Poster Abstract: Meeting the Evolving Reliability Requirements for WSN Applications

Faisal Karim Shaikh, Abdelmajid Khelil and Neeraj Suri
Department of Computer Science,
Technische Universität Darmstadt, Germany
{fkarim,khelil,suri}@informatik.tu-darmstadt.de

***Abstract*— Data transport (DT) is a core function for Wireless Sensor Networks (WSNs) with different applications running on the same WSN, and having varied requirements on the reliability of data delivery. Furthermore, application requirements may evolve over time. Given that the DT reliability is a function of the continuously changing network properties and protocol parameters, a framework for online adaptation of DT reliability is a major contribution to meet the evolving application requirements for different network conditions. In this poster we sketch a novel approach that relies on the Reliability Block Diagrams to realize such a framework.**

I. Introduction

Wireless Sensor Networks (WSNs) constitute a rapidly growing research area covering both a wide variety of devices and applications. Typical applications involve tracking or monitoring as (a) either statically as embedded sensors or (b) dynamically as mobile (semi-) autonomous entities. Empirically the core function for a WSN is to collect data from the environment and transport it to a gateway node termed as *sink*. The general data collection and dissemination process involves the flow of the *raw data* from source nodes towards the sink.

A WSN may be designed for different missions, i.e., different applications can run on the same WSN. A WSN deployed for fire detection in a forest can also be utilized for other tasks, such as measuring the humidity in forest. The application requires the fire to be detected and reported with high reliability whereas the delivery reliability required to measure the humidity may be relatively low. Clearly, the different applications have different requirements on the reliability of *Data Transport* (DT). In addition, the requirements of the same application may evolve in time, for example if the mission of the WSN changes. Considering the above example, after the detection of fire and notifying the user, the (fire detection) application should stop reporting the fire and continue reporting the perimeter of the fire field. As the applications main task, reporting the fire detection, is accomplished, the delivery reliability of the perimeter of the fire may be tolerable.

Furthermore, the WSN is obviously subject to a wide range of computing and communication level perturbations, changing the WSN properties over time which affects the reliability of DT. For example, the number of nodes in WSN are changing due to node crashes and new node deployments. The link quality may vary over time due to variable network load or environmental conditions. To overcome the changing properties of WSN, the DT protocols use different parameters such as retransmissions, number of nodes detecting the phenomenon etc.

The problem becomes of how to tune the DT protocol parameters to adapt to both the evolving application requirements and network properties. Most of existing effort for protocol adaptation focus on tolerating the changes in network properties and not on application requirements [1]. In [2] a generic adaptation architecture is defined, which is unfortunately valid only for a specific class of applications, i.e., for code update. The above works show how adaptation is beneficial in dynamic and erratic WSNs and serve as a basis to introduce adaptive behavior into these multifaceted systems.

We use Reliability Block Diagram (RBD) to analytically express the delivery reliability [3]. Section II presents briefly how reliability of DT is modeled using RBD. Using these RBD's sensor nodes are aware of inverse functions and can adapt the DT parameters online to achieve the desired reliability of application over time. Section III details the proposed online adaptation mechanism for evolving needs of WSN applications.

II. Modeling the Reliability of Data Transport

We define DT in WSNs as a set of operations carried out on raw data from its generation till the phenomenon is reported to the sink. The decomposition of the data transport into operations simplifies the computation of the overall reliability. The reliability of data transport depends on the reliability of each operation. If one of the operation fails, then the overall data transport fails. We model these operations by means of RBD [3].

To understand the concept of online adaptation in Section III let us consider a representative DT protocol, Reliable Multi-Segment Transport (RMST) [4]. Operations for DT from the source to the sink in RMST are *routing* and *Message Loss Detection (MLD)*. MLD is used for retransmission of missing messages. For reliable delivery in RMST, a missing message is detected by Selective Negative Acknowledgment mechanism and is retransmitted by the node. The failure of one retransmission does not result in the failure of overall data transport. This effect is shown as parallel RBD blocks for RMST in Figure 1.

