EuroFGI Workshop on IP QoS and Traffic Control
P. Pereira (Ed.)
Lisbon, Portugal, December 6-7, 2007

END-TO-END RELIABILITY IN WIRELESS SENSOR NETWORKS: SURVEY AND RESEARCH CHALLENGES

Paulo Rogério Pereira*, António Grilo*, Francisco Rocha, Mário Serafim Nunes*, Augusto Casaca*, Claude Chaudet***, Peter Almström**** and Mikael Johansson******

* Inesc and IST/Technical University of Lisbon, Portugal; ** Inesc
e-mails: prbp@inesc.pt, Antonio.Grilo@inov.pt, Rocha.Francisco@gmail.com, {Mario.Nunes, Augusto.Casaca}@inesc.pt

*** GET, Groupe des Ecoles de Télécommunications, France
e-mail: Claude.Chaudet@enst.fr

**** KTH, Royal Institute of Technology, Sweden
e-mails: {peter.almstrom, mikaelj}@ee.kth.se

Keywords: Wireless Sensor Networks, Transport Protocols, Routing Protocols.

Abstract. *This paper presents a survey on transport and routing protocols for wireless sensor networks (WSN). Research challenges regarding the problem of end-to-end reliability are addressed in particular.*

1 INTRODUCTION

Wireless Sensor Networks (WSN)s are highly distributed self-organized systems. They rely on significant numbers of scattered low-cost tiny devices featuring strong limitations in terms of processing, memory, communications and energy capabilities. Sensor nodes collect measurements of interest over a given space, making them available to external systems and networks at special nodes designated sink nodes. In order to maximize the autonomy of individual nodes (and consequently the longevity of the network), power saving techniques are commonly implemented, causing nodes to sleep most of the time, complemented with low power communications that usually lead to multihop data transmission from sensor nodes to sink nodes and vice versa.

While link reliability mechanisms (e.g. MAC layer automatic repeat request – ARQ) can significantly reduce the end-to-end packet loss ratio, some critical WSN applications (e.g. battlefield surveillance applications, intrusion detection applications, or detection and tracking of chemical, biological, radiological, nuclear and explosive agents, etc.) require high or even total end-to-end reliability, demanding the use of a reliable transport layer protocol. On the other hand, some of these applications require packet-driven reliability (all packets sent by the source must reach the destination) while others only require event-driven reliability (the event must be detected, but it is enough that one notification message reaches the sink node).

Moving nodes and failing nodes due to battery power depletion are problems that raise a significant number of routing problems, demanding the use of efficient routing protocols. If the sensed information is to be used for active control (e.g. industrial process control) rather than passive monitoring, estimation and detection, the additional design goal of predictable latency appears [1]. Many control strategies can compensate for information delay and jitter (delay variations), provided that these can be deterministically bounded or statistically quantified in the design phase.

This paper presents a survey of transport and routing protocols for WSNs and identifies some research challenges. The next section analyses transport protocols. The following section addresses routing protocols and cross-layer solutions for industrial control. The final section summarizes the conclusions and points further research topics.

2 TRANSPORT PROTOCOLS FOR WIRELESS SENSOR NETWORKS

Proven transport protocols like TCP [2], designed to support user applications in infrastructure networks, usually present significant inefficiencies when employed without considerable modification in WSN systems. One of the main factors for TCP inadequacy is related with its strictly end-to-end reliability model, forcing all confirmations and retransmissions to follow the complete path between source and destination, with the consequent toll on the already scarce bandwidth and energy. Several proposals were made for alternative transport protocols, usually focused on specific optimization aspects and/or application scenarios.

An exhaustive list and analysis of transport protocols for WSNs can be found in [3] and [4]. WSN transport protocols can be broadly classified in two main functions: reliability and congestion control. In fact, these functions are related since congestion leads to packet dropping and hence to reduced reliability. Nevertheless, the majority of transport protocols only try to address one or the other directly (relegating the other function to a different protocol), while a few try to cover both functions. In this section we overview mainly the reliability function. Reliable transport protocols can be further subdivided into upstream (mostly unicast/convergecast transmission to aggregator or sink nodes) and downstream (mostly multicast/broadcast of code or configuration updates from sink nodes to sensor nodes). Table 1 presents a taxonomy of reliable transport protocols for WSNs.

