Designing Path Assured Data Transfer Protocol for Wireless Sensor Network

Ashwini D.Karanjawane[1], Atul W. Rohankar[2], S. D. Mali[1], A. A. Agarkar[2]
[1] *Department of E&TC, Sinhgad College of Engineering,Pune, India*
[2]*Department of IT, Sinhgad College of Engineering,Pune, India*

Abstract

wireless sensor networks is a growing class of highly dynamic, complex network environment on top of which a wide range of applications, such as habitat monitoring, object tracking, precision agriculture, building monitoring and military systems are built. The real time applications often generate urgent data and one-time event notifications that need to be communicated reliably. The successful delivery of such information has a direct effect on the overall performance of the system. Reliable communication is important for sensor networks.
The traditional transport layer protocols in WSN are not directly useful to meet this requirement. There is a need to synthesize the WSN characteristics and transport layer requirement for the same. Motivated by these challenges, we propose an autonomous and distributed mechanism, called as "Path Assured data Transfer" (PAT) mechanism for fast and reliable transmission for urgent information in WSNs.

1.Introduction

The wireless sensor network (WSN) is one of the most promising technologies which will help to make our society safe, secure, and comfortable[1]. A WSN as a social infrastructure would carry both urgent and non-urgent information, which apparently should not be handled equally. The urgent information, in areas like security, disaster, environmental, and vital conditions monitoring applications, has to be carried through a WSN with higher reliability and lower delay than other periodic non-urgent information for regular monitoring and working space control. It means that a WSN must be capable of differentiating and prioritizing packets depending on their urgency and importance according to requests from the application layer. Main motivating scenario for this concept is the realization of quality-enabled networks for environmental monitoring in disaster prevention and emergency response scenarios such as earthquakes, underground mines etc.

In this paper, we present survey of transport layer work cited in the literature. Classification and relevance to the WSN scenario is discussed to formulate the specification and guidelines for PAT protocol. Further we discuss the core functionalities of the transport layer protocol and its implementation issues. Simulation of the PAT is presented in ns-2 network simulator along with hardware realization of the same. The simulation results and hardware results are presented.

1.1. Organization of the paper

Rest of the paper is organized as follows: Section 2 provides overview of the related work on transport protocols and urgent information transmission. Different approaches and design issues of existing transport layer for reliability and congestion control are also discussed. Path Assured Transfer protocol its design and implementation details along with network architecture are described in section 3. Section 4 presents testing details and result evaluation and finally we conclude with features and future scope of given approach in section 5.

2.Literature survey

A large number of wireless sensor network applications require reliable data delivery. However, due to the nature of sensor networks, designing a reliable data transport protocol faces many challenges, such as node energy consumption, large number of nodes, data-centric networking, and small message size [2, 3].This section provides overviews and literature survey on transport protocol for reliable data delivery, congestion control & congestion elimination in WSN. There are several transport protocols that

have been designed for wireless sensor networks. Some of the transport protocols have been listed and summarized in Table 2.1. A separate table of the transport protocols employing congestion elimination schemes have been summarized in Table 2.2.

2.1. Transport protocols for reliability and congestion control

Table 2.1 shows some of the transport layer protocols for WSN. Description of important parameters like congestion detection mechanism, congestion avoidance mechanism and reliability technique for communication is also listed. Few of them support only reliability; some of them support only congestion control and several protocols provide both reliability and congestion control. Reliability and congestion control are the main functions at transport layer which ensure the proper delivery information from source to destination or sink node. To ensure reliable packet delivery hop-by-hop or end-to-end error recovery and acknowledgement schemes are used. PSFQ and RMST protocols use Hop-By-Hop error recovery for reliability and do not provide any congestion control scheme.

Protocols like ATP, STCP, ART, Flush, RCRT, CTCP, CRRT, offer end-to-end error recovery in which only the final destination node is responsible for detecting loss and retransmission request. This approach will cause large delay and low throughput. Other protocols like RTMC, CRRT, PSFQ, RMST, CODA, PCCP, SenTCP, offer hop-by-hop packet error recovery which is widely accepted recovery mechanism in sensor networks. Besides that, most of the protocols used negative acknowledgement (NACK) and time out for loss detection and notification stage and uses packet retransmission for loss recovery. Each proposed method has advantages and disadvantage that are application specific.

There are many protocols that provides both reliability and congestion control. These protocols can be categorized on basis of congestion detection technique.

