Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 920141, 15 pages
doi:10.1155/2011/920141

Research Article

A Wireless Sensor Network for Hospital Security: From User Requirements to Pilot Deployment

Ville Kaseva, Timo D. Hämäläinen, and Marko Hännikäinen

Department of Computer and Digital Systems, Tampere University of Technology, P.O. Box 553, 33101 Tampere, Finland

Correspondence should be addressed to Ville Kaseva, ville.a.kaseva@tut.fi

Received 28 June 2010; Accepted 13 August 2010

Academic Editor: Christos Verikoukis

Increasing amount of Wireless Sensor Network (WSN) applications require low network delays. However, current research on WSNs has mainly concentrated on optimizing energy-efficiency omitting low network delays. This paper presents a novel WSN design targeted at applications requiring low data transfer delays and high reliability. We present the whole design flow from user requirements to an actual pilot deployment in a real hospital unit. The WSN includes multihop low-delay data transfer and energy-efficient mobile nodes reaching lifetime of years with small batteries. The nodes communicate using a low-cost low-power 2.4 GHz radio. The network is used in a security application with which personnel can send alarms in threatening situations. Also, a multitude of sensor measurements and actuator control is possible with the WSN. A full-scale pilot deployment is extensively experimented for performance results. Currently, the pilot network is in use at the hospital.

1. Introduction

Wireless Sensor Networks (WSNs) are one of the main building blocks in ambient intelligence, where tiny nodes are embedded into our everyday life objects making them smart. The tight integration and collaboration with other devices and the physical world inflict a number of constraints on these devices. Typically, WSNs consist of densely deployed, independent, and collaborating microsensor nodes which are highly resource-constrained in terms of energy, processing, and data storage capacity [1, 2]. The nodes are capable of sensing, data processing, and communicating over multiple short distance wireless hops. The network self-organizes and implements its functionality by cooperative effort.

Currently, most WSN designs concentrate on improving energy-efficiency leaving network delays to low priority [3]. This makes them unsuitable for time-critical applications. Still, several envisioned WSN applications should be able to handle scenarios requiring low delays [4]. In personal security it is essential that alarm messages are delivered reliably and quickly. Other application areas requiring low communication latencies include surveillance applications and real-time localization.

At Tampere University of Technology, we have developed low-power WSNs for various different applications [5–9]. Furthermore, our research has produced a multitude of WSN node hardware platforms [5, 10, 11]. In this paper, we present a novel design called *hospital security WSN*. With the hospital security WSN, personnel can send wireless alarms in threatening situations, receive acknowledgements telling that help is on its way, make various different kind of measurements, and use actuators. The main contributions of the paper are

(i) user requirement specification for the hospital security WSN,

(ii) design and implementation meeting the presented requirements,

(iii) real world pilot deployment and experiments.

The hospital security WSN user requirements are wireless devices with room-level localization, reliable low-latency alarming, long network lifetime, and ease of installation and maintenance.

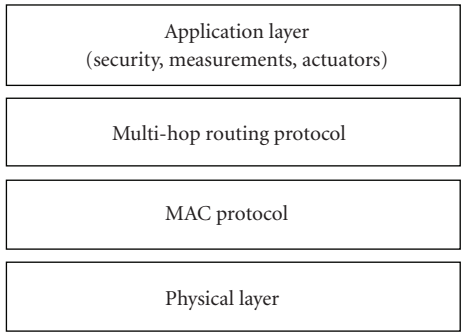


Figure 1: Hospital security WSN protocol stack. Security, measurements, and actuator control are implemented at the application level. The routing and the MAC protocol are designed for reliable low-latency multi-hop data forwarding. The physical layer consists of the hospital security WSN node hardware including various sensors.

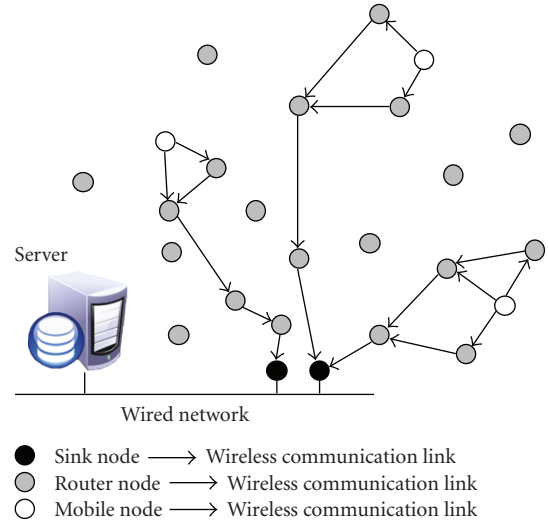


Figure 2: Hospital security WSN topology. The router nodes forward data via multiple hops to one or multiple sinks. Mobile nodes broadcast their data to the router nodes.

(i) *Wireless Devices with Room-Level Localization.* The alarming devices are continuously carried by the hospital personnel. This requires fully wireless small devices operating with small batteries. The alarms should be responded as quickly as possible by a security guard and other personnel on-site. Thus, the alarming devices should be localized within one to two rooms.

(ii) *Reliable Low-Latency Alarming.* Alarms are triggered by a person in a threatening situation. Being critical for personal security, alarm messages should not be lost. Furthermore, to ensure fast reaction to alarms, the alarm message delay should be in the order of seconds.