It is a well established fact that providing some reliability support at intermediate nodes (hop-by-hop in the extreme) is more energy-efficient than treating reliability end-to-end only. This is one of the reasons why the traditional TCP mechanisms are not suitable (at least in the presence of unreliable links). Protocols designed with hop-by-hop reliability in mind are the following: PSFQ, RMST, GARUDA (two-tier, which can eventually be made hop-by-hop), DTC and DTSN.

The question may arise of whether hop-by-hop reliability at the transport layer can replace (and even be more efficient than) link-layer reliability at the MAC layer. This could be so if application data was the only traffic to benefit from link-layer reliability, but we must not forget that most routing protocols require a minimum reliability grade in order to achieve acceptable degrees of efficiency. Besides, the MAC layer provides other important functionalities, such as dealing with the hidden-terminal problem. On the other hand, implementing hop-by-hop reliability at the transport layer allows a swift response to route failures and may be used to support mechanisms to decrease congestion in medium access. All these factors point in the direction of a cross-layer design, where the MAC, routing and transport layers can coordinate to provide the reliability grades required by the different functions, while maximizing the energy-efficiency.

The hop-by-hop reliability model brings with it the issue of the security vulnerability of the transport layer, an issue that is seldom treated in the literature. Under this model, intermediate nodes in the end-to-end path are supposed to participate in data transport by caching and retransmitting data packets, generating or changing the contents of control packets (e.g. acknowledgements), etc. in order to avoid end-to-end retransmissions. This makes it impossible to implement full transport layer encryption between the sender and the receiver. But in this way, compromised intermediate nodes are given the possibility of tampering with the communication flow, for example perpetrating denial of service attacks by destroying the synchronization between the sender and the receiver while remaining concealed (e.g., changing the contents of some negative acknowledgements in protocols like DTSN or RMST to cause an additional recovery delay). Securing the transport layer must be done in a case-by-case basis and thus is still a promising topic for research.

Table 1: Reliable transport protocols for WSNs.

Transport Protocol	**WSN Direction**	**Loss Detection and Notification**	**Loss Recovery Control**	**Loss Recovery**	**Type of Reliability**	**Reliability Level**	**XCast**
PSFQ [5] Pump Slow Fetch Quickly	Downstream	NACK	Receiver node	Hop-by-hop	Packet-driven	Total (unless complete packet block lost)	Multicast / Broadcast (a variant allows Unicast)
ESRT [6] Event to Sink Reliable Transport	Upstream	Implicit	Sink establishes update frequency	End-to-end Redundancy: frequency of update messages	Event-driven	Partial	Unicast
RMST [7] Reliable Multi-Segment Transport / Directed Diffusion [8]	Upstream	NACK	Receiver node	Hop-by-hop	Packet-driven	Total (unless complete packet block lost)	Unicast
Erasure Code ([9])	Upstream	N.A.	N.A.	N.A.	Block-driven	Partial	Unicast
RBC [10] Reliable Bursty Convergecast	Upstream	ACK / NACK (Implicit ACK at MAC layer only)	Receiver node	End-to-end (Hop-by-hop at MAC layer only)	Packet-driven	Total	Unicast
GARUDA [11]	Downstream	NACK	Receiver node	Two-tier two-stage	Packet-driven / Destination-driven	> PSFQ due to Wait-for-First-Packet	Multicast / Broadcast
DTC [12] Distributed TCP Caching	Upstream	ACK, SACK	Receiver node (sink)	Hop-by-hop	Packet-driven	Total	Unicast
ART [13] Asymmetric Reliable Transport	Upstream (events) / Downstream (queries)	NACK (queries) / ACK (events)	Sender (ACK) or Receiver node (NACK)	End-to-end	Packet-driven / Destination-driven (queries)	Partial / Total	Multicast (queries) / Unicast
ATP [14] Ad-hoc Transport Protocol	Upstream	SACK	Receiver node (sink)	End-to-end	Packet-driven	Total	Unicast
STCP [15] Sensor TCP	Upstream	ACK / NACK	Receiver node (sink)	End-to-end	Event-driven / Packet-driven	Customizable	Unicast
DTSN [16] Distributed Transport for Sensor Networks	Upstream	ACK, SACK	Receiver node (sink)	Hop-by-hop	Packet-driven / Block-driven	Partial / Total	Unicast

