Adaptive Data Transmission in WSN Using Enhanced Path Assured Transmission Protocol

Avinash Devare, G.K. Mohan and Hruturaj B. Nikam

Abstract Wireless sensor network is a highly dynamic network environment and a class of wireless network specially designed for monitoring. Large number of applications such as military systems, object tracking, monitoring, disaster reporting are designed on top of the WSN. These are real-time applications and generate very sensitive data or urgent data. This sensitive information needs to communicate reliably. Accurate delivery of sensitive information has direct impact on the overall performance of the system. Achieving reliability and congestion-free communication is important for the WSN. Some urgent data transmission protocol in WSN mainly focuses on transmission of sensitive data only at the same time it neglects the normal data traffic. Motivated by these challenges, we propose a EPAT system which is autonomous and distributed. This system achieves reliable and congestion-free urgent data as well as normal data communication at the same time.

Keywords WSN · EPAT · Congestion · Urgent data

1 Introduction

Wireless sensor networks are specially designed networks that comprise autonomous system placed in distributed fashion, this autonomous devices like sensor can monitor as well as gather the context. Context may be either location, noise level, traffic condition, vibration, pressure, sound, motion, temperature, weather condition, etc., these autonomous systems have limited computation power battery

Avinash Devare (✉) · G.K. Mohan · H.B. Nikam
Department of Computer Engineering KLU, Vijaywada, India
e-mail: devarea9@gmail.com

G.K. Mohan
e-mail: gvlkm@kluniversity.in

H.B. Nikam
e-mail: hrutu4nike@gmail.com

Avinash Devare · G.K. Mohan · H.B. Nikam
Department of Computer Engineering and Information Technology,
VJTI, Mumbai, India

S.C. Satapathy et al. (eds.), *Proceedings of the International Conference on Data Engineering and Communication Technology*, Advances in Intelligent Systems and Computing 468, DOI 10.1007/978-981-10-1675-2_28

powered, less memory, and limited bandwidth. Wireless sensor network is a wide research area where hardware designs software developer user application domain expert cooperatively design efficient system autonomous device also called as node, which has its own sensing computation and wireless communication capability. Quality of service is the main design issue in WSN to achieve the QOS and efficient network performance, many efficient routing protocols, power management technique, and data dissemination protocol are specially designed. [21] wireless sensor network is self-configuration network where every sensor node communicates with each other using radio signal, it is deployed in quality to sense monitored and understand the physical world contextual info is the data sensed by sensor. Data aggregation is the process of collection of useful contextual information in wireless sensor network. It is an efficient and effective way to save limited resources data receiving from number of sensor node is aggregate as is they are about the sane attribute of the phenomenon when they reach the same routing node on the way back to the sink while collecting info by reducing the number of transmission and network. computation at intermediate node can substantially increase network efficiency on the other end, it also increases the amount of info contained in single packet and makes the system vulnerable to packet loss.

Rather than retransmitting dropped packet that causes additional delay wireless broadcasting is an effective strategy to improve delay performance data confidentiality integrity and security issue [22]. In data aggregation process is crucial when the sensor network is deployed in adverse environment, because of high packet loss rate in WSN more reliability in data transmission is desirable because of WSN application require various level of communication reliability. We proposed urgent data transmission scheme where sensitive data is transmitted on priority basis or via dedicated path at the same time normal data packet transmission is also takes place using efficient mechanism [1].

2 Transport Layer Protocol Characteristics

In wireless sensor network, there are two major functionality of transport layer protocols that are congestion control and reliability. Transport layer in WSN supports reliable message delivery, congestion control mechanism, and efficient energy management.

Packet loss in the WSN is occurred due to congestion, wireless channel quality and sensor failure, memory full, bad radio communication, and packet collision. Proper mechanism needs to apply to recover the lost packet and in multi-hop WSN, packet should reach the destination to achieve high reliability in data delivery. Most of the applications require each packet should send correctly, i.e., packet level reliability is required. In WSN, most of the protocol provide unidirectional reliable message delivery but some application require bidirectional reliability. Reliability can be measured in terms of hope-by-hope reliability, end-to-end reliability, sensor to sink (upstream reliability), and sink to sensor (Downstream reliability).

