AReIT: Adaptive Reliable Information Transport Protocol for Wireless Sensor Networks

Faisal Karim Shaikh, Abdelmajid Khelil, and Neeraj Suri
DEEDS Group, Dept. of CS, TU Darmstadt, Germany.

Abstract— *The reliable delivery of services in service oriented architectures often entails the underlying basis of having well structured system and communication network models. With the rapid proliferation of ad-hoc mode of communication, such as Wireless Sensor Networks (WSNs), the reliable delivery of services increasingly encounters new communication and also network perturbation challenges. Empirically the core of service delivery in WSN is information transport from the sensor nodes to the service via a sink node. In this work we classify the different services provided by the WSNs, and provide a reliable information transport protocol (AReIT) for enhanced service delivery. AReIT exploits the spatial and temporal redundancies inside the WSN to provide efficient adaptation for changing service requirement and evolving network conditions. Simulation results show that AReIT provides tunable reliability allowing to save expensive retransmissions while maintaining the reliability level desired by the service.*

Keywords: Wireless Sensor Networks, Service Availability, Reliable Information Transport, Tunable Reliability

1. Introduction

The notion of services in service oriented architectures is often implicitly associated with well structured computing and communication environments. However, as ad-hoc computing environments are proliferating with associated new failure modes, the basis behind assured service delivery requires reliable information transport in these ad-hoc, often wireless connectivity environments. Wireless Sensor Networks (WSN) constitute a rapidly growing research area in ad-hoc networking, covering a wide variety of physical devices, communication networks and providing a diverse set of services. Typical WSN services involve tracking or monitoring as (a) either statically as embedded sensors or (b) dynamically as mobile entities. The users require many services from a WSN along with a set of requirements on them. In response, a WSN collect and transport information for the required services from different parts of the network. Empirically "*information transport*" is at the core of any service which builds on the information collected from different parts of a WSN via a gateway node termed as *sink*.

The service delivery requirements imposes consequent reliability requirements for the information transport in a WSN. It is also expected that these requirements may vary over time. Furthermore, being an ad-hoc and volatile environment, the WSN is obviously subject to a wide range of node and communication level perturbations which impact the availability of a service.

Realistically, it is hard to control the evolving network conditions. Hence the protocols running on top of these networks need to adapt according to these conditions. This leads to the problem of ascertaining which protocol parameters to tune and how to tune them such that the desired level of reliability by the service is maintained despite encountered perturbations. The information transport protocols utilize either temporal redundancy, (e.g., retransmissions [14]) or spatial redundancy, (e.g., number of sources [11] or paths [4]) or some combinations of them [18] to mitigate perturbations to some extent. However, they are not designed to explicitly consider the variable end application level service requirements. The existing solutions are generally designed with assumptions on application and network conditions and there exist only focused solutions for specific conditions.

In [18] the authors provide a reliable information transport protocol termed as reliable bursty convergcast (RBC). It combines most of the existing reliability mechanisms by combining both temporal and spatial redundancies resulting in high reliability. However, RBC lacks in adaptation according to service requirements and evolving network conditions. Since RBC implements a suite of reliability mechanisms, and also given the availability of its modular code, we aim at adapting RBC for different service requirements and for different network conditions. We identify the parameters of interest for information transport and tune them in such a way that service requirements are always met despite evolving network conditions.

Paper Contributions: On this background this paper makes the following contributions.

- We classify the different services provided by WSNs and develop a reliability model for them.
- We identify and show how the availability of services is maintained in the presence of perturbations by tunning information transport protocol parameters.
- We develop an adaptable reliable information transport (AReIT) protocol that builds on top of RBC for ensuring the availability of service.

This research is supported in part by MUET, EC INSPIRE and DFG GRK 1362 (TUD GKMM).

The rest of the paper is organized as follows. Sec. 2 details the system, perturbation and service models relevant in WSN, followed by the related work in Sec. 3. The problem statement is presented in Sec. 4. Sec. 5 presents the proposed AReIT protocol to ensure the availability of a services. We evaluate our proposed approach using simulations in Sec. 6. Our conclusions and future work appear in Sec. 7.