1. Congestion control with Queue Occupancy (QO)
2. Congestion control with decentralized parameters

STCP, ATP, Flush and ESRT solely detect the congestion when the buffer usage is higher than the predefined threshold, whereas CRRT and SenTCP use packet rate addition to the buffer occupancy. CTCP uses both transmission error loss rates and the buffer usage. CODA uses channel status with QO.

Table 2.1. Summary of existing transport protocols

Attribute → / Protocol Name ↓	Category	Dire-ction	Congestion		Reliability		
			Congestion Detection	Congestion Avoidance	Level	Type	ACK
PSFQ [4]	Only Reliability	DN	-	-	Packet	H-B-H	NACK
RMST[5]		UP	-	-	Packet	H-B-H	NACK
CODA[6]	Only Congestion	UP	QO,Chan. Status	Rate Adjs.	-	H-B-H	-
Sen TCP[7]		UP	QO,Packet rate	Rate Adjs.	-	H-B-H	-
PCCP [8]		UP	Metric ratio	Rate adjs.	Packet	H-B-H	NACK
ESRT[9]	Both Reliability and Congestion Support	UP	QO	Rate Adjs.	Event	E-to-E	-
ATP[10]		Up	QO	Rate Adjs.	Packet	E-to-E	NACK
STCP [11]		UP	QO	Rate Adjs.	Packet	E-to-E	NACK
Flush[12]		UP	QO	Rate Adjs.	Packet	E-to-E	NACK
CRRT[13]		Up	QO, pkt. Rate	Rate Adjs.	Packet	E-to-E, H-B-H	NACK, MAC
CTCP [14]		Up	QO, Trans error loss	Rate Adjs.	Packet	E-to-E	eAck
PORT [15]		Up	Node price	Rate Adjs.	Event	E-to-E	-
ART [16]		Both	Ack to core node	Reduce Traffic of Noncore node	Event	E-to-E	NACK
RCRT [17]		Up	Time to recover loss	Rate Adjs.	Packet	E-to-E	NACK, Cumm. Ack
RTMC [18]		Up	Memory overflow	Header Memory Info	Packet	H-B-H	-

The congestion warning is notified to other nodes explicitly or implicitly. A direct way of avoiding congestion is to simply stop sending packets into the network, or to send at a lower rate. Main congestion avoidance techniques are packet sending rate adjustment and traffic redirection. Most of the protocols follow centralized rate adjustment scheme, whereas STCP, Flush, ART and RTMC use decentralized scheme.

2.2 Protocol with congestion elimination mechanism

The protocols employing congestion elimination techniques are listed in Table 2.2. These protocols are normally termed as urgent information transport protocols. The urgent information produced in event-driven applications has some special characteristics compared with the traditional periodic collecting scenarios.

1. When an emergency happens, a large amount of traffic are injected into the network simultaneously and in a very short time
2. In emergent situations, it is urgent to get the information about the event as quickly as possible
3. There are various types of traffic with different priorities, which should be handled with different qualities of service.

WSN would carry both urgent and non-urgent information, which apparently should not be handled equally. The urgent information has to be carried through a WSN with higher reliability and lower delay than other non-urgent information.

Lulu Liang et al. proposed a reliable transmission protocol for urgent information [19] (RETP-UI) in WSN. This protocol classifies the traffic into three classes and correspondingly maintains three kinds of priority queues in each sensor node. To predict the congestion more accurately, it detects congestion by combining the queue length and its fluctuation together. Furthermore, state machine is also introduced in evaluating the congestion level to alleviate congestion; they have proposed a multistage rate adjustment scheme. The simulation results show that proposed RETP-UI can provide a reliable transmission service for urgent information with lower packet loss probability, shorter delay, and higher throughput.

Tetsuya Kawai et al. had proposed a [20] assured corridor mechanism for fast and reliable transmission mechanism for urgent information in sensor networks. An emergency packet first establishes an assured corridor from the origin node to the BS. In the corridor, all nodes keep awake and stop generating periodic packets. The other nodes stay in normal operation. The authors have also introduced a retransmission scheme to achieve reliable transmission of the emergency packets. Their experiments showed that the corridor was quickly established and then emergency packets are transmitted to the BS with a high reliability of more than 90 % delivery ratio and a low latency of less than 90 ms.

Manikanden Balakrishnan et al. have introduced Channel Preemptive EDCA[21] (CP-EDCA) scheme. In CP-EDCA, the emergency traffic preempts the services of other routine traffic in the network for achieving deterministic MAC delay bounds. The simulation results of emergency frames shows up to 50% uniform decrease in MAC delays and insensitivity to routine traffic competition.