(iii) *Long Network Lifetime.* For easy maintenance, the network should have long lifetime in the order of years. This includes all devices in the network whether they are mobile or static.

(iv) *Ease of Installation and Maintenance.* The alarm network can be installed and used in many locations. Thus, it should be possible to be installed and maintained by the personnel on-site without the need for rigorous guidance to the network operation.

To achieve these requirements, the hospital security WSN utilizes a heterogeneous architecture where variable duty cycling is used based on node responsibilities giving them different activity times. The network achieves reliable data forwarding and low delays whilst enabling the usage of fully wireless sensor nodes that can be also mobile if needed. The mobile nodes are localized using a location resolver algorithm presented in our previous work [12]. Both the communication and localization are resilient against failed nodes and communication links.

The hospital security WSN protocol stack is presented in Figure 1. The application layer consists of security, measurement, and actuator control applications. The routing protocol provides autonomous multi-hop data forwarding. The MAC protocol implements wireless communication between nodes. The physical layer consists of the hospital security WSN node hardware which includes various sensors.

The topology of the hospital security WSN is depicted in Figure 2. The network consists of sink nodes, router nodes, and mobile nodes. The sink nodes act as data endpoints for the WSN and as gateways to other networks. The router nodes forward data via a wireless multi-hop network to one or multiple sinks. To achieve low delays, the duty cycle of the routers is configured to be high. Thus, they consume more power and should be mains powered or equipped with large enough batteries. The mobile nodes have low duty cycles which can be configured according to application needs. They broadcast their data to the router nodes. Thus, the mobile nodes can operate with small batteries whilst still achieving lifetime in the order of years.

A full scale hospital security WSN was implemented for the pilot deployment and experiments. The network consists of resource-constrained WSN nodes. The nodes communicate using a low-cost low-power 2.4 GHz radio that does not include Received Signal Strength Indicator (RSSI) functionality. Before deployment to the hospital environment, the network was experimented in an office environment at Tampere University of Techology. After this the network was deployed and measured at the hospital environment.

We present communication reliability, delay, and localization accuracy results for both environments. Localization accuracy and resilience of our location resolver algorithm in an office environment were experimented in our previous work [12]. These results are also shown in this paper. We also measured the room-level localization accuracy at the hospital environment. Furthermore, we present results of the node power consumptions. Currently, the pilot network is in use at the hospital.

The rest of the paper is organized as follows. Section 2 surveys related work in low-power and low-latency WSNs.

The design of the hospital security WSN is presented in Section 3. Section 4 introduces the location resolver algorithm. The end-to-end network architecture and the hospital security WSN node hardware are presented in Section 5. Section 6 presents the experiments and results. Furthermore, the section compares our network and related work against the user requirements. In Section 7, we discuss other applications that can be implemented using the hospital security WSN. Finally, Section 8 concludes the paper.

2. Related Work

Low-latency performance is achieved through co-operation of all components in the WSN protocol stack. The MAC protocol should provide small channel access delays while routing protocol should strive for multi-hop network delay minimization. The radio transceiver is the most power-consuming component in a WSN node [13]. Thus, node energy-efficiency is most of all dictated by the MAC layer as it controls the radio usage [4]. Routing plays a key role in managing the whole network lifetime by balancing traffic among the nodes. Next, we survey WSN MAC protocols, low-latency WSN routing protocols, and low-latency WSN implementations.

2.1. WSN MAC Protocols. WSN MAC protocols are usually designed for energy-efficient operation, and low channel access delays are secondary goals or omitted completely. Also, in many cases the networks are considered to be relatively static. Thus, dynamics, especially mobility, can introduce significant additional energy consumption to their operation.

WSN MAC energy-efficiency is achieved by duty-cycling, where data is exchanged in active periods and rest of the time is spent in low-power sleep-mode. WSN MAC protocols can be divided into three categories: random-access, scheduled contention access, and Time Division Multiple Access (TDMA) [12].

The low duty-cycle random-access MAC protocols, such as B-MAC [14], are based on a technique called low-power listening. It includes the procedure of periodically polling the wireless channel to test for traffic. Typically, frames are transmitted with a preceding preamble that is longer than the channel poll interval. This ensures that the destination node is awake during the actual data transmission. These protocols are relatively simple and require less memory than the other WSN MAC categories [13].

Scheduled contention-access low duty-cycle MAC protocols, such as S-MAC [15] and IEEE 802.15.4 Low-Rate Wireless Personal Area Network (LR-WPAN) standard [16] used in Zigbee networks, utilize periodic active and sleep periods to achieve duty cycling. The start of the active period includes the transmission of synchronization frames to communicate own schedule information to neighboring nodes. The rest of the active period is reserved for data exchanges, which typically use contention-access for medium arbitration.

TDMA-based low duty-cycle MAC protocols, such as SMACS [17] and TUTWSN MAC [5], exchange data only in predetermined synchronized time slots. Rest of the time is spent in sleep mode. This makes the protocols virtually collision-free and removes overhearing. The only sources of idle listening are reception margins, which are usually relatively small. In static networks, TDMA MAC protocols can achieve even an order of a magnitude lower energy consumption than the protocols in other MAC categories [5].

