Wireless Sensor Network survey

Sachin Gajjar

***Abstract*—**Wireless Sensor Networks have enormous potential because they expand human ability to monitor and interact remotely with the physical world. Smart sensors are able to collect huge amount of hitherto unknown data, which will pave the way for a new class of computing applications. Nevertheless, to exploit the full potential of sensor networks, we must first address the peculiar limitations of these special networks and the resulting technical issues. This paper presents factors influencing Wireless Sensor Network design followed by the issues and proposed solutions based on palette of protocol stack. The survey will help a reader choose the most appropriate protocol for his application and guide designers in defining new protocols tailored to specific applications of sensor networks. Finally, the survey establishes a framework for comparing existing Wireless Sensor Network protocols.

Keywords: Wireless Sensor Networks Design, Subsystems of Sensor Networks

I. Introduction

A Wireless Sensor Network (WSN) is a Network of sensors that senses specified parameter(s) related to environment; processes data locally in a distributed manner and wirelessly communicates information to central processing centers. The center analyzes information and initiates suitable response. The near-ubiquity of the Internet, the advancements in network build-out (particularly in the wireless environment) coupled with developments in VLSI technologies (enabling low-power, size, cost processors and memory) are in the aggregate opening the door to a new generation of low-cost sensors and actuators that are capable of achieving high-grade spatial and temporal resolution. Smart sensors are able to collect huge amount of hitherto unknown data, which pave the way for a new class of computing applications. Typical applications include, but are not limited to telemonitoring of human physiological data, habitat monitoring of wildlife, context aware homes, traffic monitoring, vehicle tracking and detection for battlefield surveillance, tracking and monitoring doctors and patients inside a hospital, environmental detection of fire and flood, microclimate monitoring for precision agriculture, and vibration-based structural condition monitoring [1]. The remainder of the paper is organized as follows: Section 2 discuss the hardware and software subsystems of sensor node. Section 3 gives the factors influencing the WSN design. Section 4 concludes the paper.

II. Factors influencing the WSN design

Factors influencing the WSN design are discussed in many literatures [2,3,4]. However, none of it gives a fully integrated view of all the factors influencing the WSN and sensor nodes. These factors are significant because they serve as a guideline to design and later on compare a protocol or an algorithm for WSN.

A. **Hardware constraints:** All the hardware subsystems of the node must fit into a coin-sized module, consume extremely low power, operate in high volumetric densities, be dispensable, autonomous and operate unattended.

B. **Network Reliability:** The sensor nodes are usually deployed in hostile environments where they may fail, die due to lack of power, physically damaged or face environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network.

C. **Time Synchronization:** The fusion of individual sensor readings and synchronization of sleeping cycles is possible only by exchanging messages that are time stamped by each sensor's local clock. This mandates the need for a common notion of time among the sensors through time synchronization.

D. **Scalability:** During the studying phenomenon nodes deployed may be on the order of hundreds or thousands. The number may reach an extreme value of millions depending on the application.

E. **Data aggregation:** For WSN using a cluster based approach data aggregation is collecting, filtering, and processing data in the network, and supplying the result to BS. The volatility of data must be considered to reduce wireless communication and minimize power usage of nodes.

F. **Topology control:** Protocols should extend the lifetime of dense ad hoc networks while preserving connectivity in hostile environment. The protocols should also conserve energy by identifying redundant nodes and turning them off.

G. **Power consumption:** Node's have limited power source and replenishment of power may be limited or impossible. The sensing, data processing and communication requires power aware protocols and algorithms.

H. **Self configurability:** WSNs will most likely be required to self-configure into connected networks.

I. **Dependability and QoS:** For these services such as congestion control, active buffer monitoring, acknowledgements, and packet-loss recovery are necessary to guarantee reliable packet delivery.

III. COMMUNICATION PROTOCOL

Like the traditional computer networks sensor networks can also be analyzed in terms of seven OSI layers. Addressing the issues at different layers decreases complexity and increases flexibility. Disadvantage is it increases memory requirements.

A. Physical Layer

The physical layer is responsible for deciding radio hardware, modulation, transmission and reception of signal and providing an interface for transmitting bit streams over the physical-communication medium. For a WSN, minimizing energy consumption and maximizing network lifetime starts at the physical layer. For this modulation schemes must be simple and low-power. Strategies must be used to overcome WL channel deficiencies like high bit error rate, signal attenuation and multipath fading. Radio hardware should be tiny, low-power, low-cost and robust.

