

Beyond Sensor Networks: ZUMA Middleware

Mikael N. K. Soini, Jana Van Greunen, Jan M. Rabaey, and Lauri T. Sydanheimo

Abstract—Most wireless sensor network (WSN) proposals are unrelated to multimedia and other smart home infrastructures. This paper combines these issues and presents a solution where the Kilavi sensor network platform can be used as middleware to provide information for ZUMA. Kilavi is a centralized protocol designed for communication between high capacity management point and low capacity sensor nodes in building environment. ZUMA is a centralized future smart-home platform that interconnects all kinds devices in the home environment. This paper mainly focuses on sensor network operation issues. The discussion is on the benefits that the centralized architecture can provide in typical sensor network operations that are node discovery, routing and data dissemination, power control, and security. To support the discussion, the paper gives numbers that illustrate the benefits that centralization has over typical decentralized WSN solutions in home environment.

Index Terms—Middleware, Smart home, Network performance and evaluation, Wireless sensor networks

I. INTRODUCTION

IN the past two decades, the home environment has been transformed by the digital revolution. This revolution was started by the spread of personal computers into the home space. Lately it has been fuelled by an explosion in the number of personal electronic media and communication devices, as well as sophisticated media capturing, storage and playback entertainment devices. Personal electronic devices include cellular phones, mp3 players, and PDA's, while entertainment devices include DVD players, Digital Video Recorders (DVR), and advanced sound systems.

Advances in the electronics industry have also driven growth in several areas related to home entertainment, including surveillance, home automation products (e.g. lighting, heating, and power), home appliances (e.g. laundry machines, fridges), and ad-hoc wireless sensor networks (AWSN), which promise to add a truly ambient intelligent

Manuscript received January 2, 2006. This work was supported by Tekes and European Regional Development Fund (ERDF) under ILTa project. The ZUMA project is funded by the Gigascale Systems Research Center www.gigascale.org.

M. N. K. Soini is with Tampere University of Technology, Electronics Institute, Rauma Research Unit, Rauma, Finland; phone: +358445341513; fax: +35828240189; e-mail: mikael.soini@tut.fi.

J. Van Greunen is with Berkeley Wireless Research Center, University of California Berkeley, Berkeley, CA, USA; e-mail: janavg@eecs.berkeley.edu.

J. M. Rabaey is with Berkeley Wireless Research Center, University of California Berkeley, Berkeley, CA, USA; e-mail: jan@eecs.berkeley.edu.

L. T. Sydanheimo is with Tampere University of Technology, Electronics Institute, Rauma Research Unit, Rauma, Finland; e-mail: lauri.sydanheimo@tut.fi.

component to the home. The future home clearly represents an opportunity for the convergence of these different technologies far beyond the level of integration seen today.

The potential of ubiquitous wireless connectivity promises to dramatically change the landscape in how these devices are operated and used. Most media devices today operate in stand-alone mode, or at most operate in isolated clusters of networked elements. The possibility of dynamically connecting a variety of components opens the door for exciting new opportunities and enhanced user experiences. The future home is likely the place where these technologies will come to fruition first.

References [1, 2] present a platform for the smart-home, called ZUMA. The main properties of ZUMA are enumerated below:

- Zero-Configuration: minimal device configuration
- Universality: ability to connect any device to any other device
- Multi-User Optimality: optimized user experience, in the presence of multiple users and simultaneous tasks
- Adaptability: the platform has the ability to change according to users' desires, presence, and new devices

Sensor networks are a crucial component of the home platform. They provide the *Ambient Intelligence* component that will be used by all other components to determine conditions and occupant preferences inside the house. Until recently, the academic approach to sensor network design has advocated an ad-hoc, completely distributed network. In this paper, we argue that this decentralized architecture is not the most desirable for a home-based sensor network deployment.

In a home environment the sensor network must be easily deployable, manageable and upgradeable. While a centralized approach is not as scalable as a distributed one, this has not been found to be a problem for sensor network deployments. Reference [3] found that in sensor network implementations, even relatively large ones [4, 5], nodes mostly perform continuous data acquisition, and incorporate little or no on-mote processing. These systems are centralized in practice, but have none of the management benefits of centralized systems.

