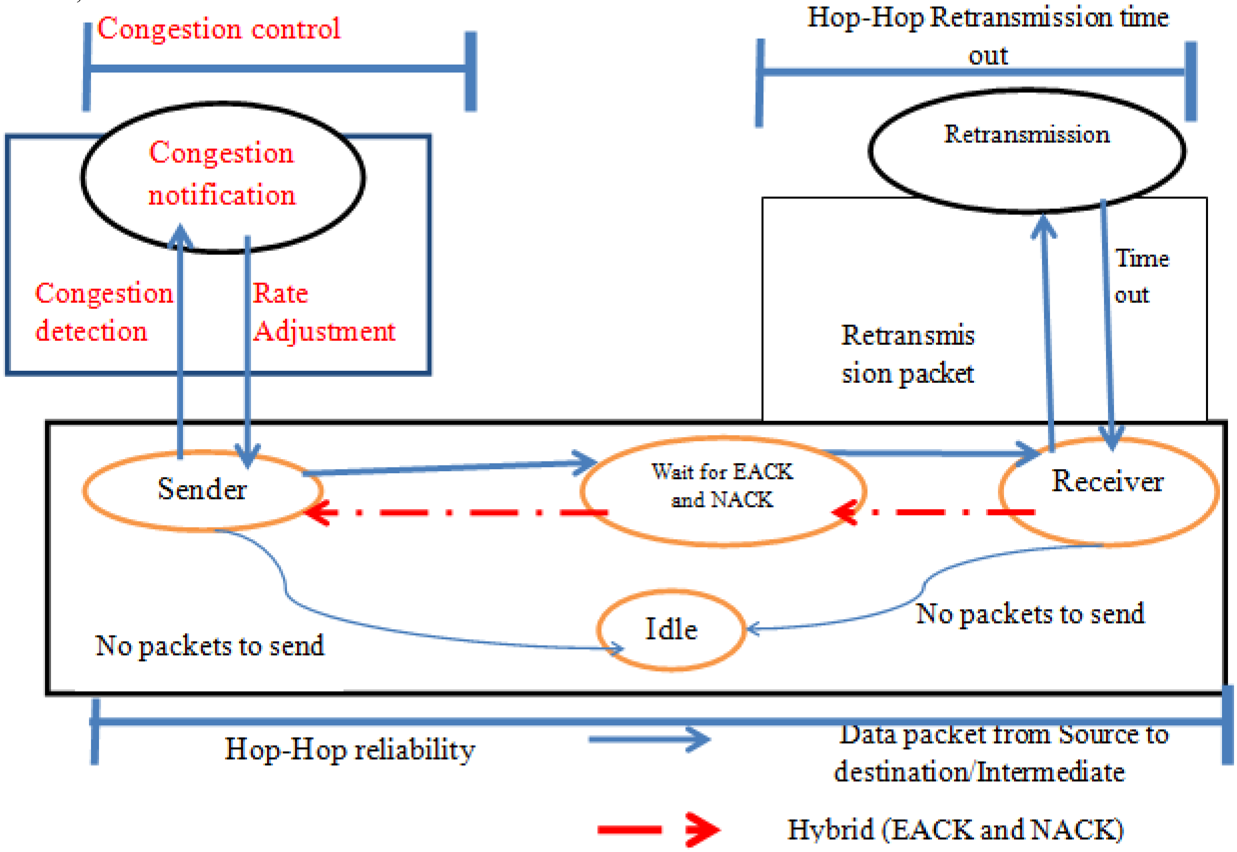

Figure 2.2: State diagram for proposed protocol

Congestion control

Congestion can occur in wireless sensor networks due to several reasons: interference between concurrent data transmissions, the addition or removal of sensor nodes in the network, or bursts of messages because of the occurrence of some events [9][10]. Congestion in the network can lead to two serious outcomes. As congestion spreads, buffer drops will increase quickly and become the dominant reason for packet loss. Significant delay can also be observed when congestion occurs.

Congestion Detection

Used to detect congestion in sensor networks based on the observation that congestion can result in excessive queuing and based on the number of times the channel is sensed busy, a utilization factor can be calculated to deduce the congestion level of the network.