The energy-efficiency of the random-access MAC protocols is reduced due to high idle listening times, high overhearing, and the long preamble. Also, there is a tradeoff between the channel access delay and energy-efficiency. As network dynamics increase, neighbor discovery starts to produce significant energy overhead with the scheduled contention-access and TDMA-based MAC protocols. Furthermore, these protocols incur high channel access delays since data cannot be transmitted immediately but in a dedicated time slot. The heterogeneous design of hospital security WSN achieves both energy-efficient mobile nodes and low-delay data forwarding.

2.2. Low-Latency Routing Protocols. Multiple real-time routing protocols have been proposed for WSNs [4]. Most of them aim at only estimating network delays and guaranteeing a worst case packet delay for application level. They do not explicitly try to decrease network delays. Furthermore, design decisions such as reactive/proactive routing and flat/hierarchical topology affect the network delays and energy-efficiency.

Geographic routing protocol SPEED [18] provides soft real-time latency guarantees proportional to path length. It maintains a desired packet delivery speed in the network by estimating one-hop delays from MAC level feedback. However, SPEED leaves reliability unattended, and the used reactive route discovery method increases latency of the data forwarding process. Also, SPEED does not take energy issues into consideration.

Multipath Multi-SPEED (MMSPEED) [19] extends SPEED by providing service differentiation and probabilistic multipath forwarding to support various reliability requirements. It offers multiple network-wide delivery speed options for different application end-to-end deadlines. Similarly to SPEED, MMSPEED does not take energy domain into consideration and makes routing decisions reactively.

A location-aware design in [20] presents a heuristic solution to find energy-efficient path for delay-constrained data in WSNs. The design achieves balancing between latency and energy consumption but is based on the usage of two different power level radios making the used hardware more energy-consuming and increasing hardware costs.

Real-time power-aware routing (RPAR) [21] protocol is a location-aware protocol proposed to achieve low communication delays and energy-efficiency by dynamically adjusting transmission powers and routing decisions. Applications can make tradeoffs between energy consumption, network capacity, and lower delays by specifying packed deadlines. The reactive broadcast method of RPAR appears to be challenging in larger networks because of the neighbor

table size and a great amount of traffic congesting replies, and in smaller networks the possibility of missed broadcast increases. This can lead to significant increases in delay.

In [22], Akkaya and Younis propose an energy-aware QoS routing protocol that searches for energy-efficient path which satisfies latency requirements. The delay requirements are converted into bandwidth requirements, and traffic is divided into different priority queues for time-critical and delay unconstrained packets. However, the proposed method consists of too complex algorithms for resource-constrained nodes in large-scale networks [4].

A cost-based routing protocol called GRAdient Broadcast (GRAB) [23] forwards packets along an interleaved mesh. Nodes broadcast packets using a cost metric. Every packet is assigned a budget. The budget consists of the minimum path cost from source to sink and a credit, which is utilized to increase reliability by channeling data along multiple paths. Although duplicate packets are controlled by a cache of recently forwarded packets, the redundant packets degrade energy-efficiency and increase delay. Also, the packet cache size increases rapidly with network size and data transmit frequency.

The proactive routing of the hospital security WSN enables fast data forwarding process. The used costs minimize the multi-hop communication latency. The mobile nodes are relieved from doing routing. Thus, this does not hinder their energy-efficiency.

2.3. Low-Latency WSN Implementations. WSN designs for time-critical applications are relatively rare. Furthermore, their experimented performance is seldom documented very accurately.

In [24], Simon et al. present a sniper detection and localization system for urban environments, which is further refined in [25]. The system is built on Mica product line [26], and the later version is extended with an external Field Programmable Gate Array (FPGA) sensor board. The used MAC layer is not documented. Routing is done with Directed Flood-Routing Framework (DFRF) [27].

DFRF is a gradient-based, best-effort converge-cast protocol with data-aggregation. The directed broadcasts of DFRF provide robustness and fast message delivery, but result in high communication overhead. Thus, the design is only suitable for one-shot type events and does not scale well.

In an experimental scenario, the network achieved low delays with an average latency of 2 seconds. However, the lifetime was low (12 hours). Furthermore, node mobility is not considered in the design.

3. Hospital Security WSN Design

The hospital security WSN communication stack design consists of a MAC and a routing protocol. The MAC protocol uses random channel access to achieve low channel access delays. Thus, nodes can transmit data at any required time instant. The routing protocol utilizes multiple cost-based, proactively constructed routing gradients to the sink nodes.

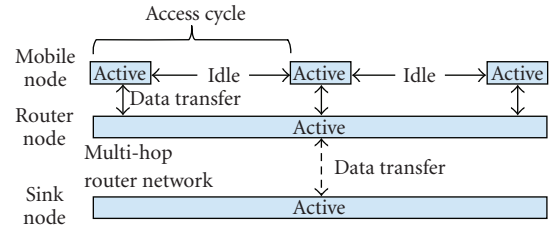


Figure 3: Node duty cycles and data transfer.