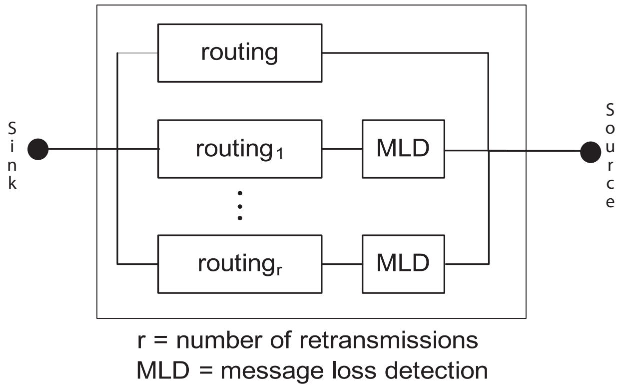

Fig. 1. Reliability Block Diagram for RMST

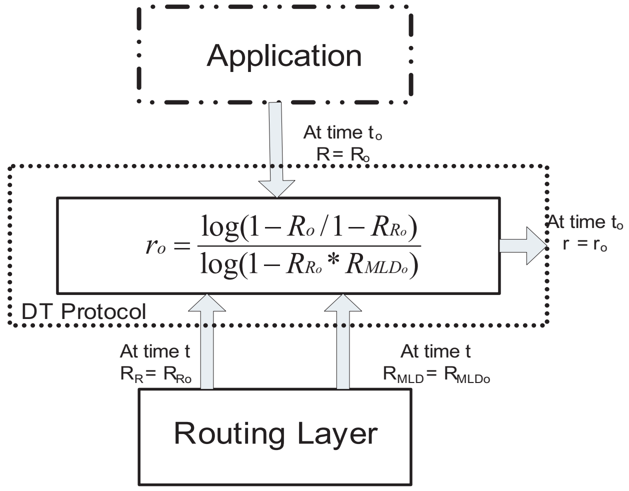

Fig. 2. Online adaptation for RMST

Using Figure 1, the reliability of RMST R is calculated as follows:

$$R = 1 - \{(1 - R_R) * (1 - (R_R * R_{MLD}))^r\} \qquad (1)$$

where R_R is the routing reliability, R_{MLD} the reliability of MLD and r is number of retransmissions. R_R and R_{MLD} depend upon WSN properties, i.e., number of nodes, network conditions etc. The DT protocol parameter r plays an important role in the reliability of the data transport.

III. Online Adaptation for DT Reliability

The reliability of a DT protocol is a function of (a) WSN properties and (b) protocol parameters. Unlike the protocol parameters, WSN properties are difficult to control in time. In most of the application scenarios it is difficult to redeploy the new nodes, or to avoid crashing of nodes due to energy depletion. On the other hand protocol parameters can be tuned, provided the adaptation mechanisms are available. The RBD establishes a relationship between WSN properties, protocol parameters and the reliability. Protocol designers can utilize this relationship and implement simple decisions at deployment.

Online adaptation of protocols can be easily achieved by tuning the protocol parameters according to current network conditions. Assuming, at time t_o application requirements for delivery reliability R_o are available to DT protocol, e.g., sink disseminates the application requirements to the nodes. Also the current network properties at t_o are available to DT protocol, e.g., via routing layer, facilitating the DT protocol to computes the protocol parameters. As shown in Figure 2, considering RMST for instance, R_{R_o} and R_{MLD_o} reflect the current network conditions. Wireless sensor nodes can keep track of network conditions either locally or sink can disseminate this information. Consequently, the protocol parameter r_o can be computed by using inverse function of Equation (1) as follows:

$$r_o = \frac{log(1 - R_o/1 - R_{R_o})}{log(1 - (R_{R_o} * R_{MLD_o}))} \qquad (2)$$

If R_R or R_{MLD} varies over time, r will be tuned appropriately such that the required degree of reliability is maintained. Similarly if the application varies its requirement for delivery reliability, r will be tuned to attain the level required by application.

In the future, we plan to expand the framework focusing on different mechanisms for nodes to be aware of application requirements using the requirement analysis presented in [5]. Also we are focusing on developing efficient and scalable mechanisms to calculate the reliabilities of different operations for DT, e.g., R_R and R_{MLD}.

Acknowledgment

This research is supported in part by MUET, NoE ReSIST and DFG GRK 1362 (TUD GK)

References

[1] T. He, B. M. Blum, J. A. Stankovic and T. Abdelzaher, *AIDA: Adaptive application-independent data aggregation in wireless sensor networks*, Trans. on Embedded Computing Sys., 3(2):426–457, 2004.

[2] P. J. Marrón, D. Minder, A. Lachenmann and K. Rothermel, *TinyCubus: An Adaptive Cross-Layer Framework for Sensor Networks*, it - Information Technology, 47(2):89–97, 2005.

[3] F. K. Shaikh, A. Khelil and N. Suri, *On Modeling the Reliability of Data Transport in Wireless Sensor Networks*, Euromicro Conference on Parallel, Distributed and Network-based Processing (to appear),2007.

[4] F. Stann and J. Heidemann, *RMST: Reliable Data Transport in Sensor Networks*, International Workshop on Sensor Network Protocols and Applications, pages 102-112, 2003.

[5] D. Chen and P. K. Varshney, *QoS Support in Wireless Sensor Networks: A Survey*, International Conference on Wireless Networks, 2004.