Reliable congestion-aware information transport in wireless sensor networks

Faisal Karim Shaikh*, Abdelmajid Khelil,
Azad Ali and Neeraj Suri

Technische Universität Darmstadt,
Hochschulstr. 10, Darmstadt 64289, Germany
E-mail: fkarim@cs.tu-darmstadt.de
E-mail: khelil@cs.tu-darmstadt.de
E-mail: azad@cs.tu-darmstadt.de
E-mail: suri@cs.tu-darmstadt.de
*Corresponding author

Abstract: Wireless sensor networks (WSNs) constitute the transportation conduit for the results of the in-network processing of the raw data. In WSNs the sensor node and communication level perturbations are often the norm than the exception due to varied environmental conditions. Consequently, the diverse applications supported by WSNs stipulate their individual (and varied) requirements for WSN information transport reliability in order to meet their specific responsiveness needs. The use of an approach that guarantees the highest reliability level for information delivery is not a realistic option as this over-provisioning wastes key resources such as energy or bandwidth. In this paper, we present a new approach termed ReCAIT that targets 'congestion-aware' reliable information transport in WSNs to provide application-specific tunable reliability and thus avoids over-provisioning. To provide tunable reliability, ReCAIT efficiently integrates probabilistic adaptive retransmissions, hybrid acknowledgement and retransmission timer management. ReCAIT proactively alleviates the congestion by transporting information on multiple paths. If congestion persists ReCAIT's back-pressure mechanism triggers the information rate control. Our simulation results show that ReCAIT provides tunable reliability and mitigate congestion, which maximises the efficiency of information transport in terms of reduced number of transmissions.

Keywords: tunable reliability; congestion control; information transport; adaptive retransmission.

Reference to this paper should be made as follows: Shaikh, F.K., Khelil, A., Ali, A. and Suri, N. (xxxx) 'Reliable congestion-aware information transport in wireless sensor networks', *Int. J. Communication Networks and Distributed Systems*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Faisal Karim Shaikh is a member of the DEEDS group at Technische Universität Darmstadt, Germany.

Abdelmajid Khelil is a member of the DEEDS group at Technische Universität Darmstadt, Germany.

Azad Ali is a members of the DEEDS group at Technische Universität Darmstadt, Germany.

Neeraj Suri is a member of the DEEDS group at Technische Universität Darmstadt, Germany.

1 Introduction

Wireless sensor networks (WSNs) constitute a rapidly growing research area, spanning a wide variety of applications. Empirically, the core operation of a WSN is to transport the information of interest from the network to the application via a gateway node termed as *sink*. The desired application reliability requirements consequently impose specific information transportation level reliability requirements on the WSN. Being an ad-hoc and volatile environment, WSN is subject to a wide range of operational perturbations affecting both the nodes and the communication links. These perturbations naturally lead to deviations between the attained and desired reliability of the underlying information transportation, thus complicating the design of transport protocols. There has been extensive research to design transport protocols suitable for WSNs (Wang et al., 2006; Rahman et al., 2008). The comparative study in Shaikh et al. (2008) has shown that the current approaches perform well only for carefully selected scenarios. Furthermore, they are usually not able to cope with varying application requirements and evolving network conditions as they are designed for specific applications. However, it is obvious that a WSN runs different applications (monitoring, network management, event detection, event perimeter tracking etc.) that require different information types with varied transport reliability requirements. For example, monitoring applications may tolerate some losses and require comparatively low reliability whereas specific event detection applications may require high reliability for meaningful operations. The existing approaches, aiming at a static transport reliability level, typically over-utilise the limited network resources even when the application does not require high reliability information delivery characteristics.

In order to maintain the reliability of information transport, the congestion in the network should be handled appropriately. To mitigate congestion some schemes implicitly assume that whenever congestion is detected, it is network wide and long lasting (Wan et al., 2003; Wang et al., 2007; Rangwala et al., 2006). On the contrary, some approaches assume that the congestion is always in a small area and short lived (He et al., 2008; Jaewon et al., 2007; Popa et al., 2006). The existing solutions are reactive in nature, i.e., when congestion happens they detect it and by the time they react on the situation some information loss may happen. Furthermore, none of these approaches considers varied application level reliability requirements.

To the best of our knowledge we are the first to target *tunable* information transport reliability with congestion awareness in face of varied application requirements and evolving network conditions.

On the above background this paper makes the following contributions:

1 we develop a Reliable Congestion Aware Information Transport (ReCAIT) approach to ensure tunable reliability

2 to recover information loss we develop hybrid acknowledgement and adaptive retransmission timer strategies

3 we develop a mechanism for mitigating wireless link congestion

4 we develop mechanisms which proactively detect and mitigate congestion in the network.

The paper is organised as follows. Section 2 presents the related work followed by details of the system, perturbation, information and reliability models in Section 3. Section 4 presents the overall ReCAIT approach. We detail the evaluation of the ReCAIT approach in Section 5.

2 Related work

The current state of the art can be classified into three areas: works providing reliability, works focusing only on congestion and works dealing with both of these issues.