Congestion Notification

When network congestion is detected, the congestion notification information needs to be conveyed from the congested nodes to their neighbors or to the source nodes or destination nodes.

Rate Adjustment:

A straightforward way of alleviating congestion is to simply stop sending packets into the network, or to send at a lower rate. The rate adjustment decision can be made by the congested nodes themselves, by a node outside the congested area (sink node), or by a predetermined policy.

Sender Operation

The sender (sensor node) sends any sensed packet to receiver, before sending the packet, it first examines the existence of retransmission packet in the queue. If there is retransmission packet, sender chooses the packet into higher priority in order to retransmission first. If the packet is being transmitted for the first time, and the sender knows that it will be sending new packet to receiver until end of the last end packet and sends EACK for last packet and wait for EACK and NACK. In the latter case, the sender will not send any new data packet until it gets an EACK back for last packet. If NACK value=1, it resends the packet.

Receiver operation

When a packet is received from the sender, the receiver accepts the packet and stores the packet in to his or her own cache. If the packet is successfully received, it acknowledges NACK=0 and EACK=1 value to back ward direction, on other hand, if there is one or more missed packet, it acknowledges NACK=1 and EACK=0 with missed packet_id and sequence number. The packets that have acknowledge EACK=0 were dropped from the sender's queue. **Algorithm 2,** Modified algorithm to improve reliable transfer of multiple messages by using hybrid EACK/NACK based loss detection and recovery.

```
Notation: BS =base station; Seq_no= Sequence number =1; Buf=Buffer ;P=Parent;
C=Children ; Node_Id=Node identification; EACK=Implicit acknowledgement
;NACK=Negative Acknowledgement ;Initially EACK=NACK=0;
    Up on sensing event /physical phenomena E:
      Begin
Create data message M= (seq_no, node_id, packet_id, Data)
        Add a copy M to message buffer
            Do send message to parent node
            While packet_id is not equal to last data packet_id
                Sequence ++;
                Send message M;
                Packet_id ++;
            End while
            Send EACK for last data packet_id;
            End Do
```

```
Up on receiving message:
IF M is successfully received;
   Send (NACK=0) and (EACK=1) to reverse direction
   Add a copy M to its own buffer
         IF Node_Id is not equal to BASESTATION/Sink
 Call ParentSelection ( ) to find a new parent Until Node_Id equal to base station;
      Send M to next parent
      Send EACK for last data packet_id;
 End both IF
Else
  Look for copy of message in its buffer;
    IF message is not found in the buffer;
 Sends (EACK=0 and NACK=1) towards reverse direction with seq_no and missed data
packet_id;
  Call LookForMesgInchild ( ) //to find message M in childes buffer
       End If
End Else
Procedure ParentSelection ( )
         IF the current node_id is BS end parent selection
            Else select next parent
                  Loop
End IF
Procedure LookForMesgInchild ( )
    IF data packet_id AND seq_no found in its buffer
         Resend the data packet
         Else,  select next Child until found missed data packet
         End IF
```

2.1. Experimental Environment Setup

The proposed protocol is implemented in the network embedded systems C (nesC) programming language and the TinyOS operating system. nesC is a component based event-driven programming language based on the C programming language. TinyOS is an open source component-based operating environment written in nesC and TOSSIM for discrete event simulator for TinyOS sensor networks. The MicaZ wireless sensor motes are used for our experiments. Each MicaZ mote has an ATMEL 7.37 MHz ATMega128L, low power 8-bit micro-controller with 128 KB of program memory, 512 KB measurement serial flash data memory, and 4 KB EEPROM. It uses Chipcon CC2420 radio, a single-chip IEEE 802.15.4 compliant radio frequency transceiver operating at 2.4 GHz, and is capable of transmitting at 250 kbps. The meyer-heavy.txt noise trace file and topology file. The Experimental parameters are:

Simulation Parameters	Values of Simulation Parameter
Number of Sensor Nodes	5,10,15
Number of Sink Nodes	1
Sending Interval	50,1000 ms
Message Size	2 Byte (default)
Data rate	250 kbps
Active Message Type	6
Simulation runs	TinyOS 2.1.x

2.2. Experimental Design

In order to demonstrate the impact of different parameters to the performance of the proposed approach, all of the experiments in this study are conducted by varying network topology ,internal noise level as well as external. Each of the sensor nodes is programmed to create data packets and send them as well receive packet from its upstream neighbor, to its downstream neighbor. Each sensor node creates a new data packet every 1000 ms.

