Reliable Transport of Data in Wireless Sensor Network

M. Kosanović, M. Stojčev

Abstract: Reliable transport of data in Wireless Sensor Networks (WSN) has become a big challenging issue for researcher community in the last few years. WSNs are currently deployed in a wide range of applications as a sensor is becoming smaller and production cost is smaller.

In this paper, we look at the problem of efficient and reliable data transport in WSN. We propose a suitable solution for information delivery in both directions, in upstream (from sensor node to master node – sink) and in downstream (form master node to sensor node). Our proposal ensures a reliable data transport in both directions, with reduced traffic between sensor nodes and sink.

I. INTRODUCTION

Wireless Sensor Networks, WSNs, are large networks composed of small sensor nodes, SNs, with limited computer resources capable for gathering, data processing and communicating [1]. WSNs are cost effective and distributed solutions implemented in various environments where conventional networks are impractical. Unlike traditional wired networks, the reliability of data transfer in WSNs is not a critical parameter. Namely, for most WSNs (monitoring environment, object tracking, etc.) some occasional amount of data losses is acceptable. However, as WSNs become ubiquitously deployed, such as multimedia and process control WSNs, reliable data transfer, RDT, is required. In this kind of applications every byte of the data packet has to be, reliable delivered to the destination. In general, in such networks more data are transferring. This implies that more conflict in traffic, more congestion in accesses, and more packet retransmissions among SNs are needed. As a result, the SN`s power consumption increases, while its life period becomes shorter. Having in mind that the TCP/IP protocol suite becomes de-facto worldwide standard in network connectivity, it is quite reasonable to look at some efficient methods for reliable data transfer in WSNs based on the TCP/IP concept. This problem is in focus of our interest. The main idea is based on grouping SNs into small entities called clusters. All SNs are dynamically addressable and controlled by the master node, MN. Dynamic multi-addressing capability allows us to decrease both the frame length and traffic intensity, and increase data transfer reliability.

Mirko R. Kosanović is with the High Technical School, Aleksandra Medvedeva 20, 18000 Niš, Serbia,
E-mail: vkosanovic@sbb.co.yu

Mile K. Stojčev is with the Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Niš, Serbia,
E-mail: stojcev@elfak.ni.ac.yu

II. SPECIFICATIONS OF RELIABLE DATA TRANSFER IN WSNS

The main factors that affect the RDT in WSNs are the following:

1. *Initial connecting process* – Most of the applications in WSNs are of reactive type. SNs passively monitor the environment and wait for events occurring before reporting to the MN. It is therefore necessary to make a efficient connecting process in order to inform the MN about of SN`s status (level of power consumption, level reliability of gathered data, transmitter rate and addresses of sensor nodes). According to the status of parameters, the MS selects an optimal trace route [2].
2. *Congestion control mechanism* – it includes the following congestion activities: detection, avoidance and correction.
3. *Rate of reliable data transfer* – Sometimes, WSN need to receive data packets correctly from a certain area, only, but not from every SNs in this area. So, the ratio of successful in respect to a total SN`s data transfer is defined.
4. *Reduced number of retransmissions* - the transport protocol should implement a mechanism for packets loss recovery such as NACK, ACK, selective ACK or selective NACK. Concerning mechanisms designed for reducing the number of retransmissions, it is better to use NACK instead of ACK message in hop-by-hop, HBH, networks, such as WSNs [3].
5. *Reduced length of frame header* – in WSNs, contrary to TCP/IP based networks, the ratio between the payload and header length is small.So, during a design of WSN`s protocol the primary goal is to reduce the header length.
6. *Equal treatment of sensor nodes* – in a communication traffic it is desirable for all SNs in WSNs to participate equally. Therefore, the balanced energy consumption for all SNs is imperative to achieve.
7. *Cross layer optimization* – communications between two neighboring protocol layers have to be short and efficient. For example, if the routing protocol signals to the transport protocol that some route failure occur, the transport protocol knows that the packet is loosed because of route failure and therefore freezes the sender status.