Moreover, delegating network management to an infrastructural element may not turn out to be a severe restriction. The home infrastructure can be made compute-powerful with plentiful storage capacity. In addition, although centralization usually decreases fault tolerance (there is a single point of failure), in this case, the centralized sensor node is part of a larger, more robust infrastructure, which is not likely to fail often. This is similar to Ethernet networks.

Although the central Ethernet switch may fail, in practice it is robust enough that this is a very rare event.

A centralized architecture has a single point for network management. We propose infrastructure devices capable of managing dataflow through the sensor network and handling complex processing. Thus, the sensor nodes will be able to act simply as data forwarders. This is sensible from an economic point of view as it allows sensor peripherals to be inexpensive and allows greater flexibility in protocol selection.

This paper introduces the Kilavi sensor network platform. Kilavi, as part of the ZUMA infrastructure, assumes a central approach. The Kilavi platform was developed at the Tampere University of Technology, Finland and consists of a physical sensor node platform in addition to a gateway device that manages the network. For more detailed information on the Kilavi platform and protocols; please see [6, 7]. There are many issues that affect sensor network operation. Due to space constraints only a few of them have been chosen for evaluation. Issues such as power consumption, response time, and fault tolerance are not discussed in depth in this paper.

The main contribution of this paper is to compare the centralized Kilavi approach to traditional distributed sensor networks, focusing specifically on:

- Localization and Synchronization
- Node Discovery
- Routing and data dissemination
- Power control
- Security

The rest of the paper is organized as follows. Section II gives an overview of the ZUMA, followed by a discussion of related work in section III. Section IV presents the Kilavi platform and it is evaluated against other sensor network platforms in Section V. Section VI discusses the benefits of integrating Kilavi into the ZUMA platform. Finally, section VII concludes the paper.

II. THE ZUMA PLATFORM OVERVIEW

From the top-down, a set of ZUMA abstractions were devised that make it easy to deploy and execute applications on the platform. From the bottom-up, [1] describes a strategy to seamlessly connect devices with varied interface formats, effectively accomplishing the *Universality* goal of ZUMA.

First, the top-down component describes an environment abstraction for users, content, and devices. The current environment can be characterized in terms of *personae*, *capabilities*, and *content*. The platform enables configuration and interaction between components in the environment.

The sensor network plays a very important role in gathering this environment information. For example, sensor networks can localize people, track objects in space and monitor temperature and other variables. While the presence of a person may change a sensor network application, for example, turn the heater on if people are home, it may also affect

multimedia applications like TV watching.

From the bottom up, we introduce the concept of the *Universal Contents Router (UCR)*. The UCR is a network overlay solution, which employs bridges to provide connectivity. This connectivity is not reduced to the physical or even transport-level, i.e., “provision of byte streams”. Rather, it encompasses the concept of exchanging semantically interpretable units of content, resulting in interoperability at the presentation or (partially) the application layers. Any device in the system must be logically accessible by all other devices. Reference [1] spells out functions that a UCR should support, discusses its architecture and presents a first-order prototype.

III. RELATED WORK

There have been several other research projects that focus on the future home. Due to space limitations, we present those that have a significant sensor network component. Most projects define sensor network middleware that describe a high-level API or programming language, augmented by algorithm descriptions of varying detail.

Perhaps the most well known sensor network abstraction is that of the database. According to this model, writing SQL queries (to gather data) programs the network. TinyDB/tiny aggregation service (TAG) [8] is an example. This model optimizes data extraction (query returns). However, the queries are not optimized and are often simply flooded.

jWebDust middleware [9] defines an N-tier application model: (i) the Sensor Tier that consists of a wireless sensor network (ii) the Control Tier that corresponds to the control centers where events are reported, (iii) the Data Tier responsible for storing sensor data, (iv) the Middle Tier that is responsible for processing the data, and (v) the Presentation Tier that interfaces the information. The structure given to the network is similar to what we propose. However, in our case, the control tier controls and optimizes data flow in the network by calculating query and data routes. Also, the higher tiers of Kilavi are closely integrated with other home networks through the ZUMA platform.

Abstract programming [10] and Hood [11] both describe higher level programming languages for sensor networks based on a local neighborhood. The projects aim to optimize in-network data processing & data fusion to reduce communication. Similarly, the Milan [12] middleware proposes an algorithm to explore the tradeoff between in-network processing and communication. Reference [13] describes a distributed resource discovery algorithm using clustering and leader election. This algorithm will be compared (below) to the central approach taken in this paper.