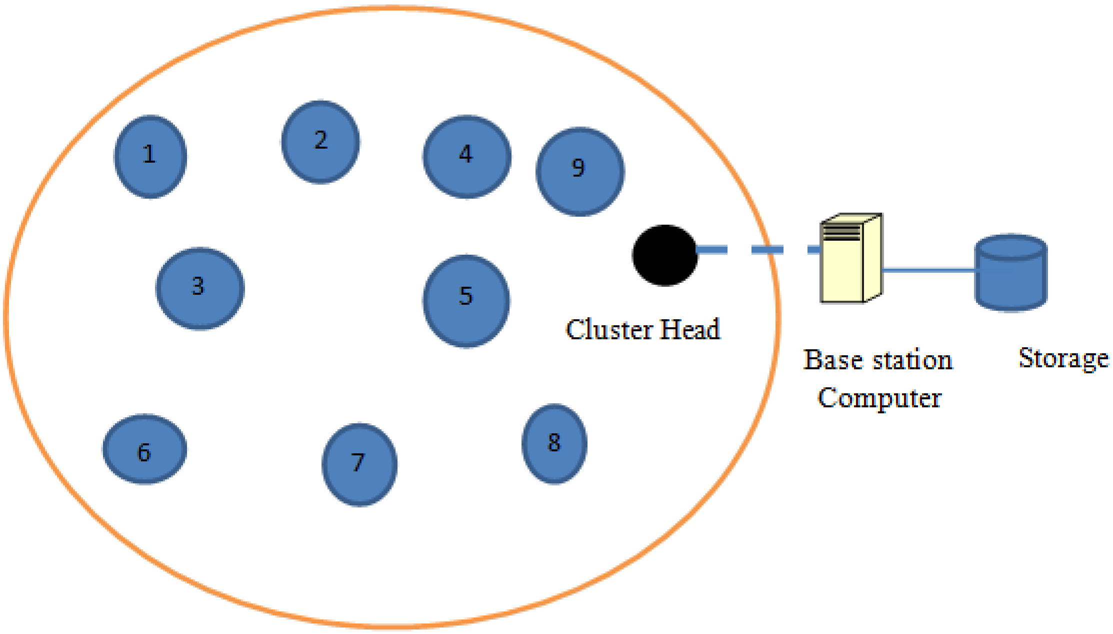

Figure 2.3: Experimental Design

The implementation of this proposed EERMST protocol is implemented on system of sensor node, which would sense temperature and transport this data to destination and applications, which detects the movement of object in a certain place to protect disaster. The role of EERMST has implemented at the time of transportation of data over network. If the radio strength between the motes is stronger than noise, data is delivered from source to destination. Otherwise, the packet is going to be lost or takes more time to deliver. In addition, in real environment there are many noises caused by interference or multipath effect. For example, waves can be reflected in building can be a noise have been included in the simulation result. From the result, all motes are powered on at the same time and the sink node enforces to start data monitoring session at the same time. Finally the motes responds it data to sink node. The Figure 2.4 displays simulation result.