Congestion has a significant impact on the performance of reliability transport protocols. The only transport protocols that support both reliability and congestion control are STCP and, indirectly, DTC. Although DTC was not developed as a solution to the congestion control problem, it relies on the TCP mechanisms. As to STCP, its end-to-end congestion control scheme mimics its limitation of end-to-end reliability. Both rely on end-to-end closed-loop rate adjustment, which is not good to deal with the frequent short term variations that frequently happen at intermediate points of routes in a multihop network. In order to constitute an effective answer to the congestion control problem, open-loop hop-by-hop backpressure mechanisms (like in e.g. PCCP [17], ARC [18]) are necessary, besides the already mentioned end-to-end regulation. Traffic differentiation is another important functionality to assure appropriate QoS to different applications.

Different kinds of sensorial data require different reliability grades. Partial reliability grades are considered in ESRT, ART, STCP, DTSN, as well as the erasure code techniques proposed by Kim et al [9] (specially suited for audio and imaging). ART and STCP include mechanisms that can be used to deliver differentiated reliability based on the fraction of confirmed packets, while erasure codes with different code rates constitute an alternative means of offering different reliability grades. ESRT considers a single reliability grade for all traffic. DTSN supports different grades of reliability. Total reliability is based on end-to-end Selective Repeat ARQ, coupled with caching of data packets at intermediate nodes so that the number of end-to-end retransmissions is minimized. For scalable bulk data transfer such as still image transmission, partial reliability can be achieved by the Enhancement Flow and Forward Error Correction (FEC) options. The Enhancement Flow option consists of buffering only a fraction of a block of data packets at the source (designated the core), being transmitted with total reliability (e.g. this may correspond to a minimum image resolution). The remaining data packets that constitute the block (e.g. image resolution increments) are granted no guarantees, since they are considered enhancement data. When coupled with intermediate caching and/or FEC, the Enhancement Flow is able to achieve high reliability grades while significantly increasing the throughput in comparison with the total reliability service. DTSN only provides the basic mechanism, not addressing how the size of the core can be adapted to keep a uniform reliability level in the presence of a highly variable link quality. The dynamic management of stable and differentiated reliability grades is still a subject for research.

While most of the WSN traffic is upstream by definition, some management and control tasks performed by the sink nodes involve downstream flows, possibly multicast/broadcast, with reliability requirements that vary with the specific application. Dynamic code update (DCU), re-configuration and querying are three important examples of such functions. PSFQ, GARUDA and ART (queries only) are designed to provide downstream multicast reliability. ART is the only one that explicitly considers both upstream and downstream reliable communication.

Almost all reliable transport protocols place the control of loss recovery at the receivers, ART and DTSN being an exception regarding the emission of ACK packets. Placing the control at the receiver enables continuous cleaning of the output queues at the sender, with a consequent increase in throughput. However, this strategy also increases the ACK / NACK overhead, with consequences in terms of energy efficiency. It is thus worth evaluating whether sender-controlled or receiver-controlled loss recovery is more suitable to a given WSN application.

Reliable transport protocols usually try to fit only one or two from the following types of reliability: event-driven, packet-driven, block driven. Of these, only the first is specific of WSNs, being usually associated with a data-centric networking paradigm (i.e. if several sensors report the same event, the transport protocol should guaranteed that at least one of those reports reaches the sink node). With the exception of ESRT and RMST, no transport protocol explicitly addresses reliability in data-centric WSN applications. In fact, none of the transport protocols mentioned in this paper is able to provide full reliability in data-centric WSN applications.

3 ROUTING PROTOCOLS FOR WIRELESS SENSOR NETWORKS

3.1 Routing protocols analysis

Even though transport layer may be granted several efficient reliability mechanisms, all these mechanics have a cost when triggered. That is why, even though one may argue that providing reliable end-to-end messages delivery falls into the attributions of the transport, and not the routing layer, in such a constrained environment, a conjoint optimization of all layers will help enhance the overall network performance.

Routing in the Internet usually relies on the assumptions that the network is hierarchically organized and addressed and that it is relatively stable. Except for Mobile IP and similar solutions, the topology is fixed and only varies when equipments suffer failures. Much work has been performed to enhance routing protocols in a mobile and distributed context, and the MANET IETF working group, in charge of standardization of a routing protocol for ad hoc networks has promoted four of the numerous proposals to the experimental RFC status a few years ago. Among these four proposals, OLSR [19] and AODV [20] seem to emerge as the probable future standards for proactive (i.e. link-state) and reactive (i.e. on demand, based on distance vector algorithm) protocols.