IV. KILAVI OVERVIEW

Kilavi is a simple and low data-rate communication protocol for building environments. Altruist nodes located, for example to power outlets, are utilized as intermediate nodes when possible to enhance network operation and lifetime. The

centralized architecture simplifies the network operation by allowing us to concentrate resources and capabilities on a single central node that simplifies used security architecture, interface to external networks, and structure and operation of the sensor nodes. This central node is part of the ZUMA UCR infrastructure.

The Kilavi network can be either a single-hop or multi-hop network. Multi-hopping utilizes high power capacity intermediate nodes to relay data between sensors and the central node. Intermediate nodes also operate as short-term data stores to hold packets until the sensors query them.

A. Physical Platform

Kilavi node is implemented around MSP430F147 microcontroller and nRF905 single channel radio with BPSK keying, 50 kbps data rate, 434 MHz communication frequency, and adjustable output power. The Kilavi uses 48-bit control packets (RTS/CTS/ACK/QUERY) and short variable size data packets (usually about 100 bits).

In the Kilavi test bed, the central node is attached to a computing device that includes a DSP processor with 16-Mbit flash memory, Ethernet, Bluetooth and serial interfaces. This device provides both local (touch panel) and remote (cellular) user interfaces. Several users can simultaneously access the sensor network.

B. Security

The security is implemented with end-to-end keys in Kilavi. The initial key exchange is enabled through a special registration device. The RC5 encryption algorithm in counter mode and CBC-MAC (Cipher Block Chaining Message Authentication Code) is used to achieve data confidentiality, freshness, replay protection, and authentication. The following RC5 parameters are used: 32-bit word size, 12 rounds, 128-bit key length, and 32-bit counter length. The MAC length is 32 bits.

C. Routing

The central node is responsible of routing in Kilavi. Routes are calculated when a sensor node floods a *Route Search* message into the network. The routing metrics are the hop count, network load, and node energy capacity. Intermediate nodes do not route but rather forward messages based on the information included in every multi-hop packet. When a route creation message is forwarded, intermediate nodes increase the hop count and add their addresses to the message.

Changes in the network are detected when: 1) a sensor node does not receive an acknowledgement for a data/query message, 2) the central node does not receive data with a query, or 3) the central node detects a change during a periodic route update. When a sensor detects that it cannot connect to the central node, it sends out a new *Route Search* message. On the other hand, if the central node detects a change in topology it sends a *Route Request* message. This message can be sent to a specific sensor node, or to all nodes in the network. When a sensor receives a *Route Request*, it responds by flooding the network with a *Route Search* message.

D. Adding a Node to the Network

When a node is added to the network the following registration procedure is performed. 1) Initial security key is transferred from the central node to a new sensor, 2) the sensor floods a *Registration Request* to the network, 3) the central node receives the request, calculates the optimal route and sends *Registration Challenge* to the sensor, 4) the sensor sends *Registration Response* to the central node, 5) the central node sends *Registration Confirmation* to the sensor (initial MAC key is created), 6) the sensor returns *Registration Acknowledgement* to the central node, and 7) the sensor starts using predetermined route for communication. During this process K_{mac} and K_e keys are created for MAC and encryption, with C&R protocol and counter synchronization

V. EVALUATION

This section compares centralized and distributed WSN management. Due space limitations, the following issues have been chosen: localization, synchronization, node discovery, routing (data dissemination), Medium Access Control, and security. Comparing different protocols is difficult because these protocols have usually been evaluated using different methods and parameters, and many publications do not offer sufficiently up-to-date information for accurate comparison. This limited the selection of protocols used for comparison in this paper.

A. Localization and Synchronization

Localization and synchronization in sensor networks often rely on cooperative algorithms for unknown nodes to find their locations/time and a few reference nodes. This cooperation incurs an overhead cost and outsourcing it to a central node reduces in-network computation, communication and may also improve accuracy.