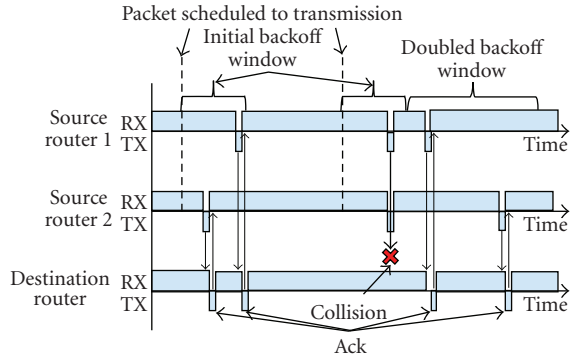


Figure 4: Router node channel access operation principle. The source routers 1 and 2 schedule packets for transmission simultaneously. The first packets are sent successfully using an initial backoff time. The second packets collide and are successfully retransmitted using a backoff window twice the length of the initial.

This allows quick routing decisions during data forwarding and QoS support based on the costs.

3.1. MAC Protocol. Figure 3 demonstrates the operation principle of the hospital security WSN MAC protocol. The operation of the mobile nodes is divided to access cycles. The mobile nodes are active only a short period of time in an access cycle, and the rest of the time is spent in low-power sleep mode to save energy.

During the active periods, the mobile nodes can exchange data with the router nodes. The router nodes are active all the time. They exchange data when needed. At the link level all routers are homogenous forming a flat network topology.

All data are exchanged in a common data channel having a specific frequency band. Network beacons, used for neighbor discovery signaling among the router nodes, are transmitted on a different frequency channel.

3.1.1. Router Node Channel Access. The router nodes use a randomized backoff-based channel access similar to the ALOHA protocol [28] with truncated binary exponential backoff. An example is presented in Figure 4. Both Source routers 1 and 2 schedule their first packet to transmission at the same time. The actual transmission time is randomized inside an initial backoff window. The source routers randomize different backoff times for the initial transmissions. Thus, they both transmit their packets successfully to the

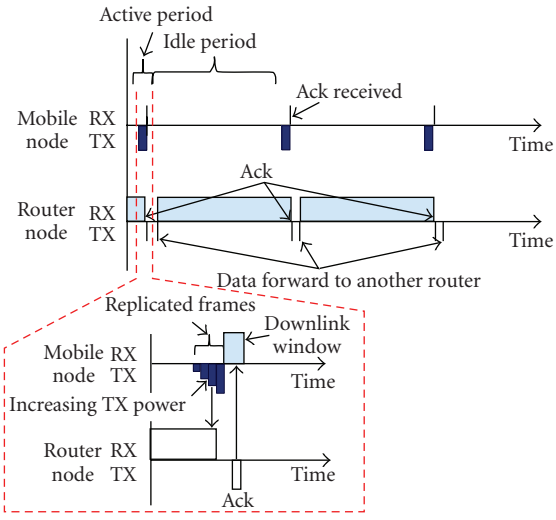


FIGURE 5: Mobile node channel access operation principle. The mobile node sends replicated frames with varying transmission powers during its active period. The router node randomizes its acknowledgement to the downlink slot. During idle period the mobile node is in a low-power sleep mode.

destination router, who acknowledges the successful data exchanges.

Again, the second packets are scheduled to transmission simultaneously. However, now both the source routers randomize the same initial backoff time and the packets collide. The source routers deduce the collision from the missing acknowledgement. Thus, they schedule their packets for retransmission. Due to the binary exponential backoff, a backoff window twice the length of the previous one is used. Using the rerandomized backoff times, the source routers are able to transmit their packets successfully.

3.1.2. Mobile Node Channel Access. As illustrated in Figure 5, a mobile node active period consists of a set of uplink packets and a downlink window for acknowledgements and data communication from the routers to the mobile node. Each packet in the uplink set contains the same frame transmitted with varying power levels. This increases reliability and enables the metering of path loss between the mobile node and the routers without the need for RSSI hardware. This data can be used for localization.

All receiving router nodes acknowledge the received data to the mobile node. The routers randomize their downlink transmissions within the downlink window. Application payload data to the mobile nodes can be piggybacked in the acknowledgement packets. This data includes the application level acknowledgements to the alarms.

For collision avoidance, the mobile nodes randomize their active period occurrence times. For this, time is divided into active period slots. The slots are indexed so that the slot giving the desired access cycle length has index zero, the slots giving shorter access cycle length have indexes below zero, and the slots giving longer access cycles have indexes above zero. Thus, the randomized slot index can be between $[-sidx, sidx]$ ($sidx \in \mathbb{N}_+$), where $sidx = (N_{\text{ap\_slots}}/2) - 1$. $N_{\text{ap\_slots}}$ denotes the amount of active period slots in one access cycle. Equal probability to adjust access cycle (T_{ac}) shorter or longer results in

$$T_{\text{ac}} = \lim_{n \to \infty} \frac{\sum_{k=0}^{n} \left(t_{\text{ap}(k+1)} - t_{\text{ap}(k)} \right)}{n}, \quad (1)$$

where $t_{\text{ap}(k)}$ is the start time of active period k. Thus, the mean access cycle length is always the desired T_{ac}.

Since the uplink frames are broadcast, the mobile nodes do not need any information about their neighbors. Thus, they do not need to do energy-consuming neighbor discoveries and can reach ultra-low energy consumption with minimal messaging overhead.