2. Models & Classification

We first present a simple yet comprehensive system and perturbation model to capture generic WSN properties. Next we classify the different services provided by a WSN and their reliability requirements for service delivery.

2.1 System Model

We consider a WSN having N sensor nodes (SNs) numbered $[0..N-1]$ with node 0 termed as sink. Typically, each node is equipped with one or more sensing devices, short range transceivers for communication and with limited processing, memory buffers and energy capabilities. We consider a sink to be adequate in power, ideally for the entire expected life of network, and possessing more memory and higher processing capabilities as compared to the SNs. We assume that all nodes are static in nature including the sink and are placed in a finite size area. SNs communicate with each other via bi-directional multi-hop wireless links employing a CSMA-based Medium Access Control (MAC) protocol. For any two nodes X, Y we define their link quality $LQ = p_{(X,Y)} \cdot p_{(Y,X)}$, where $p_{(X,Y)}$ and $p_{(Y,X)}$ indicates the probability that a packet sent by node X is received correctly by node Y and viceversa. X, Y are defined to be neighbors, if $LQ \neq 0$. This implies that implicit acknowledgements can be used in our model, since neighbors can always hear each other. The sequence of hops $(X, h_1), (h_1, h_2) \cdots (h_f, 0)$ is a path $Path_i$ from node X to the sink. We consider an underlying routing protocol which provides a SN with a next hop along the $Path_i$ towards the sink. SNs generate message(s) to form one-to-one and many-to-one convergent traffic in the upstream direction, i.e., from SNs to sink.

2.2 Perturbation Model

Service availability essentially requires the identification and classification of the relevant node and communication perturbations that can occur in the considered system model. We classify the failures in WSN with respect to *message loss* due to both communication and node level failures.

Communication Level Failures: Communication disruptions constitute the most frequent failures hindering information transport in WSN. High bit error rates of wireless links, collisions and contention constitute the major causes of message loss.

Node Level Failures: At node level message loss is caused by dropping messages from full buffers. In this work we do not consider deliberate failures such as Byzantine faults or intrusions.

Service outage is due to the above mentioned perturbations. In order to ensure the availability of services the protocol must overcome these perturbations using both temporal and spatial redundancy techniques for information transport.

2.3 WSN Service Classification and Reliability Model

As mentioned earlier the major functionality of a WSN is to support the service delivery, i.e., collect and transport the required information to the service. Based on this we provide WSN service classification. Most of the current services fall into one of the following classes.

(i) Event Transport Services: For such services one or more SNs generate the information and transport it towards the sink. In either case information is binary in nature, i.e., whether an event happened or not. Usually these services require high reliability and low latency.

(ii) Tracking Services: In such services many SNs track a moveable target and transport location information towards the sink. Information in such services is short lived and some losses are tolerable. This can be viewed as the transport of many single informations. Depending on the service the reliability requirement on information transport may vary.

(iii) Periodic Continues Services: For continues services each SN periodically generate information to be transported towards sink. Different operations such as filtering and aggregation can be applied to this information on the fly. For such services the reliability requirements are low as the information can be received in subsequent rounds.

(iv) Query Based Services: These services require a group of SNs to generate one or more query results. Query based services are pull based, i.e, upon request the information is generated and transported towards the sink. The requirement on reliability/latency of query result transport is variable and dependent on the querying service.

We refer to an information entity by a raw or aggregated sensor data that is required for reliable service delivery. Information entities can be generated centrally on a single node (e.g., an aggregator) or in a distributed manner by some nodes. In the latter case we say the information entity is replicated. The information entities can further be grouped/composed for a higher semantic such as the location of the nodes that detected the same event and define a new information, i.e., the event/region perimeter. Accordingly, we classify the information required by the services into two classes: *Atomic information* and *Composite information*. Atomic information is composed of a single information entity whereas composite information is composed of more than one information entity. This classification covers the service classes described above. In case of atomic information the service delivery reliability is the degree of tolerating the information loss, i.e., false negatives. For composite information the service delivery reliability is defined as how many losses of information entities can be tolerated by the service without loosing the semantic of the composite information. We express this by a probability p with which the WSN transports information entity towards the sink. In this work, we model a composite information as a set of independent atomic informations to be transported with a certain probability p. We assume that the source node of an atomic information knows p (which takes into account how many atomic information are composing the composite information or how many times an atomic information is replicated). We consider that atomic information is realized through a single message.