Data reliability can be defined in terms of packet reliability and event reliability. Packet reliability refers to the successful transmission of of all the packet to the destination. To achieve the packet reliability, it is required that all packet from sensor nodes must reach to the sink node but due to some interference or noisy communication channel packet are lost, retransmission of that lost packet is required which result in wastage of sensor node energy.

Event reliability refers to the successful detection of the event. It is required that event data from each sensor region needs to reach successfully, but loss of packet can be tolerated as long as sink node receive at least one packet from sensor node [2].

Reliability can be measured as per the direction of flow, i.e., classified as upstream reliability, downstream reliability, and bidirectional reliability. Upstream reliability refers to the unicast or converge cast communication between sensor node and sink node. Downstream reliability refers to the broadcasting communication between sink node and sensor node. Data transmission is broadcasting rather than unicasting, because there is only one sender node, i.e., sink node. Bidirectional reliability refers to the mechanism of two-way transmission of data, one is from sensor to sink node and other is sink to the sensor node. Instead of using two unidirectional protocol, it is important to use single bidirectional protocol because it reduces the heterogeneity of the network as well as complexity. Also it reduces the consumption of energy and one more important use is piggybacking.

For improving the reliability, it is important to identify the loss of data, i.e., loss detection technique needs to apply and the result of this technique need to intimate or notify to take appropriate action to recover from the loss. To perform this task of intimation, various methods are used. In explicit intimation technique, when packet are received at node, it send acknowledgment to the sink node which indicates, when and which packet is received correctly. On the other hand in implicit intimation technique, node understand the successful delivery of packet when it overhear the transmission of packet from neighbor node which node has sent recently. Also node explicitly intimate to the sender about the incorrectly received packet so that sender can retransmit the packet.

Error recovery mechanism in wireless sensor network is classified as end-to-end error recovery and hope-by-hope error recovery. Packet in the wireless sensor network is reached to destination via a number of intermediate node. In end-to-end recovery technique some protocol like TCP, when packet received at intermediate node, without verifying or detecting the loss and requesting for retransmission if lost, packets are sent as it is to the destination. But after receiving at destination, accuracy of packet is checked and if loss is occurred, retransmission request is send, i.e., final destination is responsible for error recovery mechanism. This approach will cause the large delay and low throughput. Some protocols like STCP, ART, RCRT, CTCP, and CRRT offer end-to-end error recovery. In hope-by-hope recovery scheme, loss detection and recovery mechanism are performed at all the intermediate node rather than just the final node. Hope-by-hope loss detection scheme is more energy-efficient scheme than end-to-end approach.

In wireless sensor network root causes of congestions are data rate of sender that is higher than receiver, interference between concurrent data transmission, collision

in the physical channel, addition or removal of sensor node in the node, many-to-one network topology. Traditional protocols such as UDP do not provide the functionality of congestion control mechanism, on the other hand protocol like TCP provide sliding window-based approach to avoid congestion. Main cause of congestion is packet service rate that is greater than the packet arrival rate. And this scenario usually found at sensor node closer to the sink node. Due to congestion in WSN, packet get dropped or delayed because of large and filled queue. Dropping of the packet results in wastage of energy due to retransmission.

Some congestion detection protocols are existing that provide the mechanism of finding the location of congestion, i.e., this mechanism identify whether congestion occurred or not and at which location. As mentioned above in the causes of congestion, lack of memory at sensor node is also cause of congestion. Sensor nodes have a memory limitation, i.e., size of buffer is less and when node receives excessive incoming traffic, buffer cannot hold the excess packet, which result in drop. In WSN, buffer size controls the contention level because when number of source nodes increased, contention level also gets increased.