Rachid Haji et. al. [22] have proposed a framework for Adaptive Management of QoS in different situations (Ad-M-QoS-DS) like management of rescue operations and cooperation during a disaster. Theframwork guarantees a level of QoS using degree of information importance and QoS parameters. Under normal circumstances, the Framework focuses on the efficiency of energy consumption. Upon detection of an event of emergency, the proposed framework adapts its behavior to minimize delay and ensure reliability. Sensors transmit the information on multi-hop to the base station which is responsible for transmitting them to the Coordination Committee. The latter analyzes the information received. If the event is safe, the data will be stored in a database and if the event presents a danger the Committee takes appropriate decisions and informs the operators on the appropriate actions.

S. Sharma and D. Kumar[23] presents a framework for adaptive routing protocol which utilizes an approach of data routing based on priority. The framework defines two paths to transmit data according to their priority. It presents an enhanced version of Ad hoc On-Demand Distance Vector Routing (AODV) in order to discover and maintain the shortest path. It utilizes an ant-based protocol to construct an energy-efficiency path in order to minimize the energy consumption.

Koichi Ishibashiet. al. [24] proposed a forwarding method for urgent messages on the ubiquitous WSN. The proposed method provides a reliable forwarding method for urgent messages, even if packet loss on the wireless links exists. The urgent messages are sent from a monitoring node, appreciating the detected event as emergency situation, to a specific node such as the network management node. To meet specified requirements, they have invented a new design scheme of the ad hoc routing protocol to overcome poor

Table 2.2. Congestion elimination in urgent protocol.

Attribute		RETPUI	FARTM	CP-EDCA	ADMQOS	OD-AODV	FMUMUWSN
Direction		UP	Up	UP	UP	Up	Up
Conge-sion	Congestion Detection	QO and Fluctu-ation	Urgent data occurrence	Emergency detection	Event detection	Event classifi-cation	Event classifi-cation
	Congestion Avoidance	Multistag e Rate Adjs.	Establishing assured path by suspension of normal data transmission	Normal data preemption	Priority wise catego-rization	Priority wise shortest path transmission	Multipath transm-ission
Relia-bility	Level	Event	Event	Event	Event	Event	Event
	Type	H-B-H	H-B-H	H-B-H	H-B-H	H-B-H	H-B-H
	Ack	ACK	ACK	ACK	ACK	ACK	ACK

quality of error-prone wireless channel, in order to support the reliable forwarding method for the urgent messages on the UWSN.

We propose a path assured data transfer protocol (PAT) based on congestion elimination mechanism as proposed protocol in [20], [24]. The proposed PAT is different on two accounts. Firstly the PAT is designed for fixed infrastructure WSN which is likely network architecture for emergency event detection networks. Secondly the PAT allows to transfer block of data with assured reliability measure.

3. Design and implementation of PAT

3.1. Network architecture

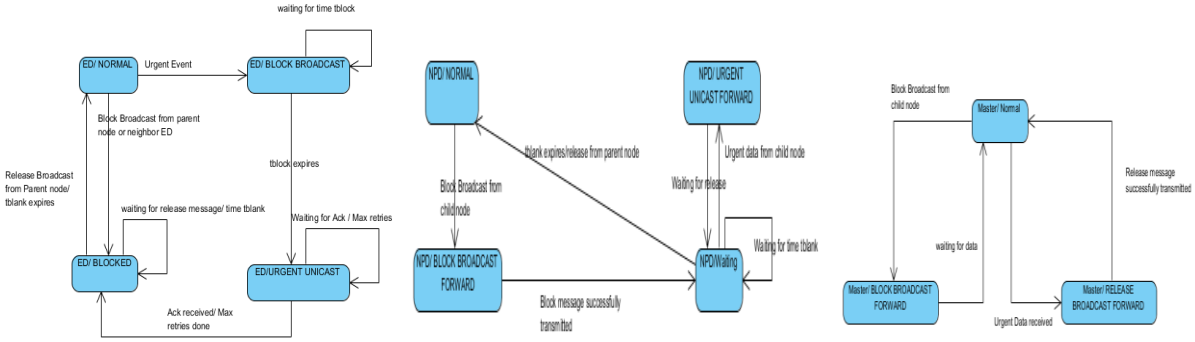
PAT uses fixed infrastructure network architecture proposed in [25]. The network architecture is three layer architecture consisting of master at first tier, network processing device (NPD) or router at second tier and end node (ED) at third tier.