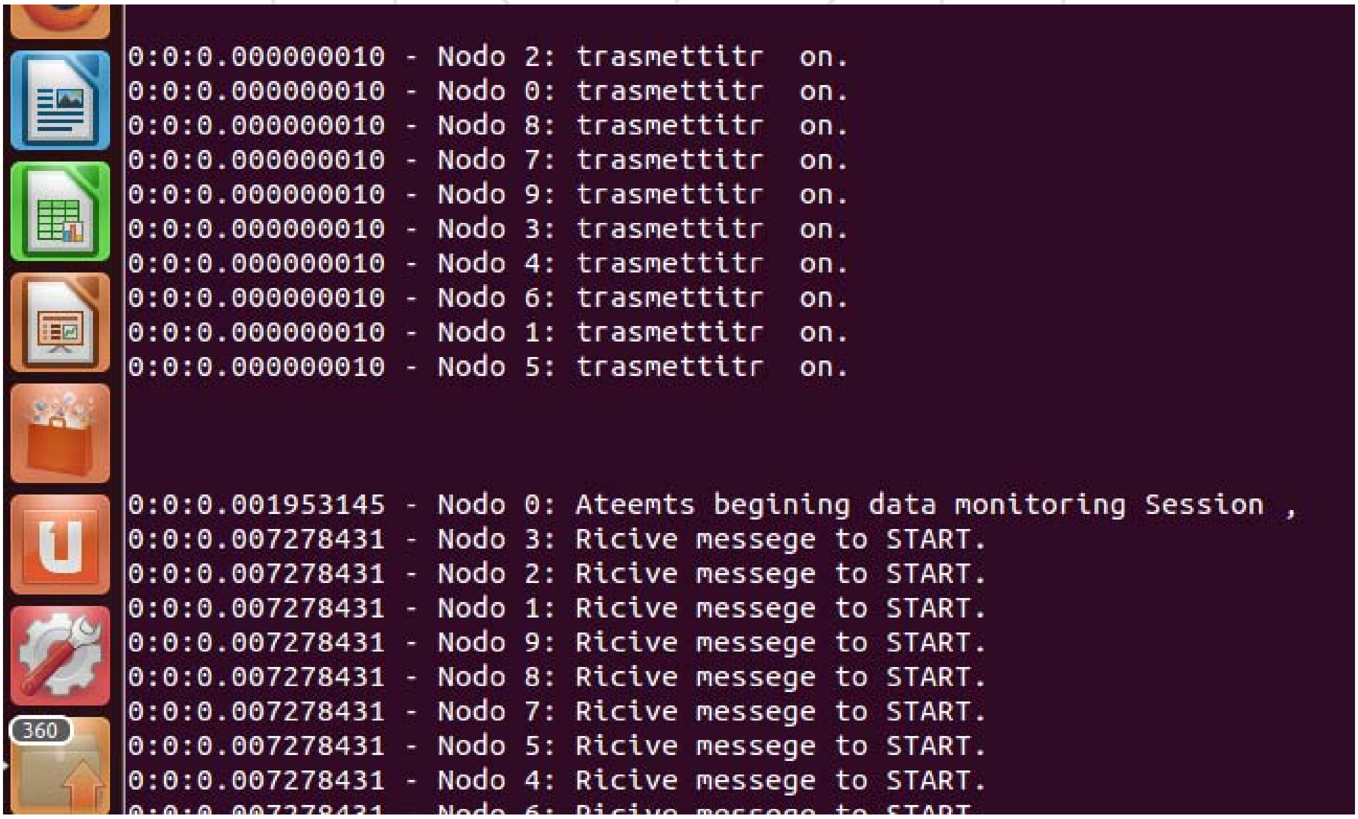

Figure 2.4: The screen shot of TOSSIM simulator (CLI)

Paper ID: ART20163569 DOI: 10.21275/ART20163569

2.3. Performance Evaluation Metrics

In the experiments, the following metrics are considered when analyzing the performance of the proposed protocol:

2.3.1 End-to-End Delay: The end-to-end delay is measured as the interval between the generation of a data packet at its source and the reception of that packet at the sink. The end-to-end delay shows the average amount of time it takes for the network to deliver a data packet from a particular source node to the sink.

End-to-End-Delay =

$$\sum \frac{Packet\_Arival\_Time - Sent\_Packet\_Time}{Total\_number\_of\_Connection\_Pair} \quad \textbf{(1)}$$

2.3.2 Link Delay: The link delay measures the interval from when a packet is created at the sender to the time it is received at the next hop receiver.

2.3.3 Delivery Ratio

It is defined as the ratio of the number of unique packets successfully received at the sink to the number of packets forwarded by the sources. This illustrates the level of delivered packet to the destination. Equation (2) shows the delivery ratio calculation.

$$\textbf{Delivery Ratio} = \frac{\sum \text{Number of packet received}}{\sum \text{Number of packet send}} \quad \textbf{(2)}$$

2.3.4 Resend Rate

As the name indicates, the resend rate is a measure of the frequency of retransmissions by a node. The resend rate for each sensor node is calculated as the number of resent data packets divided by the total number of data packets sent by the node. A higher resend rate indicates that more of the senders' transmissions at the link are unsuccessful. Since retransmitting packets may cause higher waiting time in the transmission queue, the resend rate has significant impact on both the end-to-end delay and the link delay.