Packet rate is also one cause of congestion, packet rate defines the number packet sent or received within a specific time interval. At the particular node, the rate of receiving packet is higher than sending packet rate, buffer overflow is possible because the node has limited memory capacity.

After congestion detected at the node, the congested node conveys the congestion occurrence information to the neighbor node, i.e., node in the vicinity of congested node. This information is conveyed using control packet, i.e., it sets congestion notification field (CN Bit) in the header field of control packet. Also it may specify that packet may contain the allowable data rate. The way of intimating the congestion occurrence information is explicit or implicit. In implicit intimation, congestion information is piggybacks in the normal data packet, whereas in explicit intimation, explicit control message can be sent to notify the congestion.

After congestion detected and notified node needs to avoid the congestion. Congestion avoidance can be done by simply stoping the sending packet in the network or send the packet at lower rate. Also dynamic rate adjustment policy is applied where congested node can make the rate adjustment decision and notify to all its neighbor. Rate adjustment can be decide by two ways, centralize or distributed. In centralize policy, decision of rate adjustment is done at the sink node and in distributed it is done at each hope of network. Another method for congestion avoidance is traffic redirection where excessive traffic is redirected via high-speed network or network has long communication range.

3 Literature Review

There are a number of transport layer protocols that are designed for WSN. These protocols are characterized into three different categories.

1. Protocols which provide only reliability
2. Protocols which provide only congestion control mechanism
3. Protocols which provide both reliability and congestion control mechanism.

3.1 Reliability Guarantee Protocols

PSFQ: Pump Slowly Fetch Quickly (PSFQ) protocol.
This protocol works in downstream direction, i.e., from sink node to the sensor node. It uses hope-by-hope error recovery mechanism. The key features of this protocols are low signaling overhead. High error tolerance, scalable, and efficient, finally it is a customizable protocol. It operates in three-step pump operations, fetch operations, and report operations. Working of this protocol is it distributes the data slowly, i.e., pump the packet into network slowly. As it provides hope-by-hope recovery, node can recover quickly from errors. This protocol performs multimodal operation where packet is sent by sink at very low data rate on the other hand intermediate node store and forward at very high data rate. Fetch mode starts when it found any missing sequence number of packet, for that it send NACK. NACK is not propagated beyond 1 hope. It can also send cancel NACK if node overhears same NACK or repair request from other node. At the end sensor report hope-by-hope the delivery acknowledgment to the sink node [3].

RMST: Reliable Multi Segment Transport Protocol
RMST protocol is transport layer protocol and specially designed to provide the reliability in upstream direction, i.e., from sensor to sink node. RMST provides end-to-end data packet transfer reliability. This protocol consists of two mode: caching and noncaching mode. In caching mode, The nodes are assigned as RMST node if they are being used to transfer the data to the sink node. It is selective NACK-based protocol and it is configured for network caching and repair. RMST node caches the fragment and WatchDog timer is maintained. If the fragment is not received before timer expires negative acknowledgment is sent backward in the reinforced path. RMST depends on the directed diffusion scheme for recovery. RMST provides guaranteed end-to-end delivery of all the fragments, but it does not guarantee in-order delivery [4].

3.2 Congestion Control Protocols

CODA: Congestion Detection and Avoidance
It is one of the best algorithm that directly pointing to congestion control and avoidance in wireless sensor network. In CODA three different mechanisms are involved such as congestion detection, open-loop hope-by-hope backpressure notification, and closed-loop multisource traffic control to reduce traffic congestion. In CODA, congestion is detected based upon current buffer occupancy as well as present and past

channel loading. Continuous listening to the channel causes energy consumption so in CODA instead of continuous listening to the channel, it provide sampling scheme which listen the channel when required. When congestion is detected, the node notifies about congestion to its neighbor via backpressure mechanism. This backpressure control packet is propagated toward the source and the nodes, which receives this packet will take action (rate reduction or packet drop) based upon their local congestion status. Also in converge network, i.e., multiple sources are sending data to the single sink node, this protocol employ closed-loop multisource traffic regulation. In this traffic regulation, when source do not get the acknowledgment of data it automatically reduces the transmission rate. Though it is energy-efficient mechanism due to backpressure and ACK scheme, extra energy will be wasted also reduction in transmission rate may result in the quality of service (QOS). Specially in long period of congestion, latency and high data error rate is occurred because of mitigation in the response [5].