3. Related Work

In [3] authors have proposed a hop-by-hop technique for information transport. In order to assure reliability the sequence of packets is sent to the next hop with explicit acknowledgement (EACK). Our works differs from them in considering spatial redundancy along with retransmissions. Also our work exploits the broadcast nature of WSN and utilizes implicit ACK (IACK) which reduces the overhead of explicitly sending an ACK.

Reliable Multi-Segment Transport (RMST) [14] jointly uses selective NACK and timer-driven mechanisms for loss detection and notification. It places responsibility for message loss detection at the receivers (which can be intermediate nodes as well as the sink). RMST also does not exploit the spatial redundancy inside the network and propose retransmissions at the MAC and transport layers. Similarly Asymmetric Reliable Transport (ART) [15] utilizes timer driven retransmissions between essential nodes and source nodes and does not explicitly consider spatial redundancy. Reliability tuning is also not available in these works.

In [11], the authors present Event to Sink Reliable Transport (ESRT) protocol that achieves reliability by adjusting the reporting rate of sensor nodes depending upon current network load. ESRT is developed for continuous event services, where an adaptation of the data report rate makes sense. Our work provides reliability at the hop level whereas ESRT provide end to end reliability which is difficult to maintain in WSN.

Distributed Transport for Sensor Networks (DTSN) [8] and Sensor Transmission Control Protocol (STCP) [5] provide differentiated reliability using end-to-end retransmissions. DTSN beside retransmissions uses forward error codes (FEC) to enhance reliability. End-to-end retransmissions do not respond quickly in face of perturbations thus we adopted hop-by-hop retransmission strategy. On the other hand FEC requires a high level of computation thus limiting its practicality for WSNs.

4. Problem Statement

As we develop our approach on the RBC [18], we first highlight the RBC limitations in terms of its adaptability for varying service delivery requirements and evolving network conditions. A comprehensive performance analysis of RBC can be found in [13], [18].

4.1 Brief Overview of RBC

The RBC protocol provides information transport reliability through hop-by-hop retransmission-based loss recovery. The RBC reliability design is based on a windowless block ACK and IACK along with fixed number of retransmissions to cope with the perturbations. RBC proposes intra- and inter-node message scheduling to avoid collision and contention caused by retransmissions. RBC implicitly assume that more than one SNs are sending the information towards the sink. It should be noted that the RBC does not distinguish between different service requirements and always try to provide high reliability.

4.2 Non-adaptive RBC

For motivation we consider a scenario where service requires information transport reliability for atomic information. We consider a case where the atomic information is generated by many SNs. To this end we assume that 4 SNs are sending redundant information towards the sink. We investigate the RBC's capability to adapt to varying network conditions and to maintain the desired service delivery reliability. This is crucial for availability of service since the network conditions may change during the lifetime of the service. We consider the wireless channel bit error probabilities (BEP) as a link quality indicator, which varies the link reliability between the SNs. In wireless communication quite high average BEP in orders from 10^{-4} to 10^{-2} are possible [6] and to represent this we vary the BEP between a node and its neighbors from 0 to 0.02.