In a reliable sensors network context, though, these protocols require several modifications to reach the aforementioned objectives. First of all, no particular energy preservation consideration has influenced their design. In proactive protocols, several control packets are required to maintain an accurate vision of the network topology and in reactive protocols, the networks is flooded every time a new communication is initiated. Sensors networks are often considered to have a quasi-static topology and to have a convergecast traffic pattern, i.e. all flows involve the sink, or one of the sinks in the case of multiple data collection points, as a source or destination. There is no need for bringing a complete view of the topology to every sensor node. In most foreseen applications, keeping up-to-date one or several paths to the sink would be sufficient, allowing a drastic reduction of the routing tables sizes. In the extreme, simply applying the spanning tree protocol at the routing layer would provide the necessary convergecast tree. Concerning cleverer routing protocols, there is at least no need to frequently update the routing tables of the nodes.

However, things are never that simple. On one hand, nodes may be mobile, which is seldom considered, or the sink could be mobile, which represents a far more plausible scenario. There is therefore a need for routing table updates. On the other hand, a common energy preservation technique consists in putting nodes asleep when they do not need to play a particular role, router or emitter. Nodes may also disappear from the network when they have depleted their battery power. The question of distinguishing these events immediately arises, as they should not provoke the same reaction regarding routing.

There have been also numerous proposals for a routing protocol dedicated to the wireless sensor network environment. Some proposals, such as SPIN in its second version [21] modifies the route comparison criterion in the classical algorithms, replacing the classical hop count or delay by a measure of the energetic cost or by the remaining battery power of nodes on the route. Such strategies are usually efficient, SPIN-2 increases efficiency of the routing protocol by 60% at similar power consumption, but are tightly linked to the underlying hardware and its consumption characteristics. Another strategy consists in revisiting the routing scheme, alleviating the need to maintain routes constantly, for instance. Approaches such as Directed Diffusion [22] propose to let the data sink explicitly query the sensors by broadcasting an interest request. This flooding creates several reverse paths on the fly, allowing selected nodes to send back their measurement results. Geographic forwarding, for instance GPSR [23], has also been extensively studied, as it allows automatic addressing and routing of data frames as soon as the nodes are able to localize themselves.

Considering our objective, namely reliable end-to-end communication, the previously mentioned proposals lack several aspects. However, the question of what to do when an established path was broken arose very soon in the ad hoc networking community. Repairing a broken path may be realized by re-discovering a completely new path, by patching the existing route temporarily, or by using an alternate path. Every strategy has obviously its interests and costs in terms of performance, but also in terms of energy consumption. For example, SWR [24] examines strategies for local recovery while, following the classical Beyond BGP-like approaches, REAR [25] propose to use several redundant paths to link each sensor to the sink. This latest strategy obviously requires a k-connected connectivity graph.

The whole challenge lies in cost-effective identification and maintenance of these redundant paths in the presence of nodes performing regular sleep periods with coarse time synchronization. Many building blocks are already present in the literature, but to our knowledge no protocol has been proposed that solves the whole problem. We are currently investigating such issues and intend on identifying some bounds and feasibility results on the setup and maintenance of disjoint reverse broadcast trees routed at the sink.

3.2 Cross-layer solutions to reliable low-power industrial wireless sensor networks

One important application area for wireless sensor networks is industrial monitoring and control. The current interest in industrial wireless is driven by promises of increased productivity (enabled by real-time access to process data), decreased costs (from simpler commissioning, decreased downtime due to better condition monitoring, reduced cost of cabling, etc.) and improved control (allowing, for example, sensing in mobile and harsh environments). However, industrial control is an extreme application of wireless sensor networks, in the sense that packet latency, loss rates and energy consumption must all be kept at a minimum. It is important to understand that industrial control is not a single application with a single requirement, but rather a continuum: in an industrial plant, comprising thousands of sensors and actuators, sampling times might vary from hours (long-term production planning) to milliseconds (low-level control of industrial drive systems); monitoring applications might have graceful degradation with increased loss rates and latency while control applications can go unstable, causing expensive production stops.