3.3 Reliability and Congestion Guarantee Protocols

There are number of protocols in Wireless Sensor Networks for achieving both reliability and congestion control.

[6] **ESRT**: Event to Sink Reliable transport protocol
This protocol offers the reliability at the application level also provides reliable delivery of the packet from sensor node to the sink node, i.e., in upstream direction. ESRT applies regulation on sensor report frequency to achieve desired reliability. This protocol runs on the sink node, because sensor nodes have limited resources, e.g., Power. ESRT is a dynamic state changing protocol which takes action depending upon the current state of network. First, it computes reliability from successfully received packet within a time interval. Based on the reliability, it computes required sensor report frequency. This sensor report frequency is informed to the all sensor nodes. If the reliability at node is less than the required reliability, ESRT increases the sensor report frequency to achieve target reliability also if the reliability is greater than required reliability it reduces the sensor report frequency. This dynamic nature of ESRT is required in random and dynamic topologies of Wireless Sensor Networks.

Drawback of ESRT is it treats all node equally so if congestion in one area of the network, all other nodes have to reduce their data rate as per sensor report frequency message which ultimately affect the network throughput.

[9] **ATP**: Ad hoc Transport Protocol
The core functionality if ATP protocol is rate-based transmission, i.e., it transmits the fixed size of data in each time interval. Unlike TCP it uses the timer to clock the new data, not window-based transmission. For controlling the congestion in the network source node uses the data packet (feedback) from intermediate node to adjust transmission rate. This feedback is piggybacked from receiving node to the sender node. Feedback sends periodically as well as in case of path failure and queuing delay.

If feedback packet is lost, sender waits for certain time period, if it is not received within a epoch time then it multiplicatively reduces the transmission rate also till the end of third epoch if feedback packet is not received, sender sends the probe packet to receiver. Also for achieving the desired reliability, receiver uses selective ACK to report any new holes in the data stream. Based on SACK, sender mark the packet for retransmission and provide high priority than new data packets. advantages of ATP is (1) sending rate estimation is accurate (2) it lowers the data traffic on reverse path (3) Recovery of lost packet at single time. Some issues of this protocols are (1) It need assistance and coordination from the intermediate node (2) It has detect and recover the lost packet very fast.

[10] **STCP**: Sensor Transmission Control Protocol
Sensor transmission control protocol (STCP) is reliable transport layer protocol. This Protocol offers congestion detection and control mechanism as well as Upstream reliability. In SCTP, before actual transmission of data, Sensor node transmit data packet called session initiation packet which contain the Transmission Rate, Type of data, Expected reliability and number of currently running transmission and receiving activity. When this packet is received at receiver (sink) end, Receiver (sink) send the acknowledgement (ACK) to the source sensor node. Then source node start transmitting the data. As the sink node knows the transmission rate from source node, it estimate the arrival time of data packets. If packet do not received within an estimated time it sends negative acknowledgement. Also as expected Reliability is provided to the sink in session initiation packet, Sink node measure the reliability in terms of number of packet received successfully. It offers end-to-end reliability. SCTP has a functionality of congestion detection by analyzing the size of buffer. To avoid the congestion at sink node it provide mechanism of setting the congestion bit in ACK packet. If sink node face the problem of buffer overflow it intimate to the source node by sending ACK packet in which congestion bit is set. To Reduce the congestion it offers the traffic redirection scheme as well as end-to-end rate adjustment mechanism.