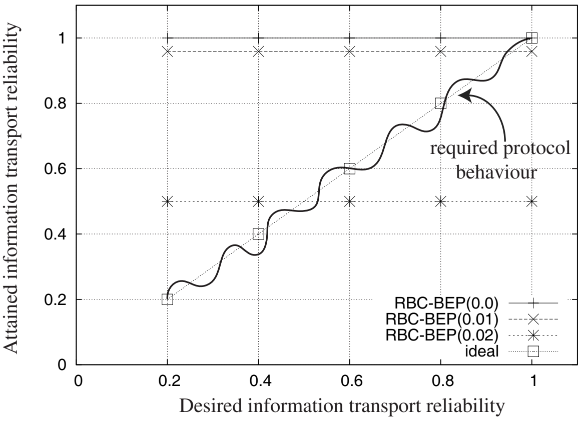


Fig. 1

NON-ADAPTIVE BEHAVIOR OF RBC

We performed simulations for 25 nodes with simulation settings as described in Sec. 6. Fig. 1 depicts the RBC's adaptation for different service requirement and evolving network conditions. For lower BEP's (0.0 - 0.01) RBC over performs and provides higher information transport reliability than required by the service. This trend of RBC depicts the lack of adaptation for different service requirements and suggests that the information transport protocol must be aware of service requirements. As BEP increases the RBC reliability decreases suggesting that the protocol performs poor in erroneous network conditions and thus do not adapt well. Although RBC by default includes a fixed number of maximum retransmissions, i.e., 2, they are not sufficient to cope with the evolving network conditions. In general, RBC provides a constant reliability for a given network condition and thus does not adapt to varying service requirements which can be either higher or lower than the achieved reliability. This motivates for an adaptable protocol which provides service specific reliability and adapt to network conditions in appropriate way such that it follow the ideal case as shown in Fig. 1.

4.3 Parameter Classification

The different information transport protocol parameters for the availability of the service are important, e.g., number of sources ($\#src$), maximum number of retransmissions ($\#ret$) and number of cache points ($\#CP$). $\#CP$ are related to the storage of messages along the path such that in case of message loss the recovery can be initiated. It is shown that for WSN the hop-by-hop approach outperforms other approaches in terms of reliability [16] thus we assume that the information is cached at each hop along the path until an ACK is received. Other parameters of interest are data rate and the number of paths, as they are not directly related with information transport protocol as shown in Fig. 2, we aim at exploring them in future. To monitor the network conditions the different indicators can be utilized, e.g., BEP, signal to noise ratio (SNR), received signal strength indicator (RSSI), link quality indicator (LQI), packet error rate (PER) and path estimators (ETX [2], GEM [12]). These indicators range from locally observing link quality to network wide path qualities as shown in Fig. 2. RSSI is a poor indicator of link quality [17] and LQI is specific to some radios and provide soft state of the link quality. ETX and GEM on the other hand provide path quality and can be misleading due to evolvable network conditions. In this work, we consider BEP as a generic link quality indicator which provide local conditions around the node and represents the elementary indicator for other aggregated indicators such as PER [7]. BEP reflects wide range of cases, i.e, network congestion, collisions and contention, since they tend to corrupt the messages which is similar to BEP.

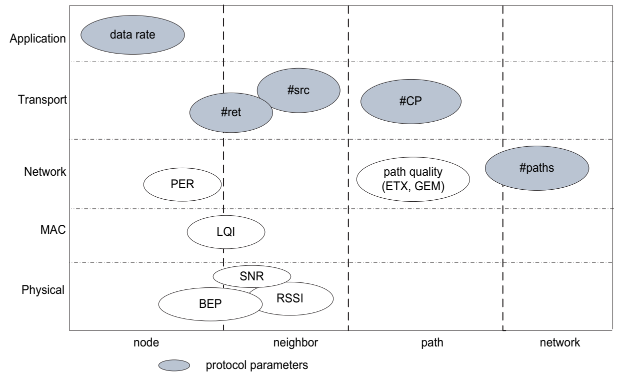


Fig. 2
PARAMETER CLASSIFICATION

5. AReIT: The Adaptive Reliable Information Transport Protocol

We now develop the AReIT protocol that allows for tunable parameters to provide reliable service delivery. As discussed earlier the important parameters for information transport protocol are $\#src$ and $\#ret$. We focus on how to integrate and tune them such that the service requirements are fulfilled despite the encountered WSN node/communication level perturbations.