2.4. Result and Discussion

2.4.1. Analysis of End-to-End Delay

This metric is important to know how long time for each packet to reach from its source to destination. The proposed algorithm (EERMST) which is the combination of two loss recovery approaches compared with each ACK, NACK loss detection, and recovery mechanism. The experiment tests the performance of ACK, NACK approach with the same 50 and 100 ms timer in order to manage the expiry of time and having five, ten nodes with the same gain value of -30.0 dBm. Figure 2.5 and 2.6 depicts the result of the simulation, which shows end-to-end delay of three protocols. In the ACK protocol, each data packet requires acknowledgement and the new data packet cannot be sent until the previous sent was acknowledged by receiver, in addition it assures each packet delivery however has more delay than other. In NACK protocol, only the lost data packet requires acknowledgment. The hybrid proposed protocol is compared with NACK in 50 and 100 ms timer, the performance results in the NACK 50 and 100 ms experiment are closer to the result of new approach. However, resend rate is low compared with two experiments. In these approaches, the new data packet cannot be sent until the receiver acknowledged previous sent packet with in sending interval. The analysis result of proposed approach shows that, each sensor node is started monitoring session twelve times roundly. From these rounds, only two nodes required resending the missing packet from its local buffer and the other nodes delivers their packet effectively.

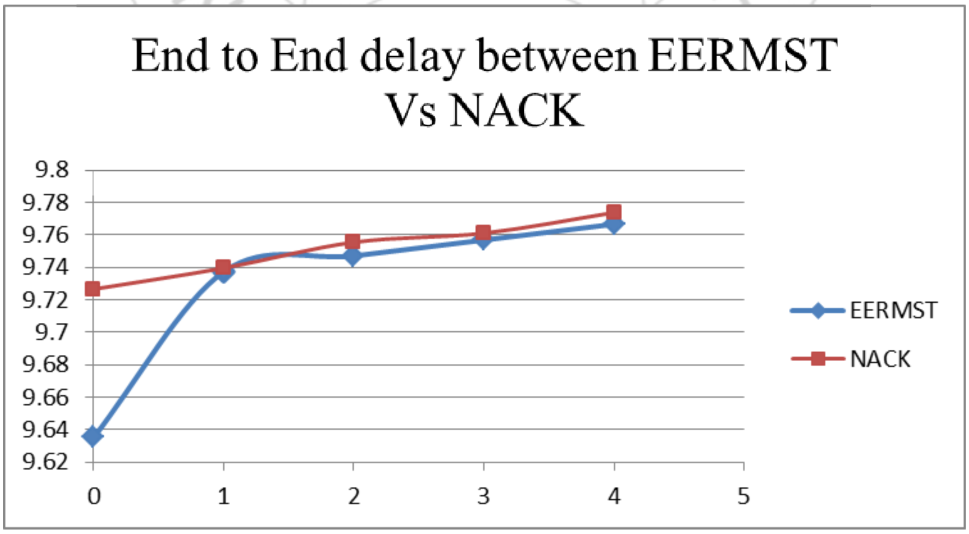

Figure 2.5: End-to-End delay between EERMST Vs NACK

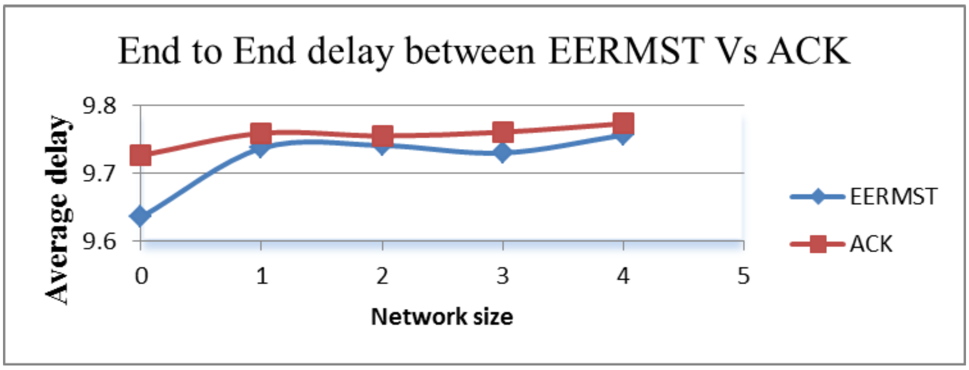

Figure 2.6: End-to-End delay between EERMST Vs ACK

2.4.2. Analysis of Link Delay