III. RELATED WORK

Standard transport layer protocols, such as TCP and UDP, are not suitable for severely resource constrained

978-1-4244-1882-4/08/$25.00 © 2008 IEEE

WSNs [4]. Numerous reliable data transport protocols for WSNs, with limited number of resources, are developed (see fig.1) [3]. In general, most of the proposals are application-oriented i.e., application–specific. Mainly, the protocols given on the right part of Fig.1, are intended to solve the problems related to congestion control and/or reliable data transfer in upstream and downstream directions. WSN`s transport protocols that pool congestion control and reliable bidirectional data transfer are in focus of interest in the last decade [3]. An efficient reliable data transfer protocol is described in this paper. In order to put more light to the considered problematic we will give now, a short review of the most popular reliable data transport protocols implemented in WSNs.

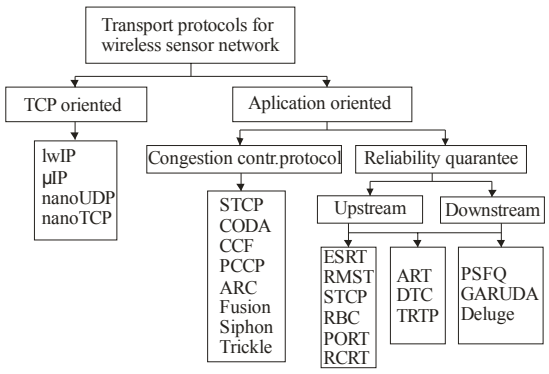

Fig. 1. Current transport protocols in WSNs

PSFQ (*Pump Slowly, Fetch Quickly*) – It is designed to be scalable and energy efficient, trying to minimize the number of signaling messages and relying on multiple local timers. It addresses reliable communication from MS to SNs (*downstream*). The main idea is to send packets from the MS to SNs at low speed in order to give time to the SNs to recover any missing frame before the next frame arrives. Data losses are detected as a gap in a sequence numbering of the received frames, and the frame recovery takes place HBH by aggressively asking for retransmissions via NACK messages [5].

GARUDA – This protocol is scalable in respect to the network size, message properties, loss rate, and reliability semantics. GARUDA is designed to be operational in networks composed of SNs located at fixed locations. It solves the problem of reliable transport by transmitting a high-energy pulse, called WFP (Wait-for First-Packet), before transmitting the first packet. This pulse is almost immune to channel loss, and either idle SNs or sensors already receiving a data packet can hear it. Pulse characteristics are different from data packets, with make possible to receive it, and the data packet at the same time without interference problems [6].

ART (Asymmetric and Reliable Transport) – addresses the reliability both in upstream and downstream directions. This is an event-based protocol that does not need to offer reliability at message level. In the upstream direction, ART assumes that the information from nearby SNs will be highly correlated, and proposes a scheme for event reliability. Consequently, it is not necessary to transport reliable all packets generated by SNs from event region. In opposite direction, it guaranties reliable messages reception from a subgroup of SNs that cover the entire area of interest, but not all located SNs in that area [7].

RMST (*Reliable Multi-Segment Transport*) – the goal of this protocol is to achieve reliable data transport from SNs to MN i.e. upstream direction. It works on top of the multicast diffusion routing protocol (Directed diffusion) [11]. If the packet does not arrive at MN, it is recognized by timer expiration, which the packet requires by a NACK. The protocol is suitable for receiving continuous data streams but not for event based streams [8].

ESRT (*Event to Sink Reliable Transport*) – it grants that some random event which occurs in the deployment WSN`s region should be accurately registered. ESRT takes profit of the information redundancy from packets coming from nearby SNs. Reliable transmission of all of packets is not necessary. Only a minimum number of packets that deliver to the MN, is a necessary information. It does not use node IDs but event IDs. ESRT supports congestion detection based on the queue level of the SNs also. When a SN recognizes congestion it informs the MN by setting the specified bit into a packet, and on this way MN can reduces SN`s report frequency [9].