5.1 Analytical Model for Convergecast Reliability

Consider a node X sending a message regarding an information via node Y along the $Path_i$, h hops away from the sink. The reliability of reaching the information from X to the sink is:

$$R_{inf} = \prod_{h} R_{hop} \tag{1}$$

where R_{inf} is the information transport reliability required by the service and R_{hop} is the reliability across a single hop. Since hop-by-hop reliability assurance is appropriate for WSN [16] and also RBC uses hop-by-hop reliability control, from here and onwards we focus on how to enhance information transport reliability across a hop along the $Path_i$. To ensure reliability across a hop (X, Y) and to overcome node and communication level perturbations, i.e., message loss, more than one transmissions are carried. Let r be the number of transmissions than information transport reliability across a hop (X, Y) is:

$$R_{hop} = 1 - (1 - p_{(X,Y)}p_{(Y,X)})^r = 1 - (1 - LQ)^r \tag{2}$$

where $p_{(X,Y)}$ is the link probability to receive a message and $p_{(Y,X)}$ is the probability to receive an ACK. Since r is total number of transmissions therefore $\#ret = r - 1$. In RBC, when a message m is received at a receiver Y, the acknowledgment for m can reach back to the sender X in two ways: X snoops m when it is forwarded by Y later, or X does not snoop m but snoops a message whose block ACK acknowledges the reception of m. Therefore, according to [18] the $p_{(Y,X)}$ is derived as follows:

$$p_{(Y,X)} = 1 - p + \frac{p(1 - 3p + 4p^2 - 2p^3)}{1 - p + p^2} \quad (3)$$

where $p = p_{(X,Y)}$. Using Eq. 3,

$$LQ = p - p^2 + \frac{p^2(1 - 3p + 4p^2 - 2p^3)}{1 - p + p^2} \quad (4)$$

In response to many WSN services, more than one SN generate messages and send towards the sink, e.g., event transport services. For these services the source nodes normally have spatial correlation and send information in a convergent manner towards the sink, therefore the integrated reliability across a hop will be:

$$R_{int} = 1 - (1 - R_{hop})^s \quad (5)$$

where $s = \#src$ sending the information to the sink. Putting Eq. (2) in Eq. (5) yields

$$R_{int} = 1 - ((1 - LQ)^r)^s \quad (6)$$

Eq. (6) utilizes an integrated mechanism which explicitly accounts for the spatial redundancy in the form of $\#src$ and temporal redundancy in the form of $\#ret$.

5.2 AReIT Adaptation

AReIT adapts to the changing service requirements and evolving network conditions to overcome the perturbations. For a specified information transport reliability $R_{desired}$ imposed by the service and known number of hops from the sink, we can calculate the desired reliability requirement R_{h_d} across a hop as:

$$R_{h_d} = (R_{desired})^{1/h} \quad (7)$$

Eq. (7) considers a uniform reliability requirement across the hops along the $Path_i$. When the source node sends a message it first decides whether to send the message or not. The decision is based on source node's local network condition, i.e., link reliability (R_L) and the service requirements on the information transport reliability (R_{h_d})as follows:

$$p_s = \begin{cases} R_{h_d}/R_L & \text{if } R_L > R_{h_d} \\ 1 & \text{if } R_L \leqq R_{h_d} \end{cases}$$

where $R_L = (1 - LQ)$. If $R_L > R_{h_d}$ the source node sends the message with probability $p_s = R_{h_d}/R_L$ in order to maintain the required service delivery. For the case $R_L \leqq R_{h_d}$ the source node always sends the message to its parent node. This step ensures that AReIT always maintain the specified information transport reliability thus adapting to service requirements.

Once the node decides to send the message, it will calculate how many transmissions are required to fulfill the service requirements. The node checks, if $R_{int} \geqq R_{h_d}$, it will transmit the message once to its parent node else the node will calculate the number of transmissions required to attain the R_{h_d} using Eq. (6).

$$r = \begin{cases} \frac{log(1-R_{h_d})}{s \cdot log(1-LQ)} & \text{if } R_{int} < R_{h_d} \\ 1 & \text{if } R_{int} \geqq R_{h_d} \end{cases} \quad (8)$$

Here we have chosen probabilistic transmissions [3], i.e., if $r = 1.34$ than the node will do first, one transmission and then another retransmission with a probability of 0.34. Using Eq. (8) AReIT ensure the reliability of information transport by exploiting spatial and temporal redundancy. In this work, we assume that each source node knows the number of other sources sending the replicated information, e.g., in query service the query may specify the number of nodes reporting the information. In future we explore how to tune the number of source nodes, i.e., $\#src$. To avoid infinite transmissions the service can specify the maximum threshold r_{th} and node will discard the message after r_{th}.