3.2. Assured Path Data Transfer

The PAT operates in three phases: a. Blocking or muting the network for assured and reliable urgent data transfer b. urgent data transfer with reliability mechanism and c. releasing the network for normal operation. A state transition diagram for each of the device in network is explained in the following sections.

3.2.1. State transition of ED. A state transition diagram for ED node is shown in Figure 3.1 (a). ED node stays in the NORMAL state in its normal operation. When a node detects an urgent event, it moves to the BLOCK BROADCAST state and initiates its tblock timer equivalent to time required to propagate the urgent broadcast message throughout the network. In this state ED begins broadcasting block message to all nodes in its range and wait for time duration tblock to finish. After tblock time ED will move to URGENT UNICAST state and start sending urgent data. Neighbor ED nodes in the NORMAL state, receives urgent broadcast moves to BLOCKED state and initiates a tblank time duration timer equivalent to time required for urgent message transfer proportional to number of packets indicated in the BLOCK BROADCAT packet. These ED nodes will wait in BLOCKED state and stop
sending normal data till occurrence of release message from its parent node or it will move to NORMAL state if tblank timer expires.

3.2.2 State transition of NPD. As shown in Figure 3.1 (b) when NPD node receives block broadcast, it moves to BLOCK BROADCAST FORWARD state and start broadcasting urgent block message to other EDs and NPDs in its range. After successful transmission of urgent broadcast NPD moves to



(a) End device (b) Network processing device (c) Master

Figure 3.1 State transition diagrams for ED, NPD and master devices

WAITING state and initiates timer of duration tblank. An Urgent packet is identified by command field in its packet header. If the NPD is a next-hop of the URGENT ED node, it moves to the URGENT UNICAST FORWARD state on receiving urgent data packet from ED. NPD will forward the received urgent packet to next hop and moves to WAITING state waiting for release message from parent node or time tblank to finish. This process of hop by hop transmission of urgent data continues till master receives urgent data packet. When all the urgent data packets are transferred this process stops. If the NPD is not involved in forwarding the urgent packet, it retains its WAITING state and wait for time tblank or release message from parent node.

3.2.3. State transition of Master. The state transition diagram for master device is shown in figure 3.1 (c). when master receives urgent broadcast from its child node it moves to state BLOCK BROADCAST FORWARD and start broadcasting urgent block message to other EDs and NPDs in its range. The master receives the urgent data packets as normal data packets. Number of urgent data packets is indicated in the BLOCK BROADCAST message. As soon as master receives last urgent packet it moves to RELEASE BROADCAST FORWARD state and starts broadcasting release message. The ED nodes in the range of master moves to NORAML state and start transmission of normal data packets. The NPD nodes in the range of master forward release message to other EDs and NPDs in its range. Accordingly, all EDs and NPDs in the network will move to NORMAL state and start normal data transmission until and unless next urgent event occurs.

The PAT operates in three stages. In the first stage the ED node desiring to transfer urgent information initiates blocking operation for rest of the devices to assure clear path for urgent data packets. In the second stage, the urgent data packets are transferred with software acknowledgment from the receiver towards the destination master node. When ll the packets are transferred, the master initiates release message for the network. The assured path guarantees collision less data transfer towards the destination devices and avoid delays due to retry transmissions.

The PAT protocol is implemented in NS2 simulator over the fixed infrastructure network architecture [25]. Hardware implementation of PAT is also studied. The performance evaluation study in this section aims at demonstrating the strengths of the proposed protocol under different topologies, packet rate variations and number of devices.

4. Result analysis

4.1. System configuration

The PAT is evaluated on WSN testbed [26]. The testbed of the hardware field experimentation consists of up to 7 sensor nodes. In each experiment, one node acts as the master and is connected through a UART interface to a computer. The Master is responsible for receiving data packets and logging network information. Every network device in the network records all the incoming and outgoing packets ,which

are retrieved after the experiment for analysis. Other sensor nodes are programmed with the normal periodic data packet transfer protocols and one with urgent data packet protocol. The new protocol is independent of the underlying network topology and routing protocol. All sensor nodes are deployed in a single line topology and the distance between two neighbor sensor nodes is 5m. The node's radio power level is set to 0 dBm and the transmission range of the resulting network is just over 1 hop. All the nodes in the experiment are time-synchronized prior to each experiment. Sensor nodes as well as the master record the information of each packet received and log them into the on-board flash memory. The Master broadcasts a control message at the end of each experiment. Upon receiving the message, sensor nodes start to send the logging information saved in their local memory until all logs are transmitted to the Master.