This metric used to know how long time the packet to reach from source node to next hope. To evaluate the performance of our protocol, the experiment tested on fixed network size with varying the internal noise level having 30, 40,50,60,30 respectively. The average delays to deliver a packet from source to next hop have computed in the results that obtained from the experiment. The result shows that, the delay increase as noise level increase. As would be expected, more packet loss will happen when increasing noise and it will extend the delivery delay.

2.4.3. Analysis of Delivery Ratio:

As stated in chapter two, many applications need success especially in critical based events, which depends upon reliable delivery of events. Delivery ratio represents an important metric to estimate reliability. The packet delivery ratios for a network size of 5, 10, and 15 nodes have demonstrated and it shows that similar delivery ratio result except with varying noise level. Each node has sent 200 number of packet sent and the sink node can received from the sent packet as shown in Figure 2.7. The proposed EERMST and ACK achieves good packet delivery ratio in all scenarios with highest noise level than other NACK protocols. They also have a best packet delivery ratio with light noise.

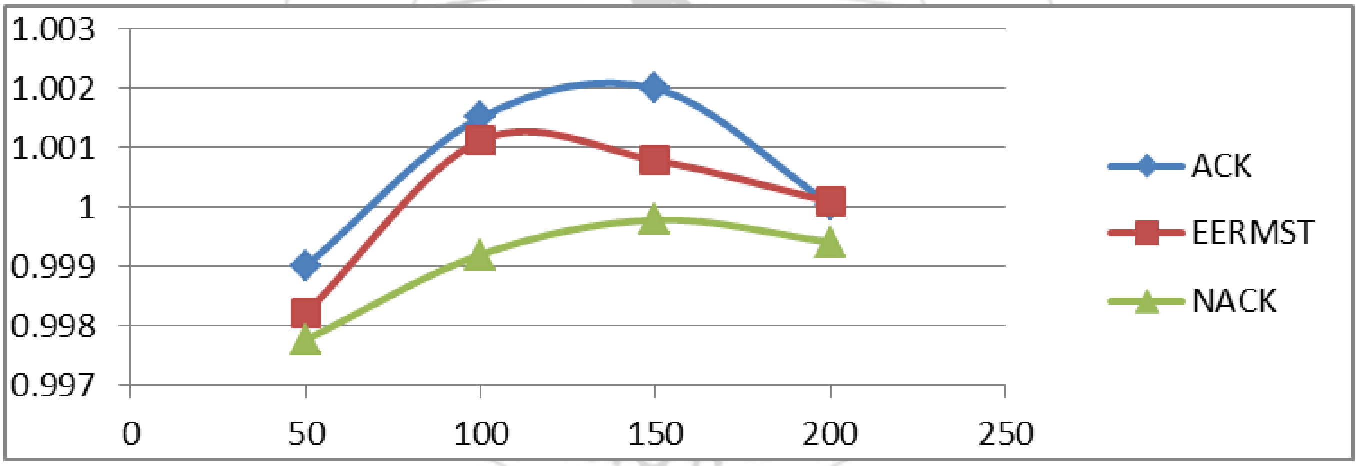

Figure 2.7: Delivery ratio of three protocols

3. Future Work

The major functions of transport control protocols are congestion control, guaranteeing of reliability and energy conservation. There are different existing protocols studied to achieve theses functionalities. The existing protocols focuses are only either congestion or reliability guarantee in uni-direction (upstream or downstream), and none of them settles congestion control and reliability simultaneously in both directions. In addition, the application which requires both congestion control and reliability guarantee, in either (upstream or downstream). Therefore, an adaptive mechanism is required to support packet reliability and congestion control in both directions. The developed queue algorithm was not implemented, for future; it needs implementation and evaluation of algorithm.