5.3 Parameter Acquisition

In order to acquire hop count h and specified desired reliability $R_{desired}$ the underlying routing protocol can be utilized. It should be noted that in this work we emphasize on information transport from SNs to the sink for ensuring service delivery and not on dissemination of service parameters to SNs. To this end the sink can use existing reliable downstream dissemination strategies, e.g., [9], [15], [16].

Node X keeps track of the link quality, i.e., BER between its parent node Y towards the sink using exponentially weighted moving average (EWMA) [17] as follows:

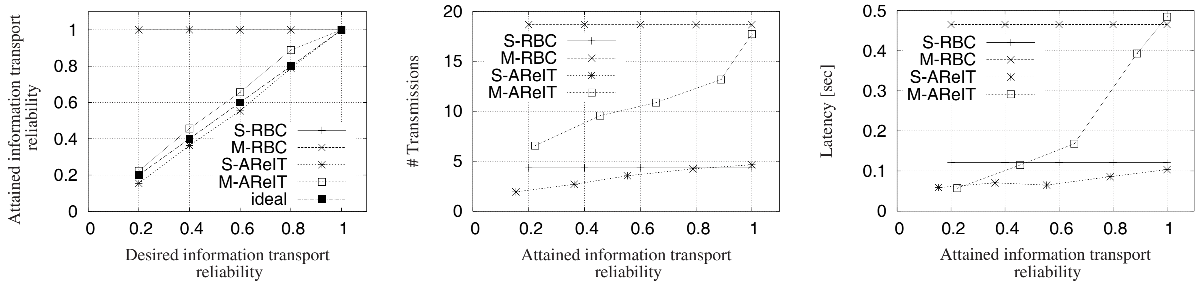
$$LQ^t = (1 - \alpha) * LQ^t + \alpha * LQ^{t-1} \quad (9)$$

where α is a weight-factor ranging between $0 < \alpha < 1$ and LQ^t is the latest observation of the link quality in terms of BEP. The EWMA approach avoids the wrong node decisions due to sudden or abrupt changes in the network. In this work, a node keeps track of BEP between itself and its parent upon reception of a message or when it snoops the channel for IACK. In the simulations we used typical value of $\alpha = 0.1$.

6. Evaluation

We evaluate our approach based on simulations in the TOSSIM [7] simulator. TOSSIM is an event-driven simulation tool widely used in the WSN community. For MAC we have used default CSMA-based implementation in TOSSIM. It does not perform any retransmissions, but notifies the upper layers of missing acknowledgements for uni-cast messages. As for routing, RBC uses by default Logical Grid Routing (LGR) [1] protocol, we continue using LGR with the default settings as described in [1]. The code of RBC is available for the mica2 mote platform, consequently we ported the RBC code to run under the TOSSIM environment.

The topology used in our simulations consists of a n x n grid topology. The sink is located at one corner. The atomic