Ref. [5]-[6], compares binary modulation and multi-level (Mary) modulation. M-ary modulation transmits symbols from a set of M distinct waveforms and binary modulation uses two distinct waveforms. For M-ary modulation, log2 M bits are sent per sample. While an M-ary scheme can reduce the transmit on-time by sending multiple bits per symbol, it results in complex circuitry and increased radio power consumption. It is concluded that M-ary modulation is more energy efficient than binary modulation when the startup time is short and the RF output power is small.

B. Data Link layer

The main functions of data link layer are Medium Access Control, framing, flow control, and error control. Traditionally the packet delay in MAC layer before it is transmitted; throughput; robustness; scalability and stability in handling traffic load fluctuations; fairness among competing nodes; efficient bandwidth utilization; energy efficiency have dominated the design of WSN MAC protocols. In WSN the main objective is to reduce energy waste caused due to collisions, idle listening, overhearing and excessive overhead. Next we discuss some representative WSN MAC layer protocols.

a) Berkeley media access control (B-MAC) [7]

It is a reconfigurable Carrier Sense Multiple Access (CSMA) protocol that achieves low power processing, collision avoidance, and high channel utilization. Based on the network load a set of adaptive bi-directional interfaces is used to reconfigure the protocol. For collision avoidance, B-MAC utilizes CCA to determine if the channel is clear. CCA searches for outliers in the received sample signals. An outlier exists if the channel energy is considerably below the noise floor. If an outlier is found during the channel sampling period, the channel is clear, else the channel is busy. If channel is busy, packet back-off is used. Back-off time is either initially defined or randomly chosen. For unicast packets B-MAC supports link-layer acknowledgement from receiver to sender. To reduce power consumption, B-MAC performs periodic channel sampling by cycling through awake and sleep periods. In the awake period, the node's radio is turned on to check for activities in the channel. If there are activities, it remains awake to receive the packet. On receiving the packet, it goes back to sleep. When the node is awake idle listening occurs but there is no activity in the channel. A timeout will force the node to go back to sleep. All B-MAC functionality such as acknowledgements, CCA, and back-off can be changed through a set of adaptive bi-directional interfaces. By enabling or disabling B-MAC functionality, the throughput and energy consumption of a node can change.

b) Z-MAC [8]

It is a hybrid MAC protocol that combines the strength of the TDMA and CSMA while compensates their weaknesses. It achieves high channel utilization and low latency under high contention; reduces collisions between two-hop neighbors at a low cost; is robust to dynamic topology changes and time synchronization. Z-MAC uses CSMA as the MAC scheme and TDMA schedule to enhance contention resolution. Unlike TDMA, a node may transmit during any time slot. It will always perform carrier sensing and transmit when the channel is clear. An owner of the slot will have higher priority over non-owners to access the channel. The goal is to allow the re-use of a slot when the slot owner is not transmitting data. By combing CSMA and TDMA, Z-MAC becomes more robust to timing failures, time-varying channel conditions, slot assignment failures, and topology changes.

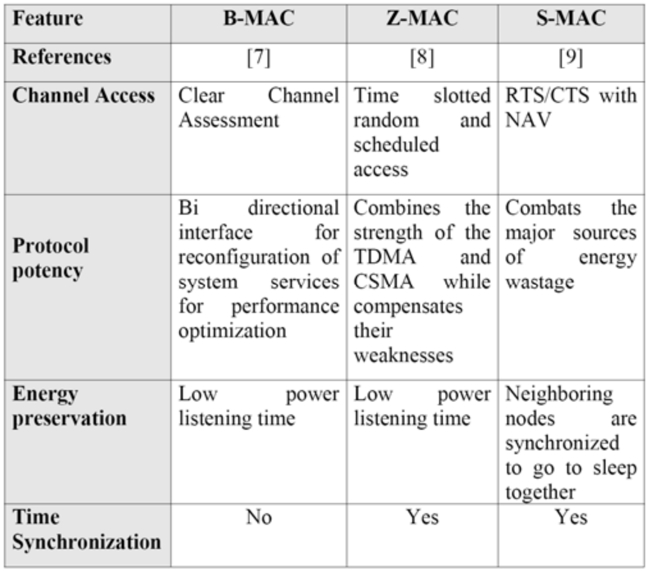
c) Sensor-MAC (S-MAC) [9]

It introduces three techniques to reduce energy consumption.