[12] **CRRT**: Congestion-Aware and Rate-Controlled Reliable Transport
CRRT is reliable and congestion control protocol for WSN. It offers the hope-by-hope as well as end-to-end reliability in upstream direction, i.e., from sensor to the Sink node. In CRRT, for increasing the hope-by-hope reliability it provided the efficient retransmission mechanism. For retransmission of dropped data it employ reservation based mechanism where sender reserve the transmission medium. It uses the PACK and NACK to achieve the desired reliability. Congestion detection is simply carried out by analyzing the buffer size as well as the transmission rate of the node. For reducing the congestion, congested node send the Control packet containing the information (Buffer Memory occupancy) about congestion so that source node automatically reduce their data transfer rate.

[13] **CTCP**: Collaborative Transport control Packet
CTCP is a transport layer protocol which offers both the functionalities, reliable of data transmission and congestion detection and avoidance mechanism. CTCP provide end-to-end reliability in upstream direction, i.e., from sensor node to the sink

node. Efficiency of this protocol is measured in terms of the packet delivery ratio and energy consumption of the network. Data delivery ratio is fraction of number of packet received to the number of packet sent and Energy consumption of Network is the sum of energy consumption of individual sensor node. Congestion detection scheme is based on analysis of buffer occupancy and error rate. To reduce the congestion, sink node sends explicit acknowledgement for reducing the transfer rate. The key features of protocol is reliable delivery of all transmitted packet source to sink node and energy efficiency, it is also capable to identify error loss.

3.4 Congestion Control with Decentralized Parameters

[14] **PORT**: Price-Oriented Reliable Transport protocol
This transport layer protocol offers the Reliability in upstream direction, energy efficiency and congestion control mechanism. In PORT, It defines the price of node which is measured as total number of transmission attempt between sensor node and sink in the network. It avoid the links which have high communication cost which causes reduction in energy consumption. PORT provide application based optimization approach to the sink node so that sink can send the optimal reporting rate of each source and energy consumption of communication (sensor to sink) as a feedback. Also for informing congestion and increase the node cost it provide optimal routing scheme based on feedbacks from source node to the sink node. Above mentioned two offers will reduce the consumption of energy across the network. Congestion detection scheme is based on two parameters, node price and link loss rate. To reduce the congestion it uses the traffic redirection scheme as well as rate adjustment mechanism.

[15] **ART**: Asymmetric and Reliable Transport
ART is transport layer protocol which offers upstream end-to-end event reliability, downstream end-to-end query reliability and upstream congestion control. The major functionalities of ART are reliable event and query transfer and distributed congestion control. From the network, ART select nodes either essential node (E node)or nonessential node (N node). Essential nodes are those who take part in reliable data transfer between sink node and sensor node in both direction, i.e., upstream and downstream. To achieve the reliable data transfer in both direction it uses ACK and NACK mechanism. It has four characteristic (1) nonessential do not take part in end-to-end communication (2) congestion method is decentralized to regulate the data traffic effectively. (3) Only few nodes can participate in the recovery from lost message. (4) It uses distributed energy aware congestion control. Drawback of ART protocol is. It provide reliability guarantee for essential node only and not for nonessential node.

[16] **RCRT**: Rate-Controlled Reliable Transport
It is Transport layer protocol which offers the upstream reliability, i.e., it provide reliable transmission of sensor data from sensor node to the sink node. It Guaran-

tee about reliable transmission of data based on NACK scheme. In NACK scheme, sink request for missing packet to the sensor node so whenever data will be reached it is 100 % correct. RCRT implemented three regulation at sink node, (1) Congestion detection scheme (2) Rate Adaptation (3) Rate Allocation. Congestion detection scheme is based on the Round Trip Time (RTT). In Rate Adaptation regulation, Every node can dynamically change the data transfer rate, i.e., if congestion is in the network it will decrease the transfer rate and increase when congestion is not there. In Rate Allocation regulation, Depending on the application requirement data transfer rate will be allocated. This protocol provide end-to-end loss recovery. Main goal of this protocols are (1) Reliable end-to-end data transmission (2) Avoid the collapse of the network due to congestion (3) Application oriented data transfer rate allocation scheme (4) Support for the dynamic environment.