4.2. Evaluation metrics

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

1. End-to-End Transmission Delay: The end-to-end Transmission delay is measured as the interval between the transmission of a data packet from its source and the reception of that packet at the Master. The average end-to-end Transmission delay for each source node is calculated as the average of end to-end transmission delay of all data packets generated by that node.

$$TD = T_{MRx} - T_{EDTx}$$

2.

$$ATD = \frac{\sum TD\ of\ all\ EDs}{Total\ no.of\ EDs}$$

Where,

$ATD = Transmission\ delay$
$T_{MRx} = Time, Master\ received\ Data$
$T_{EDTx} = Time, ED\ transmitted\ data$

2 Packet delivery Ratio: It is the Ratio of No. of packets received at master node to the No. of packet transmitted by ED. We have calculated Packet Delivery ratio of individual sensor node and of overall Network.

$$PDR = \frac{Prx, Master}{Ptx, ED}$$

Where,

$PDR = Packet\ Delivery\ Ratio$
$Prx = Total\ packets\ received\ by\ master$
$Ptx = Total\ packets\ transmitted\ \ by\ ED/\ EDs$

3 Total Throughput: The total throughput is measured as the number of data packets received at the sink divided by the time interval between when the first data packet is generated and the last packet is received. The achievable total throughput reflects the efficiency of the protocol. The higher the achievable total throughput, the faster source nodes can deliver their data packets to the sink.

$$NT = \frac{P\ rx, master\ from\ specific\ ED}{ATD, of\ same\ ED}$$

$$NWT = \frac{Prx, master\ from\ all\ ED}{ATD, network}$$

Where,

$NWT = Network\ Throughput$
$NT = Node\ Throughput$

It will be measure as a throughput per second

4.3. Simulation parameter

The PAT is implemented in NS2 simulator environment and conducted extensive simulation experiments. In all of the simulation experiments, 36 sensor nodes are uniformly and randomly distributed in a 500 m × 500 m two-dimensional region with a Master at its lower center. IEEE 802.15.4 non-beacon mode is used as the MAC protocol and the transmission range of radio signals is set to 2.5 m. We employ a general broadcast-based and unicast based routing protocol for the underlying network layer. In both routing protocols, we assume that each node knows its own hop distance from the master node. A NPD/router node forwards a packet to the next hop NPD and subsequently the packet reaches to destination master node.

Table 4.1 Simulation parameters

Sr. No.	Parameters	Values
1.	Simulation Time	20 Sec
2.	Sample rate Normal	20ms,50ms,100ms,250ms
3.	Sample Rate Urgent	50 ms
4.	Total No. of nodes	36
5.	Master Node	01
6.	Normal node	26
7.	Urgent Node	01
8.	Size of network area	85 m X 285 m
9.	Length of urgent Message	Variable set by program
10.	Number of next hop towards a Master node	2,3,4,5,6 hops
11.	Channel Speed	1 Mbps
12.	Packet Size	100 bytes

4.4. Discussions

4.4.1. Packet Delivery Ratio. Table 4.2 shows packet delivery rate for packet rates at 50, 20, 10, 4 packets rate for both normal EDs and urgent ED. The average PDR of normal packets decreases with increase in packet transmission rate. There is marginal decrease in PDR of urgent ED with increased packet transmission rate. The PDR for urgent packets is above 90% in most of the cases. At lower data packet rates it is 99%. Effect of number of hops is also studied and the figures in the table 4.2 shows that PDR for urgent data packet is not affected by the number of hops. The results shown in the Table 4.2 shows 20-45% increase in PDR for urgent ED. A graph for 20 packets per second packet from table 4.2 is plotted for PDR of normal EDs and urgent ED as depicted in figure 4.1. against number of hops on x-axis.

Comparison of urgent ED PDR with NOACK and ACK mechanisms applied for normal data packets is shown in the figure 4.2. It is clearly seen that PAT has improved PDR over these two mechanisms since PAT suppresses normal data transmission it guarantees 100 % reliability for packet transmission by establishing assured path.