Periodic Listen and Sleep: During this phase neighboring nodes are synchronized to go to sleep together so as to avoid a heavy control overhead. They listen together and sleep together by exchanging schedules with their immediate neighbors. The nodes use RTS and CTS to talk to each other and contend for the medium if they want to communicate with the same node. Synchronized nodes form a virtual cluster and hence there is no inter-cluster communication problem. Synchronization is maintained by using SYNC packets which contain the sender's address and its next sleep time.

Collision and Overhearing Avoidance: There is a duration field in each transmitted packet which indicates how much longer the transmission will last. When a node receives a packet, it will not transmit any packets for at least the time that is specified in the duration field. This is recorded in a variable in the node called the Network Allocation Vector (NAV) which is reset every time the node received a packet whose duration field is larger than the current value. When the NAV is zero, the node can start transmitting packets. Overhearing is avoided by letting the nodes, which get RTS and CTS packets which are not meant for them, go to sleep. All immediate neighbors also go to sleep till the current transmission is completed after a sender or receiver receives the RTS or CTS packet.

Message Passing: Long messages are fragmented into smaller messages and transmitted in a burst. This is to avoid the high overhead and delay encountered for retransmitting when a long message is lost. ACK messages are used to indicate if a fragment is lost at any time so that the sender can resend the fragment again. The ACK messages also have the duration field to reduce overhearing and collisions. There is no contention to achieve fairness for each lost fragment. It is allowed to retransmit the current fragment but there is a limit on the number of retransmissions the node is allowed without any contention.



Feature	B-MAC	Z-MAC	S-MAC
References	[7]	[8]	[9]
Channel Access	Clear Channel Assessment	Time slotted random and scheduled access	RTS/CTS with NAV
Protocol potency	Bi directional interface for reconfiguration of system services for performance optimization	Combines the strength of the TDMA and CSMA while compensates their weaknesses	Combats the major sources of energy wastage
Energy preservation	Low power listening time	Low power listening time	Neighboring nodes are synchronized to go to sleep together
Time Synchronization	No	Yes	Yes

Table 1 Qualitative overview of representative MAC protocols for sensor network

C. *Network layer*

The functions of network layer are routing of data across the network from the source to the destination; internetworking with external network like Internet and localization. Routing protocols in WSN should meet constraints like communication BW; limited energy, memory and processing capability of node. It should also be robust against hostile environment; scalable; efficient; fault tolerant; fair; secure and use attribute-based and data-centric addressing.

a) Flooding [10]

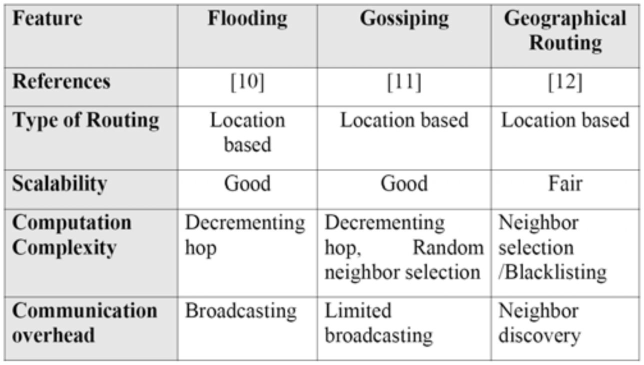
Each node receiving a packet broadcasts it, unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. Flooding is a reactive technique, and it does not require costly topology maintenance and complex route discovery algorithms. However, it has several deficiencies like duplicated messages are sent to the same node and is not energy efficient.

b) Gossiping [11]

A descendent of flooding is gossiping in which nodes do not broadcast but send the incoming packets to a randomly selected neighbor. A sensor node randomly selects one of its neighbors to send the data. Once the neighbor node receives the data, it randomly selects another sensor node. Although this approach avoids the packet duplication by just having one copy of packet at any node, it takes a long time to propagate the message to all sensor nodes.

c) Geographical routing [12]