[17] **RTMC**: Reliable transport with memory consideration
It is reliable transport layer protocol which offers hope-by-hope data transmission policy and congestion control mechanism. Rate adjustment scheme is also used to reduce the congestion but it is possibility of drop of control packet which contain the information of rate adjustment. This protocol efficiently reduce the congestion by sending the memory occupancy information. This protocol include memory information field in the header of the packet. This causes all sender get the information of memory occupancy of receiver so accordingly sender adjust their transmission speed or rate. This protocol improve the throughput of the network as well as energy efficient, i.e., reduce the consumption of energy.

3.5 Congestion Elimination Protocols for Urgent Data

Majorly Buffer occupancy notification and rate adjustment scheme are used for the congestion control. But it may be possible that In case of emergency situation large amount of traffic is injected into the network in very short amount of time and it is required to get the information of the event quickly. There are number of protocols are designed for communication and avoid the congestion control in wireless sensor network but there are few of them which offers the transmission of urgent data.

[18] **RETP-UI**: Reliable Transmission Protocol for Urgent information
This protocol categorized traffic into three different types and for each kind it maintain different queue. Congestion in the network is predicted accurately based upon the queue length and its fluctuation. This protocol provide high throughput, less delay and probability of loss of packet is very less.

[23] **Fast and Reliable Transmission mechanism for urgent information in sensor network**
This is reliable transport layer protocol for urgent data transmission. In case of any emergency data transmission, node will establish the alive connection between source node to the sink node. All nodes which are part of live connection keep awake all the time for transmission of the data as well as it refrain from emission of normal

Table 1 Comparative analysis of congestion elimination protocols for urgent data in wsn

Protocol name	Congestion detection	Congestion avoidances	Reliability level	Reliability type	Reliability direction	Acknowledge
RETP-UI	Queue occupancy fluctuation	Multistage rate adjustment	Event	H-B-H	Upstream	ACK
CP EDCA	Emergency detection	Normal data preemption	Event	H-B-H	Upstream	ACK
ADMQOS	Event detection	Priority wise categorization	Event	H-B-H	Upstream	ACK
OD AODV	Event classification	Priority wise shortest path	Event	H-B-H	Upstream	ACK
FMUMUWSN	Event classification	Multistage path	Event	H-B-H	Upstream	ACK
PAT	Urgent event	Blocking of normal data	Event	H-B-H	Upstream	ACK

packet, i.e., it neglect the transmission of normal packet until all emergency packet are not delivered. This protocol also added retransmission mechanism of lost emergency packet on priority basis. In implementation they showed the alive connection can be established very quickly and emergency data is transferred with accuracy. This protocol achieve efficient Urgent data transfer to the sink node with 92 % of packet delivery ratio and less than 92 ms delay. Congestion is eliminated by reducing or neglecting the data transmission of normal packet.

[20] **CP-EDCA**: Channel Preemptive EDCA
This reliable transport layer protocol is designed for the transmission of the urgent data. Working of this protocol is urgent data traffic is preempt the services of regular data routine traffic. This protocol guarantee the QoS of the emergency data. Simulation result of emergency data transmission shows that 50–60 % decrement in the MAC layer delays. This advantage Preemption strategy it to expand from 802.11e standard to distributed emergency reporting.

[24] **PAT**: Path Assured Data Transfer Protocol
This protocol operates three steps. In the first step emergency data node initiate the blocking request to the other node to block their normal data transmission. Due to blocking mechanism path will get cleared. In the second step, Urgent data is transferred to the sink or master node and acknowledgement is received for the same. When data transmission of urgent data completed,Sink node or Master node will send the release message. This dedicated path for a moment will guarantee collision free data transmission and reduce the delays due to retransmission of data (Tables 1 and 2).