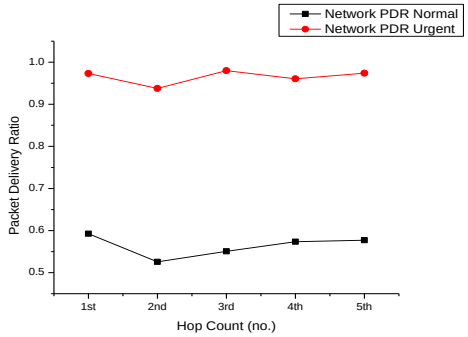


Figure 4.1. Packet delivery ratio of urgent packets hop wise (PR: Normal ED 20 pkt/sec)

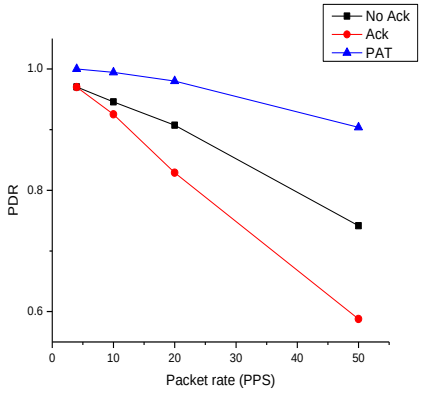


Figure 4.2 PDR of same hop ED: packet Rate wise for protocol variation (PR: 50ms both)

Table 4.2 Experimental results of packet delivery ratio

Sr. No.	Hop Count	PDR of Normal (Packet per second)				PDR of Urgent(Packet per second)			
		50	20	10	4	50	20	10	4
1.	1	0.47288	0.59256	0.83376	0.94519	0.82229	0.9734	0.98764	0.99811
2.	2	0.44614	0.52569	0.73304	0.93754	0.9036	0.93757	0.99047	0.99156
3.	3	0.42897	0.55065	0.7185	0.91177	0.8927	0.97984	0.99423	0.99904
4.	4	0.44124	0.57356	0.75955	0.906	0.89756	0.96052	0.99038	0.99904
5.	5	0.48235	0.5771	0.71245	0.91231	0.75038	0.97414	0.99327	1

4.4.2. Multiple urgent nodes. Next we consider cases where multiple nodes detect an urgent event and uses PAT protocol at the same time. The resulting Packet delivery Ratio of urgent packets for multiple number of urgent nodes is shown in Table 4.3. The more the number of Urgent nodes is, the more collisions occur. 15-20 % of urgent packets are lost in the cases of five Urgent nodes. This is because those urgent packets originated from different source nodes collide with each other in the same or merged assured path. In addition, the delay increases with the number of urgent nodes reflecting more packet retransmission due to collisions among emergency packets within a path. On the contrary, the delay slightly decreases if no. of urgent nodes are from closer hop. The reason for this can be explained as follows. In calculating the delay, we take into account only urgent packets that successfully arrive at the master. Therefore, there is a bias in favor of urgent packets emitted by urgent nodes closer to the Master than those of distant urgent nodes.

Table 4.3 Packet delivery Ratio versus no. of urgent nodes

Sr. no.	Hop count	No. of Urgent Node	Packet Delivery Ratio	Transmission Delay (msec)
1.	5	1	0.97	0.002200
2.	5	2	0.99	0.002411
3.	5	3	0.97	0.002418
4.	5	4	0.90	0.002500
5.	5	5	0.81	0.002654

4.4.3. Transmission delay. The Transmission Delay time increases linearly with the level of hierarchy of nodes for both Normal and Urgent ED, but transmission delay of normal Ed is almost double that of urgent ED for every hop. This minimum transmission delay is because of the assured path which eliminates collision and congestion.

Table 4.4: Transmission delay for normal and urgent

Sr. No.	Hop Count	Transmission delay (ms)	
		Normal	Urgent
1.	1st	0.00211	0.00105
2.	2nd	0.00178	0.00125
3.	3rd	0.00316	0.00223
4.	4th	0.00365	0.00232
5.	5th	0.00411	0.00332

4.4.4. Throughput. Figure 4.3 shows throughput for ED transmitting urgent data packet with throughput for normal data packet generating EDs. The Packet rate is 20 packets per second (50 ms packet interval) for both urgent and normal exhibits higher throughput compared with the normal data transfer protocol. The variance of the throughput is a result of the increased reliability and decreased transmission delay. Because of the implementation of the PAT the modified protocol shows 45% increase in reliability and transmission delay. The PAT shows significant improvement in the throughput as compared to the normal data transfer protocol.