It uses a greedy forwarding mechanism by choosing neighbors which are closest to the destination. It presumes that the network is dense; nodes are aware of their own and neighbors' location and multi-hop forwarding is reliable. Forwarding strategies proposed to improve the performance of geographic routing can be divided into two categories: distance-based in which node knows distance of its neighbors and reception-based where reception rates of neighbors are also known. Distance based forwarding consists of the original greedy forwarding and distanced-based blacklisting in which each node blacklists neighbors that are above a certain distance threshold from itself. The blacklist distance threshold is set as a fraction of a nominal radio range. In reception rate forwarding, each node forwards packets to the neighbor closest to the destination based on a minimum reception rate. A minimum reception rate must be met before two nodes can become neighbors. In Absolute reception based blacklisting node blacklists all neighbors that have a reception rate below a certain threshold. In Relative reception-based blacklisting node blacklists neighbors based on rank which depends on its distance to the destination and the reception rate. Best reception neighbor forwards packets to neighbors with the highest reception rate from the neighbors that are closer to the destination. In Best reception rate and distance the node computes this product value for all neighbors that are close to the destination. The neighbor with the highest product value will be chosen. Results in [12] show that reception-based forwarding strategies are more efficient than distance-based strategies.



Feature	Flooding	Gossiping	Geographical Routing
References	[10]	[11]	[12]
Type of Routing	Location based	Location based	Location based
Scalability	Good	Good	Fair
Computation Complexity	Decrementing hop	Decrementing hop, Random neighbor selection	Neighbor selection /Blacklisting
Communication overhead	Broadcasting	Limited broadcasting	Neighbor discovery

Table 2 Qualitative overview of representative Network layer protocols for sensor network

D. *Transport layer*

The transport protocol usually provides the following functions: orderly transmission, flow control, congestion control, packet-loss recovery; possibly QoS guarantee such as timing requirement and fairness; reliable end-to-end message transmission, where messages are fragmented to chains of segments at senders and reassembled at receivers. For WSN development of a transport layer protocol should be generic and independent of the application; it must consider the convergent nature of upstream traffic (node to BS); should provide variable packet reliability as different applications tolerate different levels of packet loss. Packet loss may be due to channel's high bit error rate, congestion, packet collision, receiver's full memory capacity, and node failures resulting in wasted energy and degraded QoS. It must identify the cause of loss and take appropriate action. Among the transport protocols designed for WSNs some address congestion or reliability only, others examined both of them.

a) Sensor transmission control protocol (STCP) [13]

It is a generic end-to-end upstream (nodes to BS) transport protocol for WSNs. It provides variable reliability; congestion detection and avoidance; multiple applications support in the same network. Majority of this work is done at the BS. BS is assumed to have high processing capability, storage, and power to communicate with all the nodes in the network. Before sending data source node must transmit a single session initiation packet which contains information about the number and type of data flows from the node, transmission rate, and required reliability to the BS. Source node then waits for an ACK from the BS before transmitting data. For uninterrupted data flows, the BS estimates the time of arrival of each packet from each source. If a packet is not received within a given period of time, it determines whether the current required reliability is met. Reliability is a measure of the fraction of packets that are successfully received. If current reliability goes below the required level, BS sends out a NACK to the source node for retransmission. Each source node stores its transmitted packets in a buffer. When the buffer reaches a threshold, it is cleared. For event-driven flows, the source node computes the reliability of the packet reaching the BS. If the computed value is more than the required reliability, the node will not buffer the packet to save storage space. The BS sends out positive ACK for each packet received from a source node. When an ACK reaches the source node, the corresponding transmitted packet is deleted from the buffer. Every sensor node maintains two thresholds in its buffer: low and high thresholds. When the buffer reaches the lower threshold, the congestion bit is set with a certain probability. Once the buffer reaches the higher threshold, the congestion bit is set for all packets. The congestion bit is a flag informing the BS to either notify the source to reduce its transmission rate or re-route packets along a different path.

b) GARUDA [14]