IV. Architectural Model

Note, that limited hardware and software resources characterize SNs. When we start to develop a reliable SN`s data transport protocol, the first thing what we have in mind is that it has to be *energy-aware* and simple. Further, we assume that this protocol has to be bidirectional and to guarantee reliable data transport both in upstream and downstream directions. This is necessary because the quantity of data that SNs exchange is growing from day to day (multimedia data, program code). Next, we assume that, to each SN, during the init process, a unique address within the WSN is assigned. The idea of our proposal is to provide a multi-addressing capability for each SN in the WSN, also. By using this approach, we omit the sequence-numbering field in a header. In this manner, we reduce the message length for one or two bytes (what corresponds to the length of a sequence-number field). During the data transfer process, a multi-address assignment to each SN allows us to keep track of message sequence numbering. The multi-address is in correlation with the sequential frame numbering of a single message. The address assignment process is a responsibility of the MN. From Internet point of view, the master acts as a DHCP server (Dynamic Host Configuration Protocol),which dynamically assigns addresses to SNs within the WSN. To each SN 2^n, $0 \leq n \leq 8$, addresses can be assigned. The number of assigned addresses depends on reliability level, type of data

(temperature sensor- generates small amount, multimedia system - large amount), traffic direction (upstream or downstream), and traffic congestion (more congestions less number of addresses, and vice versa). In downstream, the MN all address assigns to SNs. In upstream, a single address to each SN is assigned. In this case, the rest of the addresses are assigned to the MN. This is reason why we have one or two bytes less in the header, i.e., it is not necessary to send a frame sequence number. All frames behave now as a single message, and are sending independently. The assigned multi-address determines the number of frames/messages that this SN can receive in one block. The sender node divides the message into several data blocks. Each block consists of identical number of frames/messages. This implies that message arrival ordering, within a block, can be arbitrary, i.e., all messages in one block have a unique address. This allows us to use any of the well-known WSN`s routing protocols [11].

Figure.1. shows a scenario which corresponds to the delivering of a single message to the multi-addressed SN (four addresses). The total message is divided into two blocks. Each block consists of four frames/messages with a different destination address. When the destination SN receives all frames of one block, it sends the ACK message in order to inform all nodes in a multi-hop route that the message has been received without error. After that, the sending procedure can be repeated. If some of a message is corrupted, a NACK message is returned among neighborhood SNs. A manipulation with NACK messages is similar as in PSFQ [5]. This means that the propagation of the corrupted data is limited between two intermediate SNs, only, and consequently the amount of retransmissions is decreased.

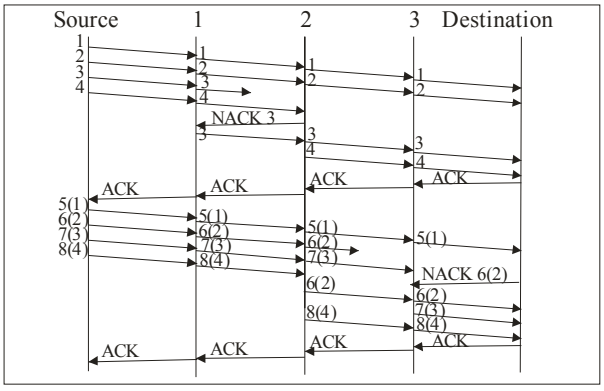

Fig. 2. Transport sequence of frames among SNs in WSN

V. Protocol Design

Three different types of messages in the proposed protocol are involved:`initial,data,and control`.

A. Initial messages

Two types of initial messages, IM1 and IM2, in term of data transfer direction we distinguish (see Fig.3):

Type	Message content							Direction
IM1	MT	DA	SA	INF	TR	RE	ECS	Upstream
IM2	MT	DA	SA	DA1	DA2	INF	ECS	Downstr.
DM	MT	DA	SA	INF	ECS			Up/Down
CM1	MT	DAn	SA	ECS				Up/Down
CM2	MT	DA	SAn	ECS				Up/Down
CM3	MT	DA1	DA2	SA	ECS			Downstr.