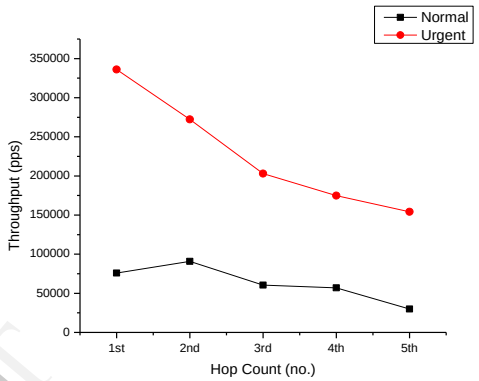


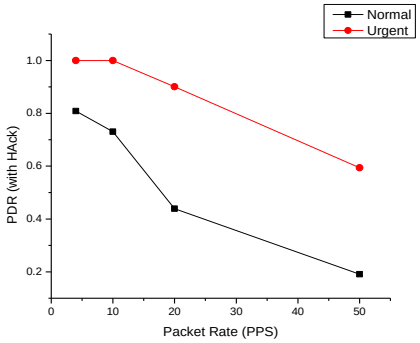
Figure 4.3 Throughput hop wise normal Vs urgent (PR: 20 Pkt/Sec,)

4.4.5 Hardware experiment results. The PAT is implemented on WSN testbed [26]. A setup of one master, one urgent packet generator ED and five normal packet generators ED nodes was used for experimentation. The protocol was evaluated for 50, 20, 10, 4 packets per second. The experiments were repeated for NOACK, HACK and SOFTACK corresponding to no acknowledgment, hardware acknowledgment, and software acknowledgment from the receiver. Three sets of experiment were conducted and average over three sets is used to compute the performance parameter.

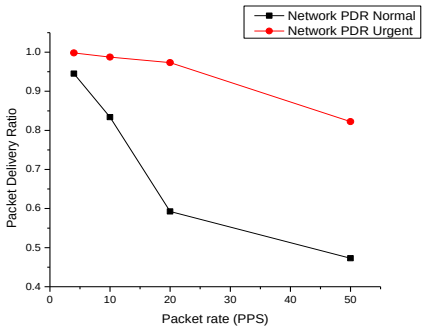
Figure 4.4 (a) shows PDR for normal packet generation scenario in which all EDs generate periodic packets at the set rate. It is compared with PDR of ED generating urgent packets. At 4 and 10 packets per second the PDR is 100% for the urgent packet ED and for normal packet generator ED it is decreasing. Further the PDR decreases for normal as well urgent packets is because the bandwidth of trans-receiver is 250Kbps and packet rate is very high causing

congestion and collision. Figure 4.4 (b) shows simulation results of PDR.

The transmission delay for normal and urgent packets is depicted in figure 4.5.The transmission delay at 4 and 10 packets per second has considerable difference, while for other higher packet rate both follows proportional increase. The hardware results for PDR and transmission delay as follows the same trend as shown simulation results.



(a) Hardware experiment result



(b) Simulation result

Figure 4.4 Packet delivery Ratio

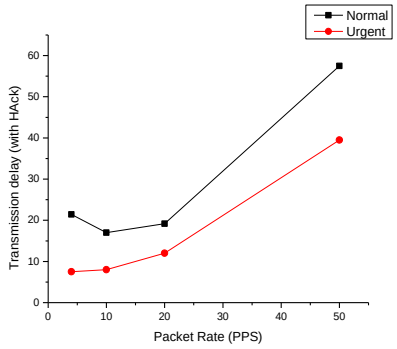


Figure 4.5: Transmission delay

5. Conclusion

WSN has many applications where time critical and urgent information needs to be transferred to the master sink node apart from regular data reporting activity. There are many protocols presented for this cause. In summary we concluded the necessity of clear path assurance to transfer urgent information. The summary also helped us to finalize some of the core functionalities for PAT. The PAT protocol presented in this paper improves the data transfer reliability over normal data transfer protocols by 20-40%.

The PAT is designed for reliable transfer of single as well blocks of urgent packets. The initial blocking time is directly proportional to size of the network and is added in to packet transmission delay of urgent packet. If block of urgent data packets is transferred then this initial delay will be distributed over all the packets and subsequently reduce the data transfer time.

6. References

[1] I. Khemapech, *et al.*, "A survey of wireless sensor networks technology," in *6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, 2005.

[2] K. S. Chonggang Wang1, Bo Li, and Weiwen Tang, "Issues of Transport Control Protocols for Wireless Sensor Networks," *University of Arkansas, Fayetteville, AR, USA,*.

[3] J. B. Postel. Sept. 1981). Transmission Control Protocol.

[4] C.-Y. Wan, *et al.*, "PSFQ: a reliable transport protocol for wireless sensor networks," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, 2002, pp. 1-11.