Table 2 Comparative analysis of congestion detection and avoiding protocols

Protocol name	Congestion detection	Congestion mitigation	Reliability level	Reliability direction	Reliability type	Acknowledge	Delay	Congestion notification
PSFQ	Packet level rate	–	Packet level	Downstream	H-B-H	NACK	Medium	Implicit
RMST	Packet level rate	–	Packet level	Upstream	H-B-H	NACK	–	Implicit
CODA	Packet level rate, Queue occupancy	Rate adjustment	–	Downstream	H-B-H	–	Small	Implicit
ESRT	Queue occupancy	Rate adjustment	Event Level	Upstream	Evt to sink	–	Large	Implicit
ATP	Queue occupancy	Rate adjustment	Packet level	Upstream	EtoE	NACK	Medium	Explicit
STCP	Queue occupancy	Rate adjustment, traffic redirection	Packet level	Upstream	EtoE	NACK, Eack	Large	Implicit
CRRT	memory overflow	Rate adjustment	Packet level	Upstream	H-B-H	–	Large	Implicit
CTCP	queue transmission error loss	Rate adjustment	Packet level	Upstream	E to E	eack, Double ack	Medium	Explicit
PORT	Node price, link loss rate	Rate adjustment	Event Level	Upstream	–	–	–	Implicit
ART	ack to core node, link loss reduce	Reduce traffic non core node	Packet level	Both	E toE	NACK	Small	Implicit

(continued)

Table 2 (continued)

Protocol name	Congestion detection	Congestion mitigation	Reliability level	Reliability direction	Reliability type	Acknowledge	Delay	Congestion notification
RCRT	Time to receive loss	Rate adjustment	Packet level	Upstream	E to E	NACK	–	Implicit
RTMC	Memory overflow	Header memory info	Packet level	Upstream	H-B-H	–	Large	Implicit
FLUSH	Ack to core node, link loss reduce	Rate adjustment	Packet level	Upstream	E to E	NACK	Small	Implicit

4 Proposed System

For Urgent data transmission there are number of protocol are designed. In Path assured data transmission protocol, Sensor node send request for transmission of urgent data to the sink node. Sink node block all other transmission of normal packet by sending the blocking request. Existing systems for Urgent data transmission mainly focused on the only transmission of urgent data. Proposed scheme aims not only transmission of urgent data packet but also the normal data packet at the same time. In existing PAT scheme, while transmission of urgent data (sensitive) from sink node to sensor node, all the normal data traffic get blocked to avoid the congestion and provide 100 % reliability for urgent data but at the same time normal data is generated at other sensor node and due to blocking request from sink node, sensor node do not send the data in the network even if the urgent data transmission is not in the vicinity. And which result in normal data packet generated at sensor node could not store at node due to Less memory. In the proposed scheme, this issue is resolved by using intelligence (Fig. 1).

It works in three phases, when sensor node has urgent data information, it send UREQ (urgent data request) to the sink node. This request will reach to the sink node via number of hops. The intermediates node will add their ID information to the request packet. When sink node receive the request packet, It immediately broadcast the blocking request which contain the ID information of intermediate node which