Fig. 3. Format of messages

Where are: MT- message type, DA – destination address, SA–source address, INF–information field (variable length), TR–data transmission rate, RE–level of reliability, DA1–first enumerated address of the multi-address , DA2 – last enumerated address of multi-address, ECS – error correction sum. The fields MT, DA, SA, TR, RE, DA1, DA2, and ECS are of single byte length.

B. Data messages

Data message (DM) is identical for both upstream and downstream (see Fig.3).

C. Control messages

Its task is to provide a mechanism for reliable data transfer among SNs. We use two types of control messages: a positive-acknowledge, ACK, and a negative-acknowledge, NACK. The NACK control message CM1 (see Fig.3) is used for HBH among intermediated nodes, while ACK is intended for end-to-end, i.e. source→destination, loss detection and recovery. ACK and NACK messages guaranty reliable data transfer. Two types of ACK control messages exist:

a) CM2 – the destination SN confirms correct reception;

b) CM3 - MN sends address range to the SNs.

The content of MT field is the following:

a) TD(traffic direction) - a single-bit subfield, TD=0 upstream, TD=1 downstream.

b) TM_i(type of massage) – binary coded three bits subfield, it denotes the type of control messages. There are possibility for eight different type of messages.

c) EA_i(extended address) – a binary coded four bits subfield, used for extending SNs address range. It defines the number of hopes between the MN and the addressed sensor. For example, it is possible to configure 256 different addresses in WSN with 16 hops, 512 different addresses with 8 hops, or 1024 with 4.

VI. Performance Analysis

The crucial idea of our approach is to decrease the header length. Namely, our frames do not specify a frame's sequence number, i.e., each frame in a packet has a unique destination address. In order to evaluate the performance of the proposal we will consider its

coefficient of efficiency, $\phi(b)$. $\phi(b)$ is defined as a ratio of Ss - Sn and *S*n,

$$\phi(b) = \frac{Ss - Sn}{Sn}$$

where: Ss– message length in bytes defined in [12] ,[13]; Sn– message length in bytes in our proposal

Further we assume that the WSN is operative in ideal conditions, i.e., without message retransmissions. Now, for both message lengths, we determine the total number of bytes that are sent from the source node to the destination one.

$Ss=(d_h+ d_p)* b + (d_h+ d_p) * b * n_1 + (d_h+ d_p) * b * n_2 + ...$

$Sn= (d_h+ d_p-1) +(d_h+d_p-1)*n_1 +(d_h+ d_p-1)*n_2 + ...$
$+(d_h+ d_p-1)*b +(d_h+d_p-1)*b*n_1 +(d_h+ d_p-1)*b*n_2 + ...$

where: p - total message length in bytes; d_h - *header* length; d_p - *payload* length; d - frame length , i.e., $(d_h+ d_p)$; n_i - number of sensor nodes active in one hop; and $b = p/d_p$ - number of frames in a single message;

Accordingly, for $\phi(b)$, we obtain

$$\phi(b) = \frac{Ss - Sn}{Sn} = \frac{(dh + dp)\,b - (dh + dp - 1)\,(b+1)}{(dh + dp - 1)\,(b+1)}$$

$$\phi(b) = \frac{db - (d-1)(b+1)}{(d-1)\,(b+1)} = \frac{b+1-d}{bd + d - (b+1)} \qquad (1)$$

In order to achieve better performance in respect to [12] a condition $\phi(b) > 0$ has to be fulfilled**.** This means that:

$$b > d - 1. \qquad (2)$$

According to the eq.(2) we conclude that the number of frames, b**,** have to be larger in respect to the frame length, d. For $b \leq d$ (this case corresponds to sending of small length messages) our proposal has lower performance. The condition defined by (2) can be easily fulfilled, since both the limited number of SN's hardware & software recourses and small frame lengths (from 16 up to 35 bytes for TinyOS Messages), are typical features of the WSNs [13].