[5] F. Stann and J. Heidemann, "RMST: reliable data transport in sensor networks," in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, 2003, pp. 102-112.

[6] S. B. E. a. A. T. C. C.-Y. Wan, "CODA: Congestion detection and avoidance in sensor networks," *in Proceedings of ACM Sensys'03,* November 5-7, 2003 2003.

[7] K. S. C. Wang, and B. Li, "SenTCP: A hop-by-hop congestion control protocol for wireless sensor networks," *in Proceedings of IEEE INFOCOM 2005 (Poster Paper)*, Mar. 2005.

[8] K. S. C. Wang, V. Lawrence, B. Li, and Y. Hu, "Priority-based congestion control in wireless sensor

networks," in *in Proc. IEEE International Conference on Sensor Networks,Ubiquitous, and Trustworthy Computing (SUTC'06)*, pp. 22–31.

[9] O. B. A. Y. Sankarasubramaniam, and I. F. Akyidiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks," *in Proceedings of ACM Mobihoc'03,* June 1-3, 2003.

[10] V. A. K. Sundaresan, H. Y. Hseeh, and R. Sivakumar, "ATP: a reliable transport protocol for ad-hoc networks," in *in Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, pp. 64–75.

[11] Y. G. Iyer, *et al.*, "STCP: a generic transport layer protocol for wireless sensor networks," in *Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on*, 2005, pp. 449-454.

[12] S. Kim, *et al.*, "Flush: a reliable bulk transport protocol for multihop wireless networks," in *Proceedings of the 5th international conference on Embedded networked sensor systems*, Sydney, Australia, 2007, pp. 351-365.

[13] M. M. A. a. C. S. Hong, "CRRT: congestion-aware and rate-controlled reliable transport in wireless sensor networks," in *IEICE Transactions on Communications*, pp. 184–199.

[14] F. J. E. Giancoli, and A. Pedroza, "CTCP: reliable transport control protocol for Sensor networks," *in Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '08),* pp. 493– 498, December 2008.

[15] Y. Z. a. M. R. Lyu, "PORT: a price-oriented reliable transport protocol for wireless sensor network," *in Proceedings of 16th IEEE International Symposium on Software Reliability Engineering*, pp. 117–126, 2005.

[16] N. T. a. W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," *International Journal of Sensor Networks*, vol. vol. 2, pp. 188–200, 2007.

[17] J. P. a. R. Govindan, "RCRT: rate-controlled reliable transport for wireless sensor networks," *in Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*, pp. 305–319, 2007.

[18] X. G. H. Zhou, and C.Wu, "Reliable transport with memory consideration in wireless sensor networks," *in Proceedings of the IEEE International Conference on Communications (ICC '08),* pp. 2819–2824, May 2008.

[19] L. Lulu, *et al.*, "A Novel Reliable Transmission Protocol for Urgent Information in Wireless Sensor Networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1-6.

[20] T. Kawai, *et al.*, "A fast and reliable transmission mechanism of urgent information in sensor networks," *Proceedings of the 3rd International Conference on Networked Sensing Systems (INSS 2006)*, 2006.

[21] M. Balakrishnan, *et al.*, "Service preemptions for guaranteed emergency medium access in Wireless Sensor Networks," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008, pp. 1-7.

[22] R. Haji, *et al.*, "Towards an adaptive QoS-oriented and secure framework for wireless sensor networks in emergency situations," in *Multimedia Computing and Systems (ICMCS), 2012 International Conference on*, 2012, pp. 1007-1011.

[23] S. S. a. D. Kumar, "An approach to optimize adaptive Routing Framework to provide QOS in Wireless Sensor Networks," *in proceeding of International Journal of wireless Networks and Communication*, vol. 1(1), pp. 55-69 2009.

[24] K. Ishibashi and M. Yano, "A Proposal of Forwarding Method for Urgent Messages on an Ubiquitous Wireless Sensor Network," in *Information and Telecommunication Technologies, 2005. APSITT 2005 Proceedings. 6th Asia-Pacific Symposium on*, 2005, pp. 293-298.

[25] M. K. N. a. A. M. A W Rohankar, "Distributed System Architecture for WSN: SWiFiNet," *IJAIS Proceedings on International Conference and workshop on Advanced Computing 2013 ICWAC*, vol. 2, pp. 49-54, June 2013.

[26] A. W. R. M. K. N. A. Mukherjee, "SWiFiNet: a real field WSN testbed," *in proceeding of International Journal of Communication Networks and Distributed Systems (IJCNDS)*, vol. Vol. 11(2), 2013.