- *Reliability:* In this area, the major focus is on maximising network level reliability, i.e., not loosing the messages. In order to increase reliability, different acknowledgement (ACK) schemes are widely adapted. In Deb et al. (2003), a sensor transport node sends the sequence of messages to the next hop and the receiver node uses explicit acknowledgement (EACK) to ensure reliability. Reliable multi-segment (Stann and Heidemann, 2003) utilises timer driven retransmissions for loss detection and notification. Distributed transport for sensor networks (Marchi et al., 2007) and sensor transmission control protocol (Iyer et al., 2005) provide differentiated reliability using end-to-end retransmissions. DTSN beside retransmissions uses forward error codes to enhance the reliability. For high information rates, reliable bursty convergecast (RBC) (Zhang et al., 2005) provides a reliability design based on a windowless block ACK and implicit acknowledgement (IACK) along with a fixed number of retransmissions. Another approach to increase the reliability is to utilise multiple paths. In Felemban et al. (2006), MMSPEED protocol is proposed to provide probabilistic QoS guarantee in WSNs using multipath forwarding.
- *Congestion control:* The major focus in this class is on congestion control and not on providing reliability. The existing approaches (Wan et al., 2003; Wang et al., 2007; Rangwala et al., 2006) limit the information rate to mitigate the congestion, which sometimes may be in contradiction to the application requirements. All these works consider that if the path is congested, the whole network is congested, which may not necessarily be the case. These approaches require feedback from the sensor nodes, which results in extra communication overhead in the network. Reducing congestion with multipath routing has been addressed recently (He et al., 2008; Jaewon et al., 2007; Popa et al., 2006) without considering reliability.
- *Reliability and congestion control:* There are very few works that consider both reliability and congestion control. Congestion control is necessary to to provide information transport reliability since congestion in the network deviate the attained reliability from the desired reliability. Event to sink reliable transport (ESRT) protocol (Sankarasubramaniam et al., 2003) achieves reliability by adjusting the reporting rate of sensor nodes depending on current network load. Upon congestion detection, nodes notify the sink for appropriate action. By the time sink takes some action, the current network state may be changed, thus resulting in waste of network resources. RCRT (Paek and Govindan, 2007) also works on the principle of ESRT and provide end to end best effort reliability.

The lack of an integrated approach that provides tunable reliability and congestion control for information transport motivated us to design ReCAIT.

3 Models and classification

We first present a simple though comprehensive system and perturbation model. Next, we present the information model and its reliability requirements.

3.1 System model

We consider the conventional model of a WSN having **N** sensor nodes $[S, 1, \ldots N-1]$ with Node S being the sink. Typically, each node is equipped with one or more sensing devices, short range transceivers for communication typically with limited processing, memory and energy capabilities. We consider the sink to be adequate in power, ideally for the entire expected life of network, possessing more memory and higher processing capabilities as compared to the sensor nodes. We assume that all nodes are static in nature (including the sink). The sensor nodes communicate with each other via bidirectional multi-hop wireless links. Each sensor node maintains a buffer of size Q. For any two nodes X and Y we define their link quality $LQ = p_{(X,Y)} \cdot p_{(Y,X)}$, where $p_{(X,Y)}$ and $p_{(Y,X)}$ indicate the probability that a message sent by Node X is received correctly by Node Y and vice versa. X, Y are defined to be neighbours, if $LQ \neq 0$. This implies that IACK can be used in our model. All sensor nodes know their hop number $h(X)$ from the sink and their 1-hop neighbours. Based on hop number the neighbours of a node can be classified as upstream neighbours, downstream neighbours and equal neighbours. We denote the set $N_u = \{Y : \{X, Y\} \in \mathbf{N} \wedge h(Y) = h(X) + 1\}$ as the upstream neighbours of Node X, the set $N_d = \{Y : \{X, Y\} \in \mathbf{N} \wedge h(Y) = h(X) - 1\}$ as its downstream neighbours, and the set $N_e = \{Y : \{X, Y\} \in \mathbf{N} \wedge h(Y) = h(X)\}$ as its equal neighbours respectively. We assume the underlying routing protocol to establish routes from sensor nodes to the sink and to provide knowledge about $h(X)$, N_u, N_d and N_e.

3.2 Perturbation model

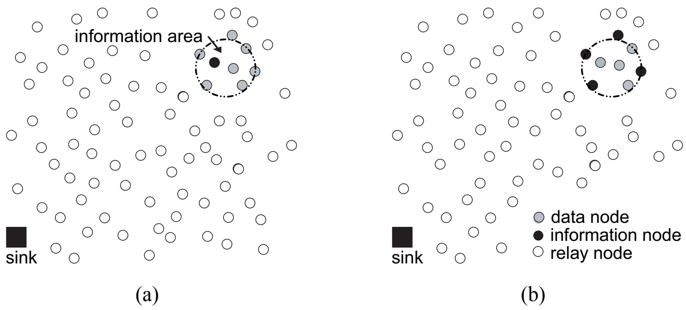
Information transport essentially requires the identification and classification of the relevant node and communication perturbations that can occur in the considered system model. We classify the information transport failures in WSN with respect to *message loss* due to both communication and node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

- *Communication level failures:* Communication disruptions constitute the most frequent failures hindering information transport in WSN. Collision and contention constitute the major causes of message loss for information transport.
- *Node level failures:* At node level, message loss is mainly caused by buffer overflow due to increasing network load.

3.3 Information and reliability model

We refer to an information entity as an aggregated sensor data that is required by the application. Information entities can be generated centrally on a single node (e.g., a cluster head) within an information area or in a distributed manner by some nodes (spatially co-related). Information entities are generated by information nodes whereas the raw data is generated by data nodes (Figure 1). The information entities can further be grouped/composed for a higher semantic such as grouping 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 applications into two broader classes: *atomic information* and *composite information*. Atomic information is composed of a single information entity, whereas composite information is composed of more than one (distinct) information entities as shown in the Figure 1.

Figure 1 Information model, (a) atomic information (b) composite information



Generally, WSN applications entail providing x% (probabilistically-guaranteed) reliable information transport instead of best effort or transporting all information entities. Therefore, the application level end-to-end reliability R_d $(0 < R_d <= 1)$ is described by the probability of information to be transported successfully to the sink. Based on the application requirements, the atomic information transport reliability is defined as the degree of tolerating the information loss over time. Similarly, the composite information transport reliability is defined as the degree of tolerating loss of information entities by the application without loosing the semantic of the composite information.