Localization for sensor networks can be divided into three categories: centralized, distributed, and beacon based. This paper considers the communication cost for these algorithms. In a centralized algorithm, described in [14], all nodes send a list of their neighbors to a central node. The communication cost is routing a packet for each node to the central node. If there are N nodes and the average path length is k the cost is $N \cdot k$. For the beacon approach [15], beacons are placed at regular intervals and nodes expend energy receiving messages. Third, the simplest distributed algorithm is DV-HOP [16] where nodes with known positions flood the network and distance is calculated by considering the number of hops. Reference [17] found that DV-HOP had a communication overhead of 10x compared to a beacon scheme and 6x to flooding the network.

Many sensor network synchronization schemes already use a master/slave configuration, for example, [18] and [19]. Centralized infrastructure could use any of these schemes, and it eliminates the overhead of finding a master node.

B. Discovery

There are three components to resource discovery. First,

when a new node joins the sensor network, it registers by advertising its own resources. Second, the node may discover available sensor network resources. Third, resource information must be maintained. The centralized architecture reduces the overhead by making the information easy to find/update. Nodes already know where the resource repository is, and less energy is wasted both in flooding the network to find services.

Kilavi stores all resource records on the central node. These are periodically refreshed when nodes update their status by either a Unicast packet, or flooding the network, which combines gathering routing information with discovery. In comparison, the Milan [12] specifies the use of the Service Discovery Protocol (SDP).

Without an explicit structure for directory agents, SDP queries must be flooded to the network. Dynamic Resource Discovery (DRD) [13] uses a clustering algorithm to improve discovery. Nodes elect a local cluster head. This cluster head then acts as the directory agent for a neighborhood.

Table I shows the communication overhead for Milan, DRD, and Kilavi in terms of the number of hops that each type of message (registration, query, and update) is transmitted. This analysis assumes that the Milan uses the same flooding as in the Kilavi registration phase, and includes the cluster-head election overhead for DRD. We assume that DRD uses the LEACH clustering protocol, with a probability of approximately 0.05 for each node to elect themselves as leader. In [21] the optimal is reached when about 5% of nodes are cluster heads. Also, it is assumed that while most nodes register once, the discovery process happens more frequently as new applications are written for the sensor network. There are n nodes in the network and k is the length of a path through the network.

TABLE I
SERVICE REGISTRATION, DISCOVERY, AND MAINTENANCE COSTS IN TERMS OF THE NUMBER OF MESSAGES TRANSMITTED

	Registration	Discovery	Maintenance
Milan	1	$n \cdot k$	1
DRD	1	$0.05 \cdot n \cdot k$	n
Kilavi	n	k	k

C. Routing & Data Dissemination

There are four main types of routing protocols used in sensor networks, flooding, geographic, cluster-based (LEACH [21]), and gradient-based (SPIN [20]) routing. Kilavi is a hybrid flooding approach, where flooding is only employed for route discovery, but not used for data dissemination. The use of a central routing cache is beneficial in many ways, for example, in Kilavi; there is a single flooding stage wherein the central node learns all network routes. Other protocols, such as directed diffusion, have a similar stage, except the route discovery is for a single sink. In Kilavi, the central node has global information and can compute other sinks' routing tables.

Although Kilavi is by no means a perfect implementation, its benefits can clearly be seen in comparison to the other routing implementations (note, we are not considering

geographic routing due to its problems in routing around obstacles). When compared to SPIN (that is intended to large scale networks), Kilavi does not need ADV/REQ packets before sending out a DATA packet because it can determine beforehand which nodes need to directly receive packets. Also, SPIN takes 50% longer to converge than flooding/Unicast. The centralized architecture can be used to distribute the load among nodes and optimize paths through the network. For example, LEACH-C results in a 20-40% longer network lifetime over LEACH (p.97 in [21]).

Fig. 2 shows a comparison of the overhead for the various protocols. A 25 node network with a diameter of 8 hops and an average neighbor degree of 4.7 is assumed. For the LEACH protocol, new cluster heads are elected approximately every 100 messages. We also assume that each interest message receives on average 100 data replies. The centralized Kilavi approach far outperforms the other protocols. All routes are pre-specified, and no negotiation or reinforcement messages are required beyond the cost of periodically maintaining routes.