The wireless control area is one of few in which standards are moving close to acceptance. In particular, the wireless HART and ISA-100 standards are supported by several of the major equipment manufacturers. To meet the goals of reliable low-power communications, the standards use a cross-layer approach comprising data link (MAC), networking and transport layers. The proposed protocol, Time-Synchronized Mesh Protocol, TSMP [26], is based on TDMA and maintains synchronization of the network on a node-to-node level (i.e., it does not employ beaconing) by piggybacking timing information on data and ACK packets. To increase overall spectral efficiency and robustness to frequency-dependent fading, nodes also use frequency hopping, utilizing a different channel at each transmission attempt (according to a pseudo-random schedule generated when the node joined the network). Each node in the system acts as a (full functional) mesh router that forwards packets towards their destination. Reliability is further improved by temporal and spatial diversity routing. Nodes attempt to maintain connectivity with at least two neighboring nodes, and forward packets on a FIFO-basis at the next available transmission opportunity. Should communication with one parent fail (for example, due to poor channel conditions), the next transmission attempt will be to another parent (and most likely on another channel), effectively using another path, realizing both spatial and temporal diversity.

Some of the many research challenges include evaluating TSMP for heterogeneous traffic (not only single-packet sensor data, but also applications where packet reordering plays a role), multiple traffic/QoS classes and prioritization of data when a node has multiple packets waiting to be transmitted; looking into the routing layer to see if one can combine the simple multipath routing algorithm with something that guarantees latency (e.g. putting a hop limit on forwarding paths).

4 CONCLUSIONS AND FURTHER WORK

Different WSN applications require different grades of reliability. Communication protocols for WSN should be *energy-efficient* to avoid useless wasting of energy resources through minimization of the control and retransmission overhead; should have *distributed functionality* to exploit the WSN resources in cooperative way, so that overall WSN operation is not hindered by the limited capacities of individual nodes; and should provide *reliability differentiation* to support different reliability grades in order to suit the requirements of different applications regarding throughput, latency and energy consumption.

The DTSN transport protocol addresses all these issues, supporting several reliability grades based on the integration of partial buffering at the source, intermediate node caching and erasure coding. Future work includes evaluating the performance of DTSN in different types of WSN applications, such as alarm and image transmission. The use of different underneath routing protocols is also of interest.

An additional topic of future research is the cost-effective identification and maintenance of redundant routing paths in the presence of regularly sleeping nodes. This study will be applied to the setup and maintenance of disjoint reverse broadcast trees routed at the sink.

A final future research topic, of importance to real-time industrial applications, is the study of latency guarantees for heterogeneous traffic. This study will be based on the use of the TSMP protocol. The analysis can then be generalized to different transport and routing protocols and application-level mechanisms can be designed to compensate for the variations of transmission delay.

ACKNOWLEDGEMENT

The authors acknowledge the research funding from IST FP6 UbiSec&Sens project and IST FP6 EuroFGI's E2E-WSN specific research project.

REFERENCES

[1] Sinopoli, B.; Schenato, L.; Franceschetti, M.; Poolla K. and Sastry, S. "Foundations of Control and Estimation over Lossy Networks". *Proceeding of the IEEE,* **95**(1):163-187, January 2007.

[2] Postel, J. "Transmission Control Protocol". IETF RFC 793, September 1981.

[3] Wang, C.; Sohraby, K.; Li, B.; Daneshmand, M.; and Hu, Y. "A Survey of Transport Protocols for Wireless Sensor Networks". *IEEE Network*, May/June 2006, pp.34-40.

[4] Wang, C.; Sohraby, K.; Hu Y.; Li, B. and Tang, W. "Issues of Transport Control Protocols for Wireless Sensor Networks". *Proceedings of International Conference on Communications, Circuits and Systems (ICCCAS)*, Hong-Kong, China, March 2005.

[5] Wan, C.Y.; Campbell, A.T. and Krishnamurthy, L. "PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks". *WSNA'02*, September 2002, Atlanta, Georgia, USA, pp. 1-11.

[6] Sankarasubramaniam, Y.; Akan, O.B. and Akyildiz, I. F. "ESRT: Event-to-sink Reliable Transport in Wireless Sensor Networks". *Proceedings of the ACM MobiHoc'03*, June 2003, Annapolis, Maryland, USA, pp. 177-188.