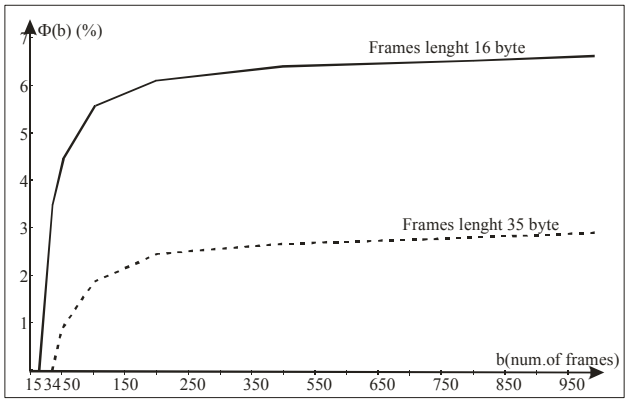

Fig.4 Coefficient of efficiency in dependence of number of frames

In Fig. 4. the coefficient of efficiency, $\phi(b)$, given in percents, in term of b**,** is given. As can be seen from Fig. 4, when the frame length is 35 byte long, the efficiency is approximately 2-3 %, but if we reduce the frame length to 16 bytes, $\phi(b)$ becomes larger and is within the range of 5-7 %.

VII. Conclusion

In this paper, we introduce an efficient WSN transport protocol. It provides reliable communication for both upstream and downstream data transfer direction. We involve the idea of multi-addressing for single-sensor node. On this way, we reduce the frame length, since the frame sequence number in header is omitted. Consequently, each frame represents now a single message. In addition, large SN's memory buffers are not needed, what is especially critical in a hop-by-hop scheme of data communication. By applying our proposal, the SN's power consumption can be improved, too. Finally, we achieve a reliable and selective E2E data transfer.

References

[1] I.F.Akyildiz, T.Melodia, K.R.Chowdhury,''A survey on wireless multimedia sensor networks'', Computer Network (2006), doi:10.1016/j.comnet. 2006.10.002

[2] C.Wang, M.Daneshmand, B.Li, K.Sohraby, ''A Survey of Transport Control Protocols for Wireless Sensor Networks'', IEEE Network Magazine, Special Issue on WSN, 20(3):34-40,2006

[3] C.Wang, K.Sohraby, B.Li, W.Tang, ''Issues of Transport Control Protocols for Wireless Sensor Networks'',

[4] A.Dunkels, ''Towards TCP/IP for Wireless Sensor Networks'', Malardalen University Licentiate Thesis No.45, Swedish Institute of Computer Science, March 2005.

[5] C.Y.Wan, A.T.Campbell, ''PSFQ: A reliable Transport Protocol for WSN'', Proceedings of ACM WSN '02, September 2002, Atlanta, USA

[6] S.J.Park, R.Vedantham, R..Sivakumar, I.F.Akyildiz, ''A scalable approach for reliable downstream data delivery in WSN'', Proceedings of ACM MobiHoc '04, May 2004, Roppongi, Japan

[7] N.Tezcan, W.Wang, ''ART: An Asymmetric and Reliable Transport Mechanism for Wireless Sensor Networks'', Int.Journal of Sensor Networks, 2006

[8] F.Stann, J.Heidemann, ''RMST: Reliable Data Transport in Sensor Networks'', Proceedings of IEEE SNPA '03, May 2003, Anchorage, USA

[9] Y.Sankarasubramaniam, O.B.Akan, I.F.Akyildiz, ''ESRT: Event-to-sink reliable transport in WSN'', Proceedings of ACM Mobihoc '03, June 2003, Annapolis , USA

[10] C.Y.Wan, S.B.Eisenman, A.T.Campbell, ''CODA: Congestion detection and avoidance in sensor networks'', in: Proceedings of ACM Sensys '03, November 2003, Los Angeles, USA

[11] K.Akkaya, M.Younis, ''A Survey on Routing Protocols for WSN'',www.ece.gatech.edu/research/labs/bwn/ee8863/supplements/routing1.pdf (10.10.2007)

[12] J.Jones, M.Atiquzzaman, ''Transport Protocols for WSN: State-of-the-Art and Future Directions'', International Journal of Distributed Sensor Networks,3:119-133, 2007

[13] Jeff Thorn, ''Deciphering TinyOS Serial Packets'', Octave Tech Brief #5-01, March 2005