In this work, we model composite information as a set of independent atomic information to be transported. We assume that the source node knows R_d, i.e., the probability with which information is to be transported. R_d takes into account the set of atomic information comprising the composite information. In this work, we also assume that atomic information is realised through a single message and is generated by a single sensor node. Furthermore, we consider high information rates, i.e., bursty information to be transported to the sink.

4 ReCAIT: the proposed approach

We first provide a conceptual overview of ReCAIT. Consequently, we show how it adaptively integrates and controls different techniques on-the-fly to provide tunable reliability and congestion control for information transport.

4.1 Overview of our approach

The primary motivation behind ReCAIT is to provide the desired reliability of information transport despite dynamic network conditions. The basic idea of ReCAIT approach is very simple. When there is no congestion ReCAIT tolerates the message loss by adapting the number of retransmissions. ReCAIT provides tunable reliability by probabilistically suppressing the information, since sending more information which is not required by the application will waste the resources. The sensor nodes proactively monitor the information flow across them and detect congestion. Due to high information rate wireless link congestion builds up and to overcome it ReCAIT provides application-aware reliability oriented scheduling. When a node detects short lived congestion, it splits the information across its neighbours (potentially creating the multiple paths) in order to tolerate message loss due to buffer overflow. If the congestion still persists, ReCAIT detects long lived congestion by observing the buffer status of neighbouring sensor nodes. To mitigate long lived congestion ReCAIT utilises the back-pressure mechanism (without any extra overhead) to adjust information rate at the source nodes.

Next we detail the ReCAIT mechanisms by progressively defining the elements of:

a tunable reliability (Section 4.2)

b congestion awareness (Section 4.3).

4.2 Tunable reliability in non-congested scenarios

In order to provide tunable reliability Algorithm 1 proceeds with the calculation of the desired application reliability across the hops along the path towards the sink. Next, the sensor nodes determine whether to forward or suppress the information to maintain the desired reliability. To efficiently recover message loss ReCAIT utilises a hybrid ACK and an adaptive retransmission timer scheme.

More specifically, ReCAIT utilises the default single path (SP) for transporting the information when there is no congestion. Usually, in WSN the information is transported over many hops from the source nodes to the sink. For the known R_d and number of hops from the sink, the desired reliability requirement across a hop (R_{h_d}) is calculated as $R_{h_d} = (R_d)^{1/h(X)}$, where X is the source node. When a sensor node has an information to transport, it first decides whether to send or probabilistically suppress (p_s) the information to next hop. The decision is based on node's local network conditions and application requirements as follows:

$$p_s = \begin{cases} (R_{h_d}/R_{hop}) + \Delta_{th} & \text{if } R_{hop} > R_{h_d} \\ 1 & \text{if } R_{hop} \leqq R_{h_d} \end{cases} \tag{1}$$

where R_{hop} is the reliability across a hop along SP and $0 < \Delta_{th} \ll 1$ is used to ensure the attained information transport reliability is always bounded by R_d and $R_d + \Delta_{th}$. Once the sensor node decides to send the information, it calculates the maximum number of transmissions (r) required to attain the R_{h_d} as follows:

$$r = \lceil \frac{\log(1 - R_{h_d})}{\log(1 - R_{hop})} \rceil \tag{2}$$

A sender Node X starts a retransmission timer after sending information to the next hop Node Y (Algorithm 1, L 15–16). If Node X snoops IACK it discards the retransmission timer and purges the information from its buffer (Algorithm 1, L 20–22). Node X may not snoop IACK either due to IACK loss or due to suppression of information at Node

Y. To mitigate IACK loss Node X retransmits after the expiry of retransmission timer. If Node Y decides to suppress the message it sends EACK back to Node X (Algorithm 1, L 25–28). Using the hybrid ACK scheme (combination of IACK and EACK), ReCAIT saves extra retransmissions carried out by Node X due to either suppression at Node Y or IACK loss.

Small timeout values of retransmission timer cause unnecessary retransmissions, whereas large timeout values increase the information transport delay. Thus, to estimate the retransmission timer (t_{ret}), sensor nodes utilise the buffer occupancy (q_o) of next node along SP and time for transmitting a message (t_o) as follows: $t_{ret} = q_o \cdot t_o$. Due to congestion the buffer occupancy of sensor nodes is drifted and the retransmit timer is adapted as $t_{ret} = q_o \cdot (t_o + 4t'_o)$, where t'_o is the deviation of t_o. In Jacobson (1988) and Zhang et al. (2005), it is shown that a quick increase in retransmission timer provides better results during congestion and the authors propose $4t'_o$ to be appropriate. Thus, we adopted deviation as $4t'_o$.

Algorithm 1 ensures tunable reliability and efficiently tolerates the information loss due to collisions by using hybrid ACK and adaptive retransmission timeout values.

Algorithm 1 Tunable reliability by ReCAIT

```
   Data: R_hd, h(X), t_ret, msg, Y_i ← next hop
1  if (source node) then
2  |  msg.R_hd ← R_hd = (R_d)^(1/h(X));
3  |  transport(msg, Y_i, FALSE);
4  end
5  if (forwarding node) then
6  |  if (msg in buffer) then
7  |  |  send EACK;
8  |  |  wait random time ≥ t_ret;
9  |  |  purge msg;
10 |  end
11 |  transport(msg,Y_i,FALSE);
12 end
13 function transport(msg, Y_i, congestion):
14 \\ check - send or suppress using Eq. (??);
15 if (send) then
16 |  calculate r using Eq. (??);
17 |  for (each t_ret fired) do
18 |  |  send msg to Y_i;
19 |  |  if (!congestion) then t_ret = q_o · t_o;
   |  |  else t_ret = q_o · (t_o + 4t'_o);
20 |  |  if (snoop IACK) then
21 |  |  |  stop t_ret; purge msg; exit();
22 |  |  end
23 |  end
24 end
25 if (suppress) then
26 |  send EACK; wait random time ≥ t_ret;
27 |  purge msg;
28 end
29 end function
```

Now we elaborate ReCAIT congestion awareness and present algorithms for short (Algorithm 2) and long lived congestion (Algorithm 3) inside the network.