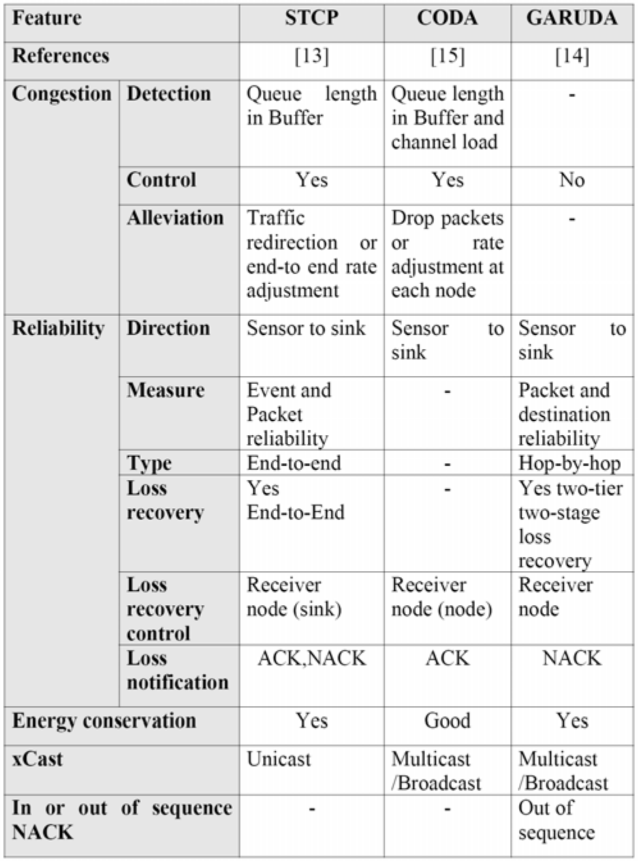
It is a reliable downstream (BS to nodes) data delivery transport protocol for WSNs. Reliability is defined in four categories: (1) Guarantee delivery to the entire field, (2) Guarantee delivery to a sub-region of sensors, (3) Guarantee delivery to a minimal set of sensors to cover the sensing region, and (4) Guarantee delivery to a probabilistic subset of sensors. GARUDA's design is a loss-recovery core infrastructure and incorporates a two-stage NACK-based recovery process. The core infrastructure is constructed using the first packet delivery method that guarantees first packet delivery. This is done using a Wait-for-First-Packet pulse which consists of small finite series of short duration pulses sent periodically by the sink. Sensor nodes within the transmission range of the sink receive this pulse and wait for the transmission of the first packet. The first packet delivery determines the hop-count from the sink to the node. Nodes along the path can become candidates for the core. A core candidate elects itself to be a core node if it has not heard from neighboring core nodes. In this way, all core nodes are elected in the network. An elected core node must then connect itself to at least one upstream core node. Out-of-order forwarding is used which allows subsequent packet to be forwarded even when a packet is lost. GARUDA uses a two-stage loss-recovery process. In the first stage core nodes recover the packet. When a core node receives an out-of-sequence packet, it sends a request to an upstream core node notifying about missing packets. The upstream core node receiving the message will respond with a unicast retransmission of the available requested packet. The second stage is the non-core recovery phase, which involves non-core nodes requesting retransmission from the core nodes. A non-core node listens on all retransmissions from its core node and waits for completion before sending its own retransmission request.

c) Congestion detection and avoidance (CODA) [15]

It is congestion control for upstream convergent traffic in WSN. CODA uses three mechanisms: congestion detection; hop-by-hop backpressure; and multi-source regulation. Congestion detection is done by monitoring buffer occupancy and measuring channel load. When buffer occupancy is high, nodes listen to the local channel load conditions to detect congestion. On congestion detection, the sensor node broadcasts a suppression message to its neighbors and a backpressure message upstream to the source. Each upstream node receiving the backpressure message determines whether or not to propagate the message. Depending on the congestion policy, a node can prevent further congestion build up by dropping the incoming data packets or adjust their sending rate. In the event of a persistent congestion, CODA uses a closed-loop multi-source regulation method to pronounce congestion control over multiple sources from the sink. When the source node event rate is less than some fraction of the maximum theoretical throughput of the channel, the source regulates its own rate. When this value exceeds, the source node is most likely to be contributing to congestion. In this condition, the source enters sink regulation and the sink sends a message to the source with a pre-defined computed event rate. When congestion is relieved, the sensor node would then regulate itself again without the sink.