The mobile nodes adjust their access cycle lengths (T_{ac}) according to application QoS demands. For time-critical data, a low-delay mode is used. In this, the access cycle length is shortened so that the application frame is transmitted immediately upon arrival to the MAC layer. Furthermore, the shorter low-delay access cycle is maintained until the frame is acknowledged by a router. Rest of the time a longer access cycle is used resulting in a low-power mode. Frames that are not time-critical are sent using this longer access cycle.

3.1.3. Router Neighbor Discovery. Network beacons are used for neighbor discovery among routers. The beacons are transmitted periodically in a common network-wide channel. A neighbor discovery is performed by listening to the network channel in a network scan. A separate channel is used to reduce interference with the data channel. The network beacon transmissions are scheduled by randomizing the transmission interval (T_{nb}) between $T_{\text{nb\_min}}$ and $T_{\text{nb\_max}}$.

The randomization prevents sequential beacon collisions. $T_{\text{nb\_min}}$ can be used to reduce congestion in the network channel. $T_{\text{nb\_max}}$ gives a theoretical upper bound for discovering all neighbors in the same radio coverage area and limits the maximum network scan length. The network beacons are transmitted with varying transmission powers to enable link quality monitoring without RSSI.

3.2. Routing Protocol. In the hospital security WSN, router nodes form a multi-hop network that forwards data towards sink nodes. Mobile nodes can act only as leaf nodes with no routing capabilities. The protocol discovers routing gradients based on cumulative costs in the network. The gradients with the lowest route cost are chosen for data forwarding.

The routing protocol allows multiple sink nodes in the network. They can be either individuals or replicas. The sinks request data from the network using interests. Individual sinks have unique addresses and separate interest information. Replicated sinks share the same address and interest information. Routing to the nearest sink lowers latency further by minimizing the amount of hops that a packet has to traverse. The routing protocol functionality is divided into route discovery, route calculation, and data forwarding.

3.2.1. Route Discovery. To establish and maintain routes to sinks, routing information related to these sinks needs to be exchanged in the network. This is done using *sink information units*. A sink information unit includes the sink address, sink interests, sink sequence number, and costs to reach the sink.

The address is used to identify individual sinks. The interests signal the attributes of the data requested by the sink. That is, the interests tell what kind of data needs to be sent and how often it is sent, for example, send alarms on-demand and temperature information every 10 minutes. The sink sequence number is used to resolve the latest sink information and reject old information. It is incremented by a sink when it disseminates new interests to the network. The costs are used to choose routes to the sinks. Individual cost value is included for each QoS class.

The routing information is signaled in two kinds of packets: the network beacons provided by the MAC protocol and route advertisements sent in the common data channel. Complete sink information, including all interests, is sent in the network beacons. The number of sink interests is not limited, as the routing protocol supports information fragmentation to multiple beacons.

The advertisements signal minimal routing data for route maintenance. This data includes the sink information unit without the interests. Thus, the route signaling data at the data channel is kept minimal. Also, the advertisements enable fast interest diffusion to the network as neighbors can start scanning for the whole sink information when new sink sequence number is found from an advertisement.

The route discovery process is divided into sink-initiated route *construction* and router node-initiated route *maintenance*. Route construction is for sink interest diffusion and fast network build-up. Route maintenance allows adaptation to network dynamics (e.g., failed nodes or changed link qualities) and the joining of new nodes. No periodic route refreshing is needed but maintenance procedures are used only when needed.

3.2.2. Route Calculation and Costs. The route calculation uses only local information available in a router node and its neighborhood. The route cost structure is depicted in Figure 6. It consists of a cost advertised by a neighbor, a cost to reach the neighbor, and local cost increase caused by the calculating node. The two latter costs are calculated locally at the node and added to the cost of the neighbor resulting in the total route cost. From all the available neighbors, the neighbor with the newest sink sequence and the lowest route cost is selected as a next hop for each known sink and QoS class. The total route costs are advertised to the neighbors resulting in cumulative cost throughout the network.

The routing cost function mechanism is tailored to match requirements of time-critical applications. Thus, cost functions concentrate on cost metrics of latency c_l and reliability c_r, while throughput and router node energy matters are left unattended. They could be added if needed it required by different applications. In the current design, the main indicator for latency cost metric is path length.

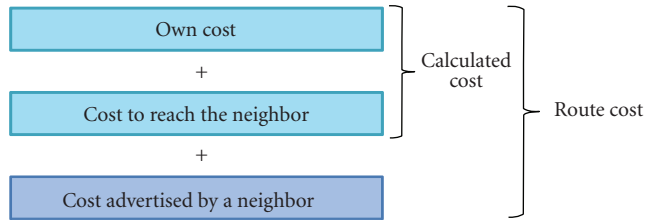


Figure 6: The route cost consists of a cost advertised by a neighbor, a cost to reach the neighbor, and local cost increase caused by the calculating node.

That is, larger amount of hops leads to bigger delay. For reliability metric link quality is used. Poorer link quality leads to additional retransmissions and possible packet drops.