4.3 Congestion-aware tunable reliability

eCAIT utilises proactive congestion detection in order to avoid the information loss. Upon congestion detection ReCAIT efficiently mitigates the congestion by dispersing the information to the neighbour nodes. ReCAIT continuously monitors the network condition and provides information rate adaptation for source nodes without explicit notification.

Due to high information rate across the sensor nodes a wireless link congestion builds up, which hinders in forwarding the information towards the sink. ReCAIT provides an efficient application-aware mechanism to schedule message transmissions. To reduce the interference inter-node message scheduling takes into account the desired reliability of messages stored by the sensor nodes. Accordingly, the nodes having more messages with higher reliability requirements transmit the messages earlier. The sensor nodes calculate and piggyback the average reliability of buffered messages $R_{q_{avg}} = (\sum_{i=1}^{q_o} R_{h_{d_i}})/q_o$. Upon snooping or receiving the message, a sensor node compares its tuple ($\langle q_o, R_{q_{avg}} \rangle$) with the received message. The node will change its scheduling only if its tuple is lower then the received tuple, i.e., its buffer occupancy and information reliability requirement are lower. If the tuple is lower the node does not send any message during $\beta \cdot t_o$ time units, where β is a waiting factor. β should be defined in such a way that the probability of all waiting nodes starting their transmissions simultaneously is reduced, and that higher-tuple nodes tend to wait for shorter time. Consequently, we define $\beta = \max(R_{q_{avg_X}}, R_{q_{avg_Y}}, \cdots) + \min(q_{o_Y}, q_{o_X}, \cdots) + \gamma$, where $0 < \gamma < 1$ is a drift and taken at random to avoid simultaneous transmission.

The high incoming information rate (ξ_i) across a node compared to the outgoing information rate (ξ_o) provides early predictor of congestion. Information accumulation at the sensor node can be due to several reasons (1) the wireless link is congested (contention) and (2) the buffer of next hop node is full. In order to provide proactive congestion control each sensor node keeps an exponentially weighted moving average (EWMA) of ξ_i and ξ_o when it receives or transmits messages. Based on this, the congestion factor (ς) can be defined as:

$$\varsigma = \mid \frac{\xi_o}{\xi_i} \mid \tag{3}$$

ς is a proactive indicator of the congestion since it provides congestion indication before it actually happens. The congestion factor first defined in Wang et al. (2007) utilises complex mechanism of computing timers for incoming and servicing of the messages compared to our efficient approach which requires only the count of incoming and outgoing messages. The time window T over which ς is calculated is critical. If the value of T is too long then the buffer can overflow due to higher ξ_i. If the value of T is too short it may lead to exacerbating the congestion. Accordingly, we set the value of T = $t_o \cdot Q_{TH}$. This ensures that the sensor node will check for ς before the buffer overflows. Also, it is not too short to behave reactively towards congestion.

Algorithm 2 Short lived congestion control by ReCAIT

```
Data: ξ_i, ξ_o, N_d, N_e, N_u
for (each time interval T) do
    ς = |ξ_o/ξ_i|;
    if (ς < 1) then
        organizeNeighbors(); disperseInfo();
    end
    else transport(msg,Y_i,FALSE);
end
function organizeNeighbors():
sort N_d,N_e,N_u according to max R_hop;
end function
function disperseInfo():
if (N_d≠∅) then
    select next Y_i ∈ N_d;
    transport(msg,Y_i,TRUE);
end
else if (N_e≠∅) then
    select next Y_i ∈ N_e;
    msg.R_{h_d} ← R'_{h_d} = (R_d/R_{h_d})^{1/h(Y)};
    transport(msg,Y_i,TRUE);
end
else
    select next Y_i ∈ N_u;
    msg.R_{h_d} ← R'_{h_d} = (R_d/R_{h_d})^{1/h(Y)};
    transport(msg, Y_i, TRUE);
end
end function
```

We now present a solution for mitigating short lived congestion (Algorithm 2) which assures tunable reliability by adjusting the per hop desired reliability upon dispersing the information to the neighbour nodes. Once a node locally detects the short lived congestion [equation (3)], it disperses the information to the set of neighbour nodes, i.e., N_d,N_e and N_u in a round robin fashion (Algorithm 2, L 11–26). The dispersion of information from the point of congestion to the neighbour nodes assure that the congestion will not accumulate on SP. The sensor node that detects the congestion sends the information to the neighbour nodes in N_d (Algorithm 2, L 12–14). If congestion persists and $N_d = \emptyset$, nodes from N_e are selected to transport the information (Algorithm 2, L 16–19). In the worst case if both sets are empty, the information is transmitted to the neighbours in N_u (Algorithm 2, L 22–24). If a node selects a neighbour node from N_d it does not change R_{h_d} since the number of hops remains constant for the information to travel. If the neighbour node belongs to N_e or N_u, the desired hop reliability is recalculated as $R'_{h_d} = (\frac{R_d}{R_{h_d}})^{1/h'(Y)}$, where R_{h_d} is the previously calculated desired hop reliability and $h'(Y)$ is the neighbour node's hop number.