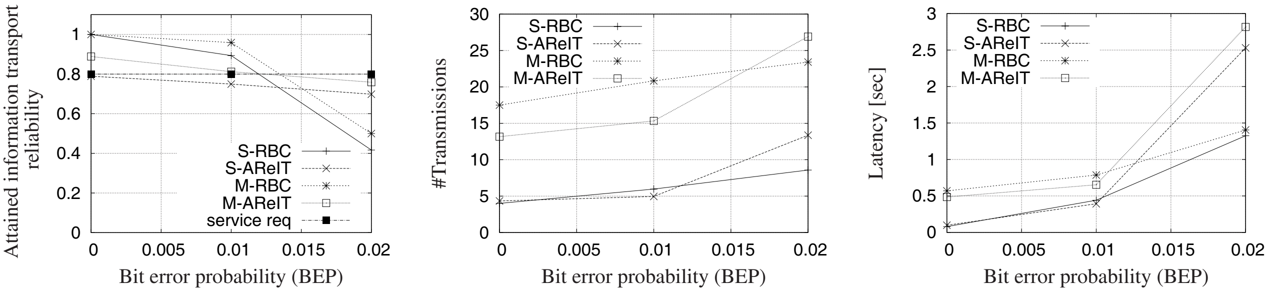
(a) Information transport reliability

(b) Information transport efficiency

(c) Information transport timeliness

Fig. 3

ADAPTATION TO SERVICE REQUIREMENTS



(a) Information transport reliability

(b) Information transport efficiency

(c) Information transport timeliness

Fig. 4

ADAPTATION TO NETWORK CONDITIONS

information is generated from one corner and transported towards the sink. We have chosen two cases: One where atomic information is generated by a single source and another where the atomic information is generated by s sources that are geographically close to each other. In our experiments 10 atomic information are generated with the gap of 3 sec to be transported towards the sink. In this work we assume number of sources $s = 4$ and each source node knows the value of s. r is calculated by the sources and relay nodes on the fly using Eq. (8). Information is generated after 10 sec from the start of the simulation to give enough time for the network to stabilize.

The performance of information transport protocol for service delivery is measured as protocol's responsiveness and efficiency. The responsiveness of the protocol is its information transport reliability and timeliness, and the protocol efficiency is mainly given by its message complexity.
Reliability: The information transport reliability of the protocol is the ratio of number of information received by the service/sink to the total number of the information generated.
Timeliness: The timeliness, i.e., latency of information transport protocol is defined as the time elapsed from the generation of the first information message to the arrival of the first information message at the sink. The timeliness of the protocol is the average of information transport latencies of all generated information. As some information may not be reported at the sink, we do not consider the corresponding messages in the calculation of the average information transport timeliness.
Efficiency: We define the message complexity of an information transport as the total number of message transmissions required for the information to be delivered to the service (including the retransmissions).

6.1 Simulation Results

Fig. 3 shows the adaptation of our approach for variable service requirements on information transport. Fig. 3(a) depicts the reliability attained by RBC and AReIT when single node (S-RBC, S-AReIT) and multiple nodes (M-RBC, M-AReIT) are sending the atomic information to the sink. We observe that S-AReIT and M-AReIT attains desired reliability with slight difference. The reliabilities attained by S-RBC and M-RBC are independent of the desired reliability and are constant. Fig. 3(b) shows the total number of transmissions required to attain the information transport reliability. The number of the transmissions for S-RBC and M-RBC do not change. The number of transmissions vary for S-AReIT and M-AReIT in proportion to the attained level of reliability. We observe that M-AReIT has relatively less number of transmissions than M-RBC due to the fact of explicitly integrating the spatial redundancy of nodes sending information to the sink. Generally, AReIT adapts to the desired service requirements with less number of transmissions than RBC. Fig. 3(c) shows the timeliness of RBC and AReIT. The latency of AReIT is well below the RBC for providing attained service reliability. For higher service reliability requirement (100%), AReIT behaves similar to the RBC in terms of efficiency and timeliness.On the other hand for all other cases AReIT outperforms RBC with respect to responsiveness and efficiency.

Fig. 4 compares the RBC and AReIT robustness for evolving network conditions. In this scenario we assume that service requirement for information transport is 80%. Fig. 4(a) shows the information transport reliability for varying BEP. S-AReIT and M-AReIT cope with the evolving network conditions and provide desired service requirement with slight difference of (+/-) 2% whereas S-RBC and M-RBC are not able to cope with evolving network conditions and provide high reliability for good network conditions (BEP 0.0 - BEP 0.01) and less reliability for worse network conditions (BEP 0.02). For BEP 0.02 M-AReIT and S-AReIT utilize more transmissions owing to the adaptation to bad network conditions by increasing number of retransmissions (Fig. 4(b)). On the other hand S-RBC and M-RBC after fixed number of retransmissions failed to transport the information, thus resulting in less number of transmission with less than desired reliability. This also impacts the timeliness of AReIT as shown in Fig. 4(c) At BEP 0.02 the latency of S-AReIT and M-AReIT is higher than S-RBC and M-RBC, but it is directly related to the number of transmissions and attained reliability. In general AReIT maintains the desired reliability with higher number of transmissions and higher latency when BEP is high.