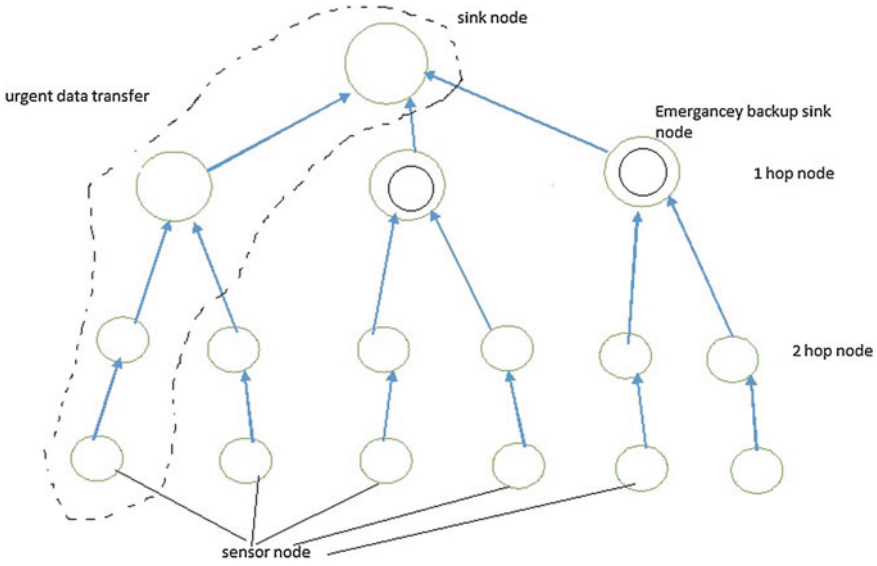

Fig. 1 Proposed system

received in request packet. When all other nodes will receive the blocking request it compare its all neighbor ID and all ID contained in blocking request. If it found any neighbor ID in the blocking request ID list then it will block the normal data traffic and if not then it will forward the traffic toward the sink node. Also when Sink node broadcast the blocking request, immediately its one hope neighbor node send the status information, i.e., currently available power, buffer occupancy to the sink node. When this information contained packet received at sink node, it will select one of them as a backup sink node and broadcast (BUPSINK) request so that all other normal data generator node transfer data to the backup sink node and urgent data is transmitted to the original sink node. Finally when urgent data transmission is completed then original sink node will broadcast the block release (BRELEASE) request. When this request is received at backup sink node, it will start sending normal data which is aggregated from normal data generator node.

5 Conclusion

In this paper, we described comparative study of many existing reliable, congestion detection and avoidance and urgent data transmission protocols in wireless sensor network. This paper describe the problems and limitations of existing transport layer protocols. We have studied and examined various requirements and some design issues of transport layer protocols. This survey of existing protocol directed us to problem in Urgent or Sensitive Data transmission protocols. Though lot of research work has been done in transmission of data in WSN but all research work assume that all data in WSN is of same type which means in the network all data is treated equally. So for sensitive or urgent data transmission, some researcher implemented reliable and congestion-free protocols. These protocol are very costly in terms of computation and energy perspective. Also in PAT protocol mechanism, We addressed problem of transmission of normal data packed during transmission of Urgent data. Our proposed system presented in this paper eliminate the problem of currently existing PAT protocol and provide efficient transmission of urgent data and normal data in intelligent manner.

References

1. Khemapech, et al., “A survey of wireless sensor networks technology,” in 6th Annual Post graduate 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.
3. 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.
4. 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.

5. S. B. E. a. A. T. C. C.-Y. Wan, "CODA: Congestion detection and avoidance in sensor networks," in Proceedings of ACM Sensys03, November 5–7, 2003.
6. K. S. C. Wang, and B. Li, "SenTCP: A hop-by-hop congestion control protocol for wireless sensor networks," in Proceedings of IEEE INFOCOM2005 (PosterPaper), Mar. 2005.
7. K. S. C. Wang, V. Lawrence, B. Li, and Y. Hu,"Priority-based congestion control in wireless sensor networks," in Proc. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing(SUTC06), pp. 2231.
8. O. B. A. Y. Sankarasubramaniam, and I. F. Akyidiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks," in Proceedings of ACMMobihoc03, June 1–3, 2003.
9. V. A. K. Sundaresan, H. Y. Hseeh, and R. Sivakumar, "ATP: a reliable transport protocol for ad-hoc networks," in Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc03), pp. 6475.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. N. T. a. W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," International Journal of Sensor Networks, vol. 2, pp. 188–200, 2007.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. A. W. R. A D Karanjawane, S D Mali, A A Agarkar,"Designing Path Assured Data Transfer Protocol for Wireless Sensor Network,"In proceeding of International Journal of Engineering Research and Technology (IJERT), vol. 2, pp. 1151–1160, 2013.