It should be noted that to mitigate a short lived congestion we assume that the sensor nodes around the congestion spot are not heavily loaded. Once the network load increases further such that a sensor node after dispersing the information to its neighbours is not able to cope with the congestion, we say that a sensor node is experiencing long lived congestion. The only solution to mitigate long lived congestion is to inform the source nodes to decrease the information rate such that the congestion can be alleviated. ReCAIT allows sensor nodes to keep track of q_o of their neighbours upon dispersing the information. When the buffer occupancy of all neighbour nodes is above a certain threshold (Q_{th}), the sensor node concludes that it can not disperse the information further to its neighbours (Algorithm 3, L 2–8). The sensor node waits for T units and tries again to send the information. During this time it can receive further messages till its buffer is Q_{th} filled. By observing Q_{th} the child nodes stop sending the information to this node and the same procedure continues till the source node also observes that it can not disperse the information. ReCAIT tries to alleviate congestion at each hop during back propagation and thus does not require any explicit long lived congestion notification. Once the source node detects long lived congestion (Algorithm 3, L 2–8) it reduces the information rate. We rely on existing works for rate regulation, where commonly additive increase multiplicative decrease (AIMD) scheme is used. Once the source node detects congestion, multiplicative decrease is performed (Algorithm 3, L 10–11). AIMD additively increases the information rate once congestion is mitigated (Algorithm 3, L 12–13).

Algorithm 3 Long lived congestion control by ReCAIT

```
1  if (forwarding node) then
2      if (∀ q_o = Q_th) then
3          wait for time interval T;
4          for each neighbour node do
5              if q_{o_i} < Q_th then
                   transport(msg,Y_i,TRUE);
6          end
7      end
8  end
9  if source node then
10     if (∀ q_o = Q) and (ς < 1) then
11         infoRate[N_d,N_e,N_u]
           *=decInfoRate[N_d,N_e,N_u];
12     else if (∀ q_o ≠ Q) and (ς > 1) then
13         infoRate[SP] += incInfoRate[SP];
14     else if (∀ q_o ≠ Q) and (ς < 1) then
15         disperseInfo();
16 end
```

4.4 ReCAIT parameter acquisition

ReCAIT relies on different parameters to be available by sensor nodes. In order to maintain R_{hop}, a sensor node keeps track of the link quality in terms of bit error probability (BEP) between its neighbour nodes using EWMA approach as follows $R_{hop} = (1-\alpha) * R'_{hop} + \alpha * R_{hop}$, where R'_{hop} is the previous observation of R_{hop} and α is a weighting factor. In simulation environments BEP is readily available to sensor nodes. Other parameters such as t_o, t'_o, ξ_i and ξ_o are calculated similarly.

5 Performance evaluation

In order to evaluate our approach we first describe simulation settings and performance metrics. Next, we present and discuss the simulation results.

5.1 Simulation settings and performance metrics

We evaluate our approach based on simulations using TOSSIM (Levis et al., 2003) simulator. The general simulation settings are summarised in Figure 2.

Figure 2 Simulation settings

#Nodes	100
Node placement	Grid
Node distance	5 units
Effective comm. radius	7 units
Avg. hop distance	8
Message size	29 bytes
Q, Q_{TH}	36, 30
#Msgs generated	50
#Information nodes	4
α	0.1

We compared the ReCAIT with MMSPEED protocol (MMP) and RBC. We compared ReCAIT with MMP in order to observe the impact of on-demand and always available multiple paths. As the code for MMSPEED is not available for TOSSIM, we implemented its reliability module, i.e, MMP relying on details in Felemban et al. (2006). We also compared ReCAIT with RBC as it specifically provides reliable information transport in presence of high information rates. We compared the variants of ReCAIT, i.e., ReCAIT with no congestion control (ReCAIT-NoCC) and ReCAIT with only short lived congestion control (ReCAIT-SLCC). For underlying routing we utilised the default proactive routing protocol used by RBC, namely logical grid routing (LGR) (Choi et al., 2006) for fair comparison. We enhanced LGR to provide $h(X)$ and the list of one hop neighbours.

The performance of ReCAIT is measured in terms of responsiveness and efficiency. Responsiveness is defined as the information transport reliability and timeliness, while efficiency is mainly given by message complexity.

- *Reliability:* Information transport reliability is the ratio of amount of information entities received by the sink to the total amount of information entities generated.
- *Timeliness:* Timeliness is defined as the time elapsed from the generation of the first information entity to the arrival of the first information entity at the sink.
- *Efficiency:* Efficiency is measured in terms of message complexity. We define the message complexity as the total number of message transmissions required for the information transport (including the retransmissions).

5.2 Simulation results

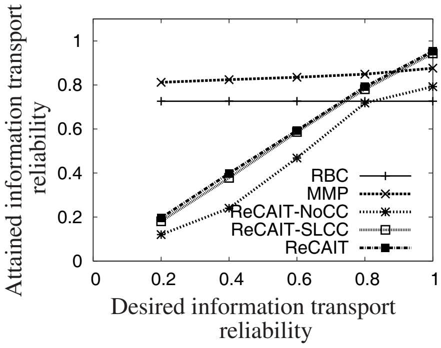
Now we present our simulation results for different studies that we conducted, i.e., tunable reliability, information rate, network conditions, number of nodes and number of information flows.

- *Tunable reliability of information transport:* First, we evaluate the performance of ReCAIT for tunable application requirements. In this study, we consider information rate equal to 10 msg/s. Figure 3(a) shows the tunability of the different protocols. Since RBC does not provide tunability it achieves a static reliability, which is lower than 1. Though RBC is developed specifically to cope with the bursty nature of information, it cannot handle high information rate. MMP also shows almost constant behaviour since it always tries to provide highest reliability. ReCAIT-NoCC is not able to fulfil tunability requirements since it starts dropping information due to congestion. ReCAIT and ReCAIT-SLCC fulfils the tunable reliability requirements despite the high information rate by dispersing the information on different neighbour nodes. This is also evident from Figure 3(b) where ReCAIT-SLCC shows more transmissions compared to ReCAIT-NoCC. MMP and RBC always have almost static number of transmissions. The number of transmissions for ReCAIT-SLCC and ReCAIT remains lower than MMP and comparable to RBC for application reliability 0.2 to 0.6, since it adapts #ret, suppresses information and utilises hybrid ACK. For reliability of 0.8 and 1.0 ReCAIT-SLCC and ReCAIT have higher number of transmissions which corresponds directly to the higher reliability achieved than any other protocol. Figure 3(c) shows the timeliness tradeoff for different protocols. For ReCAIT-NoCC the timeliness remains low, which corresponds to the low reliability attained. MMP shows lower latency than ReCAIT due to use of multiple paths.
- *Adaptation to information rate:* As the information rate impacts the congestion level, now we study how the different protocols adapt to increasing information rates. In this study, we assume that the application requires 0.8 reliability. Figure 4(a) shows that the ReCAIT-SLCC and ReCAIT adapt to the information rate better than all other protocols. At a low information rate, i.e., when there is less congestion RBC and MMP provide higher reliability than required and ReCAIT adapts to provide the required reliability and probabilistically suppresses the information. Similarly, ReCAIT-NoCC also provides desired reliability at low information rate. However, as soon as the information rate is increased MMP, ReCAIT-NoCC and RBC degrade whereas ReCAIT-SLCC and ReCAIT maintain the desired application reliability owing to adaptive spatial reuse. The reliability of MMP decreases because of the increasing information flow on multiple paths which result in more collisions and