IV. CONCLUSION

Unlike other networks, WSNs are designed for definite applications. Applications include, but are not bounded to military; indoor and outdoor environmental monitoring; human health monitoring; logistics control. Each application has different characteristic and requirement. To support this variety of applications, the development of new communication protocols, algorithms, hardware designs, and services are needed. The new developments need to satisfy the constraints introduced by WSN factors such Hardware constraints; Network Reliability; Time Synchronization; Scalability; Data aggregation; Topology control; Power consumption; Self configurability;



Feature		STCP	CODA	GARUDA
References		[13]	[15]	[14]
Congestion	Detection	Queue length in Buffer	Queue length in Buffer and channel load	-
	Control	Yes	Yes	No
	Alleviation	Traffic redirection or end-to end rate adjustment	Drop packets or rate adjustment at each node	-
Reliability	Direction	Sensor to sink	Sensor to sink	Sensor to sink
	Measure	Event and Packet reliability	-	Packet and destination reliability
	Type	End-to-end	-	Hop-by-hop
	Loss recovery	Yes End-to-End	-	Yes two-tier two-stage loss recovery
	Loss recovery control	Receiver node (sink)	Receiver node (node)	Receiver node
	Loss notification	ACK,NACK	ACK	NACK
Energy conservation		Yes	Good	Yes
xCast		Unicast	Multicast /Broadcast	Multicast /Broadcast
In or out of sequence NACK		-	-	Out of sequence

Table 3 Qualitative overview of representative Transport layer protocols for sensor network

Dependability and QoS. Many researchers are currently engaged in developing the technologies needed for different layers of the sensor networks protocol stack. We have summarized and compared different proposed aim to give more insight into the problems and intend to motivate a search for solutions and close the gap between technology and application making sensor networks an integral part of our lives.

V. References

[1] Mohammad Ilyas and Imad Mahgoub, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press Publication, ISBN 0-8493-1968-4, 2004.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey”, Computer Networks Vol. 38 , Elsevier Science Pub., pp. 393–422, 2002.

[3] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “Wireless sensor network survey“, Journal of Computer Networks, ScienceDirect, 2008.

[4] Kazem Sohraby, Daniel Minoli, Taieb Znati, “Wireless Sensor Networks: Technology, Protocols and Applications”, John Wiley, 2007.

[5] E. Shih et al., “Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks,” Proc. ACM MobiCom ’01, Rome, Italy, July 2001, pp. 272–86.

[6] A.Y. Wang, S. Cho, C.G. Sodini, A.P. Chandrakasan, Energy efficient modulation and MAC for asymmetric RF microsensor systems, in: Proceedings of the ISLPED’01, Huntington Beach, CA, 2001.

[7] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proceedings of the Sensys’04, San Diego, CA, 2004.

[8] H. Dubois-Ferriere, D. Estrin, M. Vetterli, Packet combining in sensor networks, in: Proceedings of the Sensys’05, San Diego, CA, 2005.

[9] W. Ye, J. Heidemann and D. Estrin, “Medium Access Control with coordinated adaptive sleeping for wireless sensor networks” IEEE/ACM Transactions on Networking, Vol. 12, No. 3, June 2004, pp. 493-506.

[10] P. Downey and R. C. Oliver. Evaluating the impact of limited resource on the performance of flooding in wireless sensor networks. International Conference on Dependable Systems and Networks, Jul.2004.

[11] S. Hedetniemi, S. Hedetniemi, and A. Liestman, “A Survey of Gossiping and Broadcasting in Communication Networks,” Networks, vol. 18, 1988.

[12] K. Seada, M. Zuniga, A. Helmy, B. Krishnamachari, Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks, in: Proceedings of the Sensys’04, Baltimore, MD, 2004.

[13] Y.G. Iyer, S. Gandham, S. Venkatesan, STCP: a generic transport layer protocol for wireless sensor networks, in: Proceedings of the 14th IEEE International Conference on Computer Communications and Networks, San Diego, CA, 2005.

[14] S.-J. Park, R. Vedantham, R. Sivakumar, I.F. Akyildiz, A scalable approach for reliable downstream data delivery in wireless sensor networks, in: Proceedings of the ACM MobiHoc’04, Roppongi,Japan, 2004.

[15] C.-Y. Wan, S.B. Eisenman, A.T. Campbell, CODA: Congestion detection and avoidance in sensor networks, in: Proceedings of the Sensys, 2003.