The selected cost metrics are weighted with cost weights α_l and β_r. Choosing the α_l and β_r differently creates a variety of QoS classes for application purposes. The whole route cost for a QoS class can be calculated using

$$c = \alpha_l c_l + \beta_r c_r. \quad (2)$$

3.2.3. Data Forwarding. The router nodes transmit packets to neighbors by using node addresses that are globally unique inside a specific network. The routing decisions are made based on local cumulative neighbor cost information. Thus, the router nodes do not need to know the whole network address space.

As routes are proactively calculated, router nodes can transmit data packets immediately on demand. Only routing information, including final destination and intermediate source and destination addresses, needs to be included to the packets before transmission. The intermediate router nodes need only to replace the intermediate addresses and transmit the packets forward in the hop chain.

In case the packet transmission fails, the forwarding router node can immediately try another routing gradient from the routing table. Though, this gradient may not have the lowest cost, it enables the router to immediately retransmit the packet without time-consuming reactive rerouting. The primary route is recalculated later when there is time.

4. Location Resolver Algorithm

The problem of localization includes determining the physical coordinates or the area of a given node. Typically, it is achieved by doing measurements from nodes with unknown locations (localized nodes) to anchor nodes, which know their locations a priori. Then, the unknown locations are resolved using these measurements and a location estimation algorithm.

The presented location resolver algorithm follows the same principal idea as Cell Identification (CI) in cellular networks [29]. In cellular networks, Mobile Stations (MSs) try to connect to a Base Station (BS) nearest to them. Thus, the MSs can infer their location to be somewhere in the coverage area of the BS in question.

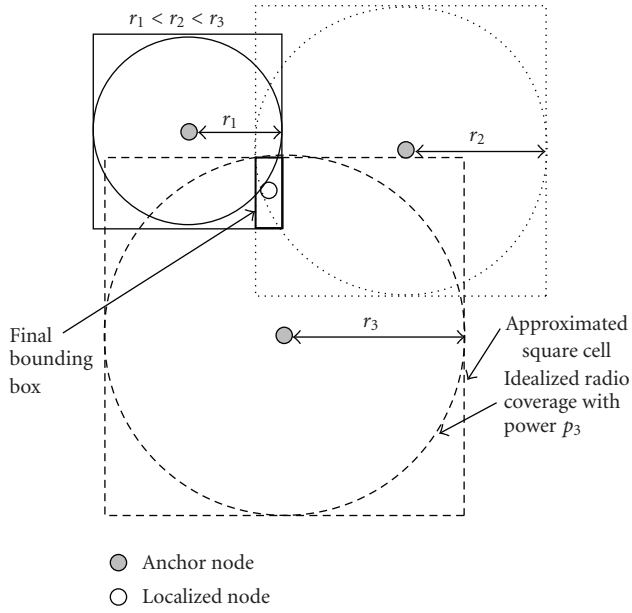


Figure 7: The location resolver algorithm operation principle. A node radio range with a certain transmission power forms a cell. Variable transmission powers are used to introduce variable sized cells. The minimum area that is bounded by the overlapping minimum sized cells around anchor nodes forms the resolved location of the localized node. To simplify calculations, the cells are modeled to be squares.

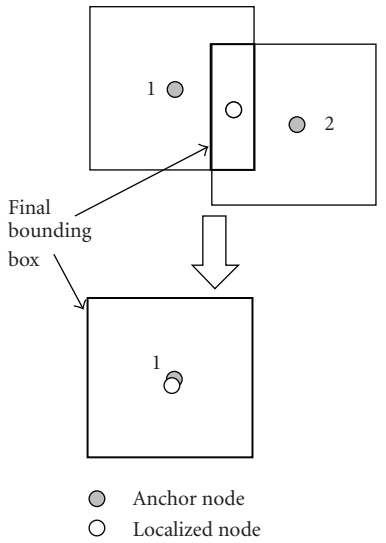


Figure 8: Location resolver algorithm resilience against failed nodes. First, both Anchor nodes 1 and 2 can hear the localized node. Then, Anchor node 2 is lost but at least a rough location is still resolved.

Our algorithm performs RF-based localization without the need for RSSI functionality. In our algorithm a node radio range with a certain transmission power is considered as a cell. Furthermore, variable transmission powers are used to introduce variable sized cells. The used algorithm finds out the minimum area that is bounded by the overlapping minimum sized cells. To simplify calculations without considerably degrading the accuracy, the cells are modeled to be squares. The measurements required by the algorithm can be acquired from the mobile node uplink packets that are sent with varying transmission powers using the routers as anchor nodes.

Figure 7 depicts three anchor nodes and one localized node. The anchor nodes can hear the localized node with powers P_1, P_2, and P_3, which map to radio ranges r_1, r_2, and r_3, respectively. Furthermore, the radio ranges map to radio coverage circles and square Localization Cells (LCs). A square can be fully determined by giving the coordinates of its bottom left and top right corners: $\mathrm{LC}_n = \{P_{\mathrm{bl\_LC}(n)}, P_{\mathrm{tr\_LC}(n)}\}$. The set of LCs used in one location resolution is denoted by LCS. In order to find the Final Bounding Box (FBB) containing the localized node, the intersection of LCs in one LCS needs to be determined. FBB is is given by

$$\mathrm{FBB} = \bigcap_{\mathrm{LC}_n \in \mathrm{LCS}} \mathrm{LC}_n. \quad (3)$$

Equation (3) can be solved by a lightweight algorithm called min-max [30–32]. Min-max relies on the fact that the intersection of all LCs can be acquired by taking the maximum of all coordinate minimums and the minimum of all maximums

$$\mathrm{FBB} = \{(\max(X_{\mathrm{bl}}), \max(Y_{\mathrm{bl}})), (\min(X_{\mathrm{tr}}), \min(Y_{\mathrm{tr}}))\}, \quad (4)$$

where X_{bl} is the set of bottom left x-coordinates, Y_{bl} is the set of bottom left y-coordinates, X_{tr} is the set of top right x-coordinates, and Y_{tr} is the set of top right y-coordinates in LCs contained by LCS.