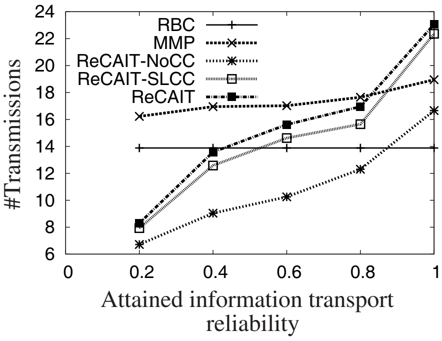
dropping of messages. RBC also fails to avoid congestion due to high information rate and starts to drop messages. Figure 4(b) shows the increase of transmissions for ReCAIT-SLCC and ReCAIT as it adapts to utilise multiple paths, i.e., Algorithm 2 to alleviate short lived congestion is triggered. We further observe that despite high information rate Algorithm 3 (long lived congestion) is not activated because the congestion build near the source nodes and remaining network is not congested. Therefore, splitting the information alleviates the congestion. The increasing number of transmissions indicates that the span of multiple paths is also increased with high information rate. It is noteworthy that the number of transmissions for all other protocols decreases with the increasing information rate. This is due to the fact that the protocols drop the information due to congestion. Similar effect can be observed for timeliness in Figure 4(c) where for RBC, MMP and ReCAIT-NoCC latency decreases which is directly proportional to reliability and dropped information. Whereas, ReCAIT-SLCC and ReCAIT follow split paths and local timer management resulting in high latency. It is also interesting to observe that the latency of MMP increases with high information rate. MMP utilises more paths due to less reliability across hops which results in longer paths.

- *Adaptation to network conditions:* We now investigate the impact of network perturbations. We consider an information rate of 10 msg/s and R_d = 0.8. Figure 5(a) shows ReCAIT-SLCC and ReCAIT effectively adapt to wireless link perturbations due to the fact that ReCAIT utilises the adaptive retransmissions and splits the information to multiple neighbours upon congestion. On the other hand RBC utilises fixed number of retransmissions and drops the information once congestion is encountered. Similarly, ReCAIT-NoCC and MMP also drop messages and do not provide the required information transport reliability as BEP increases. Figures 5(b) and 5(c) confirms the behaviour with growing number of transmissions and timeliness for ReCAIT-SLCC and ReCAIT. This shows a tradeoff between reliability, number of transmissions and latency corresponding to network conditions. We observe that at BEP 0.0 ReCAIT and its variants performs better than MMP and RBC with respect to number of transmission and latency, since it adapts to the application requirements. On the other hand, at higher BEP the number of transmissions increases resulting in higher latency to maintain the desired application reliability.
- *Adaptation to network size:* In this study, we show the scalability of ReCAIT for various number of sensor nodes. The information rate is 10 msg/s and R_d = 0.8. We vary the number of sensor nodes between 49, 81, 100, 141 and 196. Figure 6(a) depicts the attained reliability by ReCAIT and its variants. ReCAIT-NoCC deviates and provides less reliability when the number of sensor nodes increases. ReCAIT always provides application specific reliability despite an increasing number of sensor nodes by adapting localised mechanisms. We also observe that for lower number of sensor nodes, i.e., lower number of hops, ReCAIT attains application specific reliability by efficiently mitigating link congestion and using robust scheduling among the neighbour nodes. Figure 6(b) shows an increase in number of transmissions. For ReCAIT-NoCC the number of transmissions is relatively low because upon congestion messages are dropped which directly affects the attained reliability. Figure 6(c) illustrates the timeliness of the protocols and depicts the similar trend, i.e., high latency with increasing number of sensor nodes.

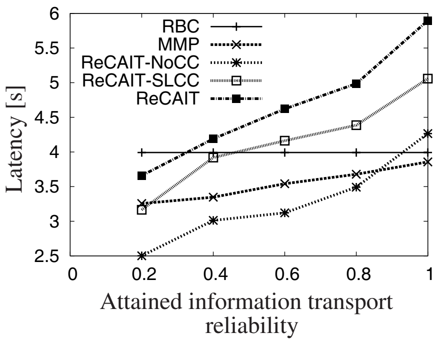
Figure 3 Tunable reliability of information transport, (a) reliability (b) efficiency (c) timeliness



(a)



(b)



(c)

- *Adaptation to number of information flows:* Figure 7 presents the performance results for 200 nodes where R_d = 0.8. The increasing number of concurrent information flows indicates that the information is flowing across the whole network. Figure 7(a) shows that only ReCAIT maintains the application specific reliability. As the number of information flows increase ReCAIT-SLCC and ReCAIT-NoCC reliability is decreased since the nodes around congestion spot are also loaded with other information flows. Accordingly, ReCAIT-SLCC and ReCAIT-NoCC starts dropping the messages with increasing number of information flows as depicted in Figure 7(b). We also observe that the number of transmissions for ReCAIT also decreases reflecting information rate adaptation at source nodes (Algorithm 3). Due to triggering of short lived and long lived congestion mitigation mechanisms the latency is also increased [Figure 7(c)].