4. Conclusion

This thesis studded the general overview of wireless sensor network, application areas, network architecture, protocol stuck, operating system used for wireless sensor network. The thesis focuses on reliable data deliver issues in transport layer of protocol. In addition, general issues in designing a reliable data transport protocol for wireless sensor networks have also discussed. The survey is conducted on existing data transport protocols focusing on reliability, control protocols and general issues in designing a reliable data transport protocol for wireless sensor networks. The challenges for providing reliable data delivery are unique network topology, diverse applications, small message size, resource constraints, frequent node failure, and congestion. The hybrid based loss detection and recovery mechanism is designed to provide a solution to last or single packet delivery problem in hop-by-hop recovery mechanism and NACK loss detection approach. The novel approach is to introducing timer based Explicit ACK approach to the NACK approach to handle the problem. In addition, a new queue management method is also introduced in order to alleviate and handle congestion control by using priority based queue method by dropping unwanted packet from the communication. Finally, new approach was tested, and evaluated with different metrics on Tinyos 2.1.x, with Five, Tenand fifteen Micaz mote, meyer-heavy.txt full noisy file, in 50, 100 ms, and TOSSIM simulator on system application. From the analysis, end-to-end delay is closer to NACK not more than 0.00046ms but in ACK, its delay is 0.00231 ms. The delivery ratio of ACK is somewhat closer with EERMST but has more packet delay. Generally, the EERMST has less packet delay and more packet delivery ratio than the other protocols.

5. Acknowledgment

First, I would like to say thank you to God who has given me the strength to endure all the difficulties and challenges of life. Secondly, I would like to thank my principal advisor Dr.Ing.Tofik Jemal and Co-Adivisor Mr. Salahdin Seid for their endless patience and giving me insightful ideas to improve the work and the constant motivation and support during my work. I would also like to express my sincere gratitude to Ing.Ermyas Girma for encouragement and initiation.

References

[1] I. Khemapech, I. Duncan, and A. Miller, "A Survey of Wireless Sensor Networks Technology," in 6th Annual Postgraduate Symposium on the Convergence of Telecommunications,Networking and Broadcasting, Liverpool, UK, 2005.
[2] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a Survey," Computer Networks (Elsevier), vol. 38, pp. 393-422, 2002.
[3] D. Estrin, "Embedded Networked Sensing Research: Emerging System Challenges," in NSF Workshop on Distributed.
[4] Mainwaring, Alan. Polastre, Joseph. Szewczyk, Robert. Culler, David. Anderson, John. Wireless Sensor Networks for Habitat Monitoring. First ACM Workshop on Wireless Sensor Networks and Applications. September 28, 2002. Atlanta, GA, USA
[5] McKelvin, M. L., Williams, M. L., and Berry, N. M. 2005. Integrated radio frequency identification and wireless sensor network architecture for automated inventory management and tracking applications. In Proceedings of the 2005 Conference on Diversity in Computing(Albuquerque, New Mexico, USA, October 19 - 22, 2005). TAPIA '05. ACM Press, New York, NY, 44-47.
[6] I. F. Akyildiz , W. Su , Y. Sankarasubramaniam , Y. , and E. Cayirci , " Wireless sensor networks: A survey " , Computer Networks (Elsevier) Journal, vol. 38 , no. 4 , Mar. 2002 , pp. 393 – 422 .
[7] I. F. Akyildiz , T. Melodia , and K. R. Chowdhury , " A survey on wireless multimedia sensor networks " , Computer Networks (Elsevier), vol. 51 , no. 4, Mar. 2007 ,pp. 921 – 960 .
[8] C. Wang and K. Sohraby, "A Survey of Transport Protocols for Wireless Sensor Networks," IEEE Network, 2006.
[9] Iyer, Y.; Gandham, S. and Venkatesan, S. "STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks". Proceedings of IEEE ICCCN 2005, San Diego, CA, USA, October 2005.
[10] N. Tezcan and W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor network," International Journal of Sensor Network, 2007.