6.2 Discussions

The different simulations have quantified the viability of AReIT. In the light of the experimental analysis we make the following observations:

Different service classes impose different reliability requirements for service delivery, thus the protocol should adapt accordingly. AReIT shows its capability of providing service specific reliability (Fig. 3(a)) and outperforms the RBC protocol. In WSN perturbations are norm rather than exception and providing reliable service delivery is difficult. We observed the AReIT capability to cope with harsh environments where network connectivity is fluctuating (Fig.4(a)). The information availability at the sink is important for reliable service delivery. AReIT manage information availability by efficiently tunning the number of retransmissions and adapting according to the number of sources. For the reliable service delivery, timeliness plays important role. Information not reaching in timely fashion is useless for a service, thus hindering the service delivery. Fig. 3(c)-4(c) show that AReIT provides required information transport reliability with less latency. Generally, it is observed that there is a tradeoff between efficiency and timeliness to provide reliable service delivery. For example, at BEP 0.0 less transmissions are carried with low latency. On the other hand at BEP 0.02 more transmissions are required leading to higher latency. Overall, our approach saves valuable retransmissions by maintaining the desired reliability and avoiding over performance.

7. Conclusion & Future Work

In this work we have presented an Adaptable Reliable Information Transport (AReIT) protocol which provides dynamic tunning of retransmission to overcome perturbations along with integrated spatial knowledge for information transport. AReIT is capable of adapting to different service requirements by exploiting temporal and spatial redundancies. In future we are looking to explore more link quality metrics and to analyze the impact of these metrics on information transport reliability. Also we are looking for different mechanisms where source nodes locally and dynamically learn about the number of sources sending the information towards the sink.

References

[1] Y. Choi, *et al.* Stabilization of grid routing in sensor networks. *J. of Aerospace Computing, Inf. and Commun.*, 3:214–233, 2006.

[2] D. Couto, *et al.* A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, 11(4):419–434, 2005.

[3] B. Deb, *et al.* Information assurance in sensor networks. In *WSNA*, pp. 160–168. 2003.

[4] D. Ganesan, *et al.* Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(4):11–25, 2001.

[5] Y. G. Iyer, *et al.* Stcp: A generic transport layer protocol for wireless sensor networks. In *ICCCN*, pp. 449 – 454. 2005.

[6] H. Karl and A. Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, 2005.

[7] P. Levis, *et al.* Tossim: accurate and scalable simulation of entire tinyos applications. In *SenSys*, pp. 126–137. 2003.

[8] B. Marchi, *et al.* Dtsn: Distributed transport for sensor networks. In *ISCC*, pp. 165–172. 2007.

[9] S. Park, *et al.* A scalable approach for reliable downstream data delivery in wireless sensor networks. In *MobiHoc*, pp. 78–89. 2004.

[10] J. Polastre, *et al.* Versatile low power media access for wireless sensor networks. In *SenSys*, pp. 95–107. 2004.

[11] Y. Sankarasubramaniam, *et al.* Esrt: event-to-sink reliable transport in wireless sensor networks. In *MobiHoc*, pp. 177–188. 2003.

[12] O. Saukh, *et al.* Generic routing metric and policies for wsns. In *EWSN*, pp. 99–114. 2006.

[13] F. K. Shaikh, *et al.* A comparative study for data transport protocols for wsn. In *WOWMOM*, pp. 1 – 9. 2008.

[14] F. Stann and J. Heidemann. Rmst: Reliable data transport in sensor networks. In *SNPA*, pp. 102–112. 2003.

[15] N. Tezcan and W. Wang. Art: an asymmetric and reliable transport mechanism for wireless sensor networks. *Int. J. Sen. Netw.*, 2(3/4):188–200, 2007.

[16] C. Wan, *et al.* Psfq: a reliable transport protocol for wireless sensor networks. In *WSNA*, pp. 1–11. 2002.

[17] A. Woo, *et al.* Taming the underlying challenges of reliable multihop routing in sensor networks. In *SenSys*, pp. 14–27. 2003.

[18] H. Zhang, *et al.* Reliable bursty convergecast in wireless sensor networks. In *MobiHoc*, pp. 266–276. 2005.