Figure 4 Adaptation to information rate ($R_d = 0.8$), (a) reliability (b) efficiency (c) timeliness

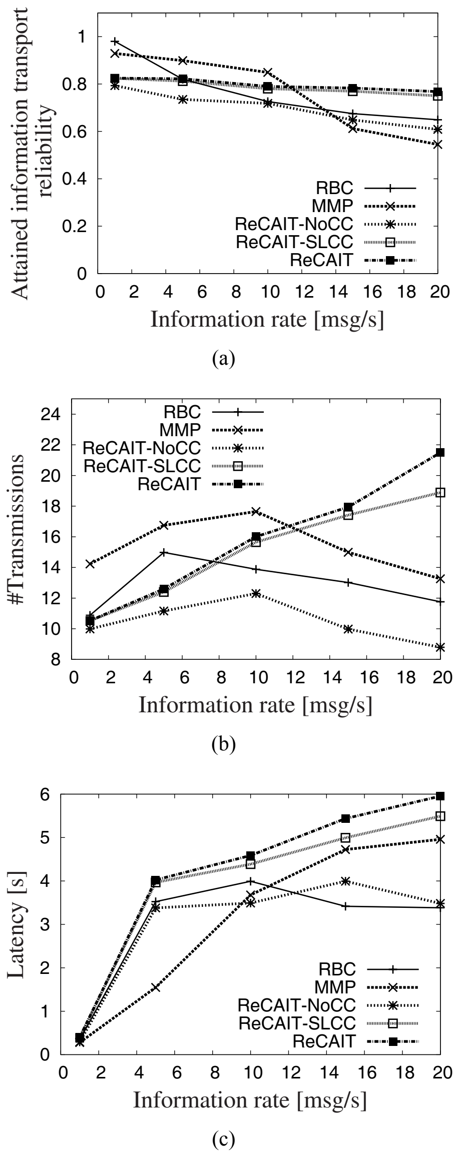
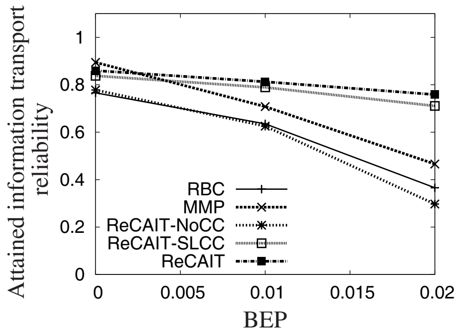
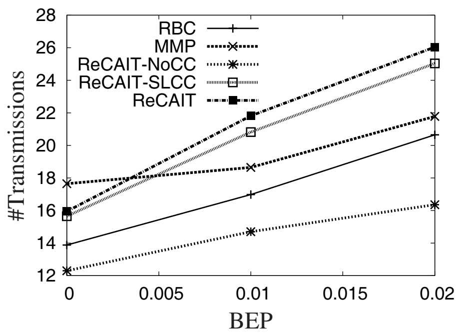


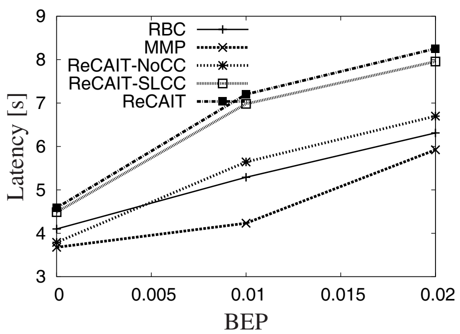
Figure 5 Adaptation to network conditions ($R_d = 0.8$), (a) reliability (b) efficiency (c) timeliness



(a)



(b)

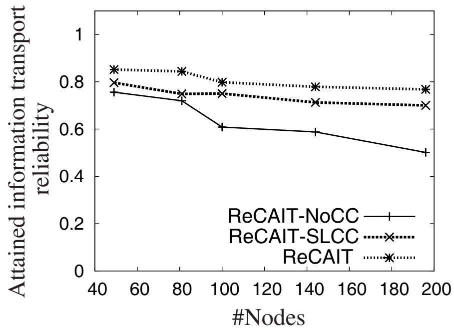


(c)

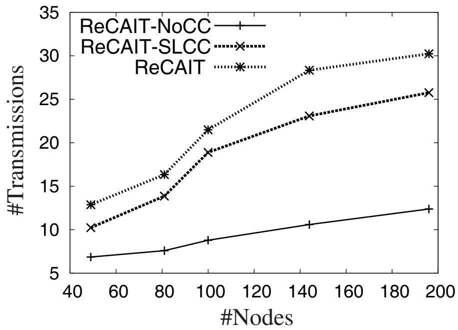
6 Conclusions

We proposed ReCAIT, a congestion aware tunable reliability approach for information transport in WSNs. ReCAIT maintains the desired reliability despite evolving network conditions by using adaptive retransmissions and suppressing unnecessary transmissions. Information loss is recovered by a hybrid ACK mechanism aided by adaptive retransmission timers. ReCAIT monitors the information flow and adapts between SP and multiple paths in order to alleviate congestion. If congestion persists ReCAIT utilises an implicit back pressure technique to reduce the information rate. The results confirm the capability of ReCAIT to adapt according to the application requirements and adaptability to information rate and changing network conditions.