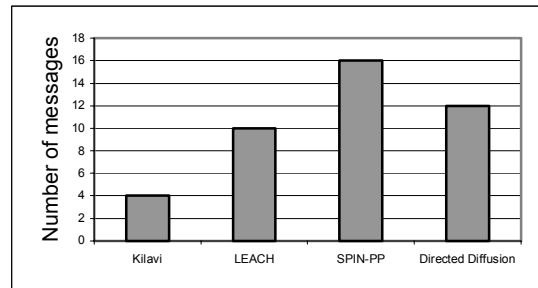


Fig. 1. Overhead (additional messages sent per 100 data messages) for various routing protocols (Note, SPIN-PP has a higher overhead in number of messages, but most of these are meta-data messages and smaller in size).

D. Medium Access Control (MAC) and Duty Cycling

The MAC energy optimization can be achieved e.g. by reducing packet overhead, idle listening time, over-emitting, over-hearing, and collisions in the shared RF medium. There are many, mostly contention-based (CSMA, *Carrier Sense Multiple Access*), proposals for WSN MAC protocols. Some of these are IEEE 802.11 inspired S-MAC [22], T-MAC [23] enhancing the energy usage of S-MAC by using a very short listening windows, and B-MAC [24] using an adaptive preamble to reduce sensor activity and idle time. Generally, contention-based solutions, compared to schedule-based, do not need very precise synchronization and are scalable. However, control messages decrease channel capacity.

MAC protocols can be compared based on energy consumption, end-to-end latency, and time spent in sleep mode in the function of packet size, packet rate, and a number of hops. Reliable evaluation is complicated because e.g. B-MAC assumes that retransmissions, hidden-terminal avoidance, and duplicate suppression are implemented in upper levels but S-MAC implements these all three.

Centralized architecture used in Kilavi gives the home automation application a chance to control duty cycles to optimize e.g. the sensor lifetime versus communication latency (e.g. when application gets information about the low

battery of the sensor it can slow down the operation of the sensor to conserve the battery until it is replaced maintaining the continuous operability). In S-MAC, T-MAC, and B-MAC duty cycles are set independently.

Fig. 2 presents S-MAC, B-MAC, and Kilavi latency per hop count measurements. S-MAC and B-MAC values are gained from paper [24] that used TinyOS based Mica2 motes. To be able to compare latency in 10-hop network, extreme data payload lengths of 100 Bytes are used. Kilavi operates well even with these very long packets. In practice, Kilavi uses very short packets (10-30 bytes) depending mainly on hop length. Centralization also enables information sharing to improve network operability e.g. by sending information about network noise levels to optimize transceiver operation.

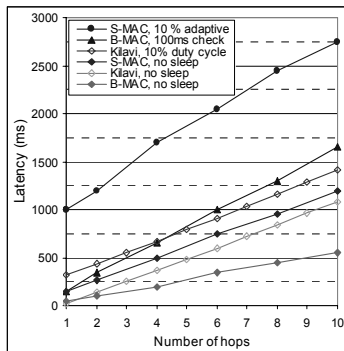


Fig. 2. S-MAC, B-MAC and Kilavi end-to-end latency versus the hop count with and without duty cycling.

E. Security

The broadcast nature of wireless communication makes it intrinsically insecure. WSN security should guarantee information confidentiality, authenticity, integrity and freshness. In WSN security the number of security related transmissions, increased latency and energy consumption due to extra bytes sent, and extra computation time and energy are important performance measures.

Conventional security protocols such as Diffie-Hellman key agreement and RSA signatures are conservative in their security guarantees, typically adding 16 to 64 bytes of overhead. This is not tolerable in WSNs because of increased use of the radio. Reference [25] evaluates that each extra bit transmitted consumes equal amount of power than executing 800-1000 instructions in the processor. Also processors and memories are too weak for the encryption of these heavy protocols. In SPINS (*Security Protocols for Sensor Networks*) over 90% of the security related energy consumption is caused by increased transmissions [26].

Keeping this in mind, in Kilavi data packets are increased only by 4 bytes if authentication and encryption are used. Similarly, in TinyOS/TinySec message length is increased just by 5 bytes [27], and in SPINS increment is 8 bytes [26]. Fig. 3 shows the latency with and without security features in multi-hop network with 26 bytes data payloads. TinySec measurement results with Mica2 motes were gained from [27]. As a summary, in TinyOS/TinySec and Kilavi the energy, bandwidth, and latency overhead is less than 10%.