[7] Stann, F. and Heidemann, J. "RMST: Reliable Data Transport in Sensor Networks". *1st IEEE International Workshop on Sensor Net Protocols and Applications*, May 2003, Anchorage, Alaska, USA, pp. 1-11.

[8] Intanagonwiwat, C.; Govindan, R. and Estrin, D. "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks". *Proceedings of the 6th Annual International Conference on Mobile Computing and Networks (MobiCom)*, August 2000.

[9] Kim, S.; Fonseca, R. and Culler, D. "Reliable Transfer on Wireless Sensor Networks". *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor Ad-Hoc Communications and Networks (IEEE SECON 2004)*, Santa Clara, CA, USA, October 2004, pp. 449-459.

[10] Zhang, H. et al. "Reliable Bursty Convergecast in Wireless Sensor Networks". *Proceedings of the ACM MobiHoc'05*, Urbana-Champain, IL, USA, May 2005.

[11] Park, S.-J.; Vedantham, R.; Sivajumar, R. and Akyildiz, I. F. "A Scalable Approach for Reliable Downstream Data Delivery in Wireless Sensor Networks". *Proceedings of the ACM MobiHoc'04*, Roppongi, Japan, May 2004.

[12] Dunkels, A.; Alonso, J.; Voigt, T. and Ritter, H. "Distributed TCP Caching for Wireless Sensor Networks". *Proceedings of the 3rd Annual Mediterranean Ad-Hoc Networks Workshop*, Bodrum, Turkey, June 2004.

[13] Tezcan, N. and Wang, W. "ART: An Asymmetric and Reliable Transport for Wireless Sensor Networks". *Journal of Wireless Sensor Networks (JSNET)*, Vol. 2, No.3/4, pp. 188 – 200, 2007.

[14] Sundaresan, K.; Anantharaman, V; Hsieh, H. and Sivakumar, R. "ATP: A Reliable Transport Protocol for Ad-Hoc Networks". *Proceedings of ACM MobiHoc'03*, Annapolis, Maryland, USA, June 2003.

[15] Iyer, Y.; Gandham, S. and Venkatesan, S. "STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks". *Proceedings of IEEE ICCCN 2005*, San Diego, CA, USA, October 2005.

[16] Bruno Marchi, António Grilo, Mário Nunes. "DTSN – Distributed Transport for Sensor Networks". *12th IEEE Symposium on Computers and Communications (ISCC'2007)*, Aveiro, Portugal, July 2007.

[17] Wang, C; Sohraby, K; Lawrence, V; Li, B. and Hu, Y. "Priority-based Congestion Control in Wireless Sensor Networks". *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trutworthy Computing*, Taichung, Taiwan, June 2006.

[18] Woo, A. and Culler, D. "A Transmission Control Scheme for Media Access in Sensor Networks". *Proceedings of the ACM MobiCom'01*, Rome, Italy, July 2001.

[19] Clausen, T. and Jacquet, P. "Optimized Link State Routing Protocol (OLSR)". IETF RFC 3561, October 2003.

[20] Perkins, C.E.; Belding-Royer, E. and Das, S. "Ad hoc On-Demand Distance Vector (AODV) Routing". IETF RFC 3561, July 2003.

[21] Rabiner Heinzelman, W.; Kulik, J. and Balakrishnan, H. "Adaptive protocols for information dissemination in wireless sensor networks". *Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, Seattle, Washington, August 1999.

[22] Intanagonwiwat, C.; Govindan, R.; Estrin, D.; Heidemann, J. and Silva, F. "Directed diffusion for wireless sensor networking". *IEEE/ACM Transactions on Networking*, **11**(1):2–16, February 2003.

[23] Karp, B. and Kung, H. "GPSR: Greedy Perimeter stateless Routing for Wireless Networks". *Proceedings of the 6th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, 2000.

[24] Tian, D. and Georganas, N. D. "Energy Efficient Routing with Guaranteed Delivery in Wireless Sensor Networks". *IEEE Conference on Wireless Communications and Networking, (WCNC)*, March 2003.

[25] Hassanein, H. and Luo, J. "Reliable Energy Aware Routing In Wireless Sensor Networks". *Proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS'06)*, 2006.

[26] Dust Networks. "Technical Overview of Time Synchronized Mesh Protocol". White paper, http://www.dustnetworks.com/docs/TSMP_Whitepaper.pdf, June 2006.