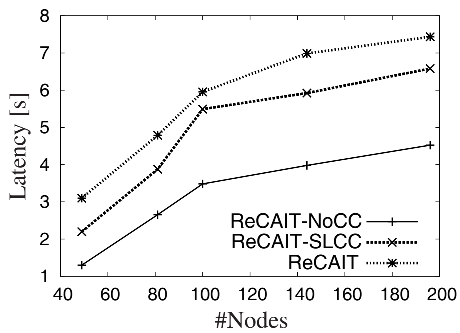
Figure 6 Adaptation to number of sensor nodes ($R_d = 0.8$), (a) reliability (b) efficiency (c) timeliness



(a)

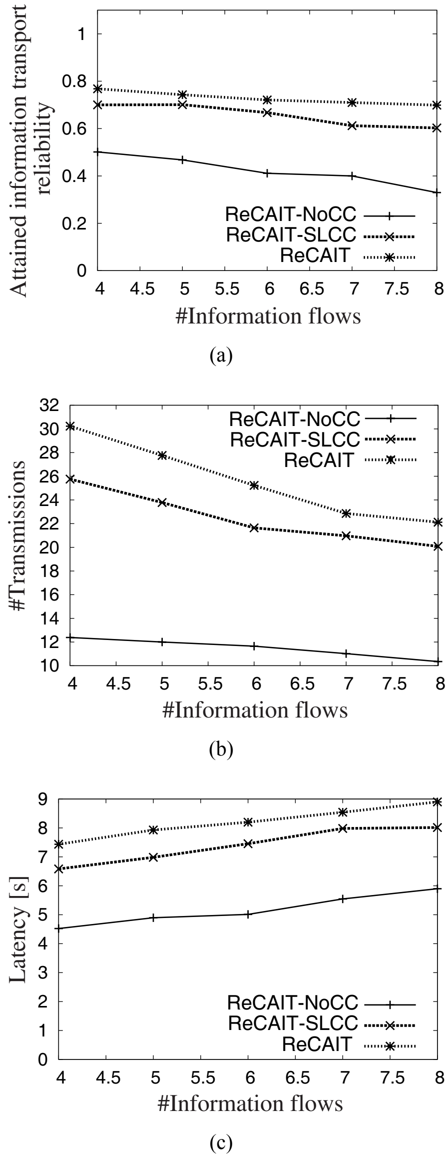


(b)



(c)

Figure 7 Adaptation to number of information flows ($R_d = 0.8$, #Nodes = 200), (a) reliability (b) efficiency (c) timeliness



(a)

(b)

(c)

Acknowledgements

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

References

Choi, Y. et al. (2006) 'Stabilization of grid routing in sensor networks', *Journal of Aerospace Comp., Inf. and Comm.*, Vol. 3, pp.214–233.

Deb, B. et al. (2003) 'Information assurance in sensor networks', in *Proc. of WSNA*, pp.160–168.

Felemban, E. et al. (2006) 'MMSPEED: multipath multi-speed protocol for QOS guarantee of reliability and timeliness in WSNs', *IEEE Trans. on Mob. Comp.*, Vol. 5, No. 6, pp.738–754.

He, T. et al. (2008) 'Alleviating congestion using traffic-aware dynamic routing in wireless sensor networks', in *Proc. of SECON*, pp.233–241.

Iyer, Y.G. et al. (2005) 'STCP: a generic transport layer protocol for wireless sensor networks', in *Proc. of ICCCN*, pp.449–454.

Jacobson, V. (1988) 'Congestion avoidance and control', in *Proc. of SIGCOMM*, pp.314–329.

Jaewon, K. et al. (2007) 'TARA: topology-aware resource adaptation to alleviate congestion in sensor networks', *IEEE Trans. on Par. and Dist. Sys.*, Vol. 18, No. 7, pp.919–931.

Kumar, R. et al. (2008) 'Mitigating performance degradation in congested sensor networks', *IEEE Trans. on Mob. Comp.*, Vol. 7, No. 6, pp.682–697.

Levis, P. et al. (2003) 'TOSSIM: accurate and scalable simulation of entire tinyos applications', in *Proc. of SenSys*, pp.126–137.

Marchi, B. et al. (2007) 'DTSN: distributed transport for sensor networks', in *Proc. of ISCC*, pp.165–172.

Paek, J. and Govindan, R. (2007) 'RCRT: rate-controlled reliable transport for wireless sensor networks', in *Proc. of SenSys*, pp.305–319.

Popa, L. et al. (2006) 'Reducing congestion effects in wireless networks by multipath routing', in *Proc. of ICNP*, pp.96–105.

Rahman, M.A. et al. (2008) 'Wireless sensor network transport layer: state of the art', in *Sensors: Adv. In Model., Design Issues, Fab. and Prac. App.*, pp.221–245.

Rangwala, S. et al. (2006) 'Interference-aware fair rate control in wireless sensor networks', in *Comput. Commun. Rev.*, Vol. 36, No. 4, pp.63–74.

Sankarasubramaniam, Y. et al. (2003) 'ESRT: event-to-sink reliable transport in wireless sensor networks', in *Proc. of MobiHoc*, pp.177–188.

Shaikh, F.K. et al. (2008) 'A comparative study for data transport protocols for wsn', in *Proc. of WOWMOM*, pp.1–9.

Stann, F. and Heidemann, J. (2003) 'RMST: reliable data transport in sensor networks', in *Proc. of SNPA*, pp.102–112.

Wan, C-Y. et al. (2003) 'Coda: congestion detection and avoidance in sensor networks', in *Proc. of SenSys*, pp.266–279.

Wang, C. et al. (2006) 'A survey of transport protocols for wireless sensor networks', *IEEE Net. Mag., Special Issue on Wireless Sensor Networking*, Vol. 20, No. 3, pp.34–40.

Wang, C. et al. (2007) 'Upstream congestion control in wireless sensor networks through cross-layer optimization', *IEEE Journal on Sel. Areas in Comm.*, Vol. 25, No. 4, pp.786–798.

Zhang, H. et al. (2005) 'Reliable bursty convergecast in WSNs', in *Proc. of MobiHoc*, pp.266–276.