The dominating traffic pattern in WSN is many-to-one where sensors communicate with central unit. Thus, centralized security architecture is natural choice, especially for smaller networks. In Kilavi, the central node manages, delivers and updates keys with every node. Nodes have one authentication and one encryption key to enable secure communication with the central node. This simplifies the operation of the nodes and reduces messages sent.

However, end-to-end security architecture is difficult to implement to a very large scale WSN, where there is a need for peer-to-peer communication. For example, in SPINS a third party manages peer-to-peer keys, which increase the communication overhead considerably compared BROS (Broadcast Session Key Negotiation Protocol) and C&R schemes [28]. BROS is a protocol where each node negotiates a session key locally with its neighbors by broadcasting.

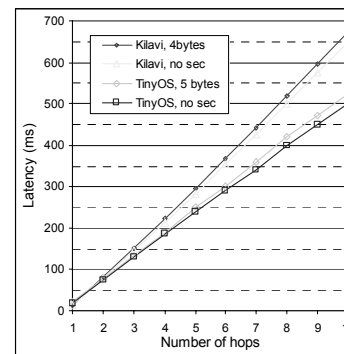


Fig. 3. End-to-end latency versus the hop count with and without security features in TinyOS/TinySec and Kilavi protocols.

VI. ZUMA AND KILAVI

The central Kilavi management device is tightly integrated with the ZUMA platform (or UCR implementation). The abstraction of this is shown in Fig. 4. This enables non-sensor network applications to seamlessly use the sensor network functionality, both actuation and information gathered. Consider the scenario of a home occupant watching a movie. This person most probably would not like a noisy appliance (laundry, dishwasher etc.) to turn on during the movie. In addition, the home automation system can use the information from the multimedia application to reduce power consumption by adjusting the heating and lighting, and by turning off media devices that are not currently being used.

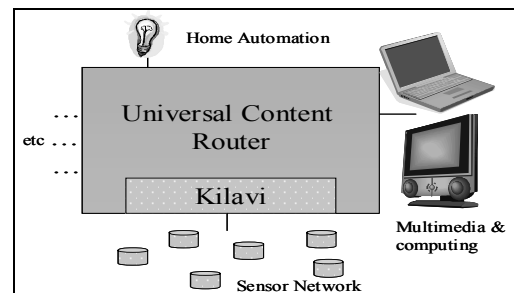


Fig. 4. The universal content router and Kilavi.

VII. CONCLUSIONS

We believe that the future of sensor networks is in integrating them with other networks in the home so that their ubiquitous component can be fully utilized by more powerful networks and applications. The combination of the ZUMA and Kilavi platforms is the first step in this integration. The simple Kilavi protocol was compared with some traditional distributed WSN approaches. Results indicate that the device discovery and maintenance can be done with reduced packet overhead, after the initial device registration. The routing is also more efficient because routes are pre-specified, and no negotiation or reinforcement messages are required beyond the periodic maintenance. Kilavi MAC provides a lower end-to-end latency for data in the sensor network when duty-cycling is increased. In addition, the centralized security architecture simplifies the WSN operation considerably and the communication overhead caused by enhanced security is tolerable.

ACKNOWLEDGMENT

We thank Mikko Torniaainen & Hannu Sikkila from TUT for Kilavi development, also Chris Baker, Yury Markovsky, & Adam Wolisz for contributions to the ZUMA project.