Figure 8 demonstrates how the location resolver algorithm inherently shows resilience against failed nodes and communication links. First, both Anchor nodes 1 and 2 can hear the localized node. Thus, the unknown location is resolved to be in the intersection of the two bounding boxes. Then, Anchor node 2 is lost. After this, the unknown location is resolved using only one bounding box. The accuracy degrades as anchor nodes are lost. Still, at least a rough location is resolved even if only one anchor node is in the radio range of the localized node.

5. Implementation

Next, we present the end-to-end network architecture and the node hardware of the alarm hospital security network. We show how information is forwarded from an individual node to User Interfaces (UIs). Furthermore, we present detailed description of the node hardware components.

5.1. End-to-End Network Architecture. The end-to-end architecture of the whole alarm hospital security network is presented in Figure 9. The mobile nodes are used as alarming devices. The router nodes forward the alarm data and act as anchor nodes for alarming device localization. The alarm hospital security WSN is connected to Ethernet Local Area Network (LAN) via sink nodes that act as gateways

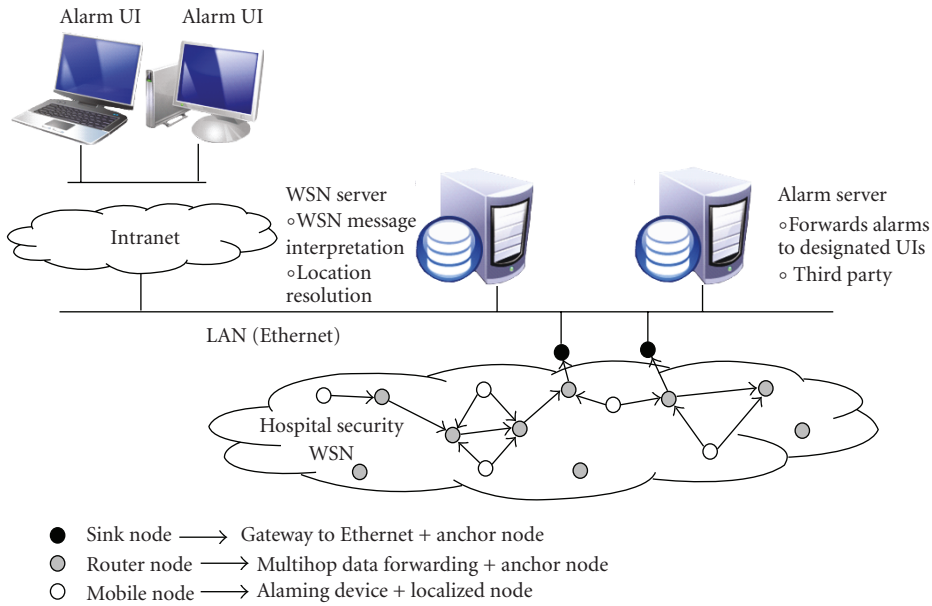


Figure 9: End-to-end hospital security network architecture.

between the WSN and other networks. The sinks forward the messages between the WSN and a WSN server.

The WSN server interprets the messages sent from the WSN and resolves the locations of the alarming devices. It provides an interface for a third party alarm server. The interface is implemented using Simple Object Access Protocol (SOAP) [33]. The third party alarm server is responsible for forwarding the alarms to designated UIs that can be, for example, in personal computers or cell phones. Via the SOAP interface, the alarm server can receive the alarming device ID, alarm time, alarm location in textual format, and alarm location highlighted in a map image.

The usage of mobile node modes in the alarming devices is depicted in Figure 10. When the node is not alarming, it stays in the low-power mode. When the alarm button is pressed, the node switches immediately to the low-delay mode. This makes quick proactive location resolution possible before the actual alarm is sent. If the button is pushed down continuously for four seconds, the node starts to send alarm packets.

The alarm packets are sent in the low-delay mode until the alarm is acknowledged telling that help is on its way. Alternatively, the alarm can be canceled by the user by pressing the button down for ten seconds. After this, the node returns to the low-power mode. This operation maximizes the node lifetime while enabling quick location resolution and alarming.

5.2. Node Hardware. The hardware platform and device enclosures are presented in Figure 11. It uses a Microchip PIC18F8722 MicroController Unit (MCU), which integrates an 8-bit processor core with 128 kB of FLASH program memory, 4 kB of RAM data memory, and 1 kB EEPROM. The used clock speed of the MCU is 8 MHz resulting in 2 MIPS performance.