REFERENCES

- [1] J. van Greunen, Y. Markovsky, C. R. Baker, J. Rabaey, J. Wawrzynek, A. Wolisz. "A platform for smart home environments – the case for infrastructure." Proc 2nd Intl Conf. on Intelligent Environments 2006.
- [2] C. R. Baker, Y. Markovsky, J. van Greunen, J. Rabaey, J. Wawrzynek, A. Wolisz, "ZUMA: A Platform for Smart-Home Environments," Proc. 2nd Intl Conf on Intelligent Environments 2006
- [3] A. Kansal, W. Kaiser, G. Pottie, M. Srivastava, and G. S. Sukhatme, "Reconfiguration methods for mobile sensor networks," ACM Transactions on Sensor Networks, 2006.
- [4] <http://www.greatduckisland.net/>
- [5] <http://www.princeton.edu/~mrm/zebronet.html>
- [6] M. Soini, H. Sikkila, P. Oksa, L. Sydanheimo, and M. Kivikoski, "KILAVI wireless communication protocol for the building environment networking issues" Proc. Intl. Symp of Consumer Electronics 2006.
- [7] H. Sikkila, M. Soini, P. Oksa, L. Sydanheimo, and M. Kivikoski, "KILAVI wireless communication protocol for the building environment security issues," Proc. Intl Symp of Consumer Electronics 2006.
- [8] S. Madden, M. Franklin, J. Hellerstein, W. Hong. TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks. OSDI, 2002
- [9] I. Chatzigiannakis, G. Mylonas, S. Nikolettseas "jWebDust: A Java-based Generic Application Environment for Wireless Sensor Networks," International Conf. on Distributed Computing in Sensor Systems, 2005
- [10] R. Newton, Arvind, and M. Welsh., "Building up to Macroprogramming: An Intermediate Language for Sensor Networks," Proc. Fourth Intl Conf. on Info Processing in Sensor Networks 2005.
- [11] K. Whitehouse, C. Sharp, E. Brewer, and D. Culler, "Hood: a neighborhood abstraction for sensor networks," MobiSys, 2004.
- [12] W. Heinzelman, A. Murphy, H. Carvalho and M. Perillo, "Middleware to Support Sensor Network Applications," IEEE Network Magazine Special Issue. Jan. 2004.
- [13] S. Tilak, K. Chiu, N. B. Abu-Ghazaleh, T. Fountain, Dynamic Resource Discovery for Wireless Sensor Networks" IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)
- [14] L. Doherty, K. S. J. Pister, and L. El Ghaoui, "Convex position estimation in wireless sensor networks," In the proceedings of IEEE Infocom, Anchorage, AK, April 2001.
- [15] N. Bulusu and D. Estrin and L. Girod and J. Heidemann, "Scalable coordination for wireless sensor networks: self-configuring localization systems," In the proceedings of Sixth International Symposium on Communication Theory and Applications, 2001.
- [16] Dragos Niculescu and Badri Nath, "Ad-hoc positioning system," Technical Report DCS-TR-435, Rutgers University, 2001.
- [17] Tian He, Chengdu Huang, Brian M. Blum, John A. Stankovic, and Tarek F. Abdelzaher, "Range-free localization and its impact on large scale sensor networks," ACM Transactions on Embedded Computing System (TECS), vol. 4, issue 4, November 2005.
- [18] S. Ganeriwal, R. Kumar, and M. Srivastava, "Network-wide time synchronization in sensor networks," Technical Report, Networked and Embedded Systems Lab, Elec Eng. Dept, UCLA, 2003.
- [19] J. van Greunen, J. Rabaey, "Lightweight time synchronization for sensor networks," Second ACM International Workshop on Wireless Sensor Networks and Applications, San Diego, CA, USA, September 2003.
- [20] J. Kulik, W. Rabiner, H. Balakrishnan Adaptive Protocols for Information Dissemination in Wireless Sensor Networks Proc. 5th ACM/IEEE Mobicom Conference, Seattle, WA, August 1999
- [21] W. Heinzelman, Application-specific protocol architectures for wireless networks, PhD thesis, Massachusetts Inst. of Technology, June 2000.
- [22] W. Ye and J. Heidemann, "Medium access control in wireless sensor networks" in Wireless Sensor Networks, Kluwer Academic Pub., 2004.
- [23] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks", Proc First ACM Conference on Embedded Networked Sensor Systems, Los Angeles, November 2003.
- [24] J. Polastre, J. Hill, D. Culler, "A versatile low-power medium access layer," ACM Conf. on Embedded Networked Sensor Systems, 2004.
- [25] Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. S. J. Pister, "System architecture directions for networked sensors," in Architectural Support for Programming Languages and Operating Systems, pp. 93-104, 2000.
- [26] A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar, "SPINS: security protocols for sensor networks," Wireless Networks Journal, 2002.
- [27] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," Second ACM Conference on Embedded Networked Sensor Systems, Nov. 2004.
- [28] B.-C. Lai, D. Hwang, S. P. Kim, I. Verbauwhede, "Reducing radio energy consumption of key management protocols for wireless sensor networks," Proc International Symposium on Low Power Electronics and Design, pp. 351-356, 2004.