For wireless communication, the platform uses a Nordic Semiconductor nRF24L01 2.4 GHz radio transceiver having data rate of 1/2 Mbps and 80/40 available frequency channels in the Industrial, Scientific, and Medical (ISM) unlicensed radio band. Transmission power level is selectable from four power levels between −18 dBm and 0 dBm with 6 dBm intervals and ±4 dBm accuracy. Loop type antenna is implemented as a trace on the Printed Circuit Board (PCB). The user interface is implemented with push buttons and Light Emitting Diodes (LEDs). The number and place of the buttons and LEDs are varied according to device.

To enable the platform usage as an Ethernet gateway, it can be equipped with an embedded Ethernet bridge which connects the MCU serial port to Ethernet. The Ethernet gateways are mains powered with 5.5 V mains power adapter. This voltage is regulated to 3.3 V with Microchip MCP1725 linear regulator. The router nodes can use batteries or be mains powered, while the mobile node uses only batteries. Router node and mobile node platforms utilize Maxim MAX8880 linear regulator, which regulates their voltage to 2.76 V.

The hardware platform hosts multitude of sensors integrated to the circuit board or via an external connector. These sensors include temperature, illuminance, air humidity, accelerometer, soil humidity, carbon dioxide, sound pressure, air flow, electrical measurements (current, voltage, resistance, and power), motion detectors (passive infrared, piezo-cable), and magnetic switches. There is also support for on/off actuator control. We are also investigating the possibility of electrocardiogram (EKG) and pulse measurements.

Compiled for the Microchip PIC18F8722 MCU, the Ethernet gateway sink node consumes 55990 bytes of program memory (42%) and 3130 bytes of data memory (79%). The router node consumes 50318 bytes of program memory (38%) and 3041 bytes of data memory (77%). The alarming

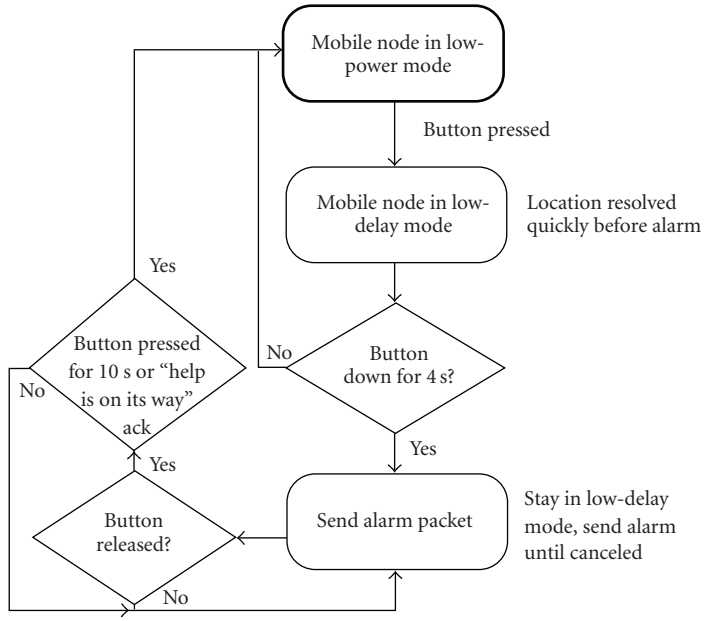
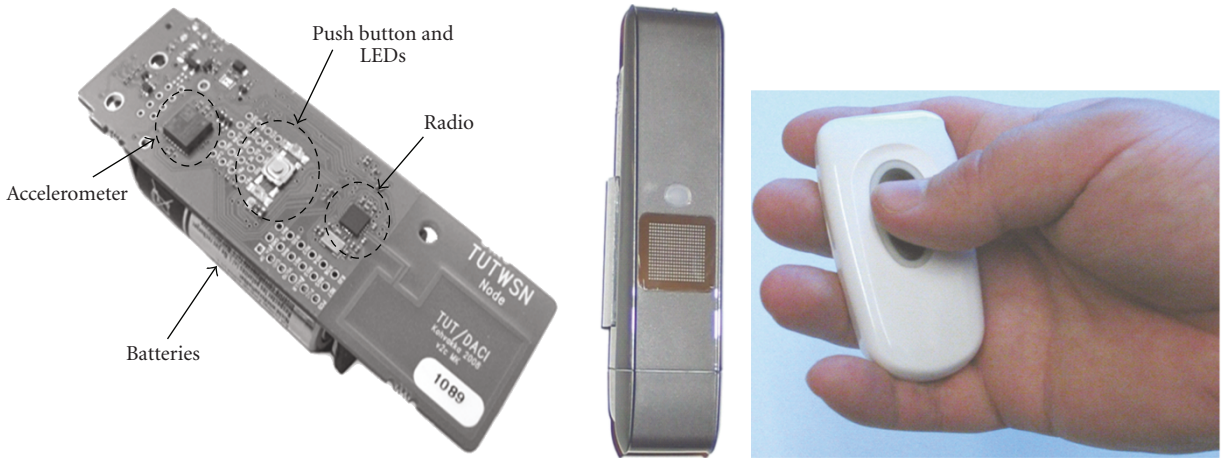


Figure 10: The alarm device operation and the mobile node modes.



(a) Hospital security WSN hardware platform

(b) Router node in enclosure

(c) Mobile node in enclosure

Figure 11: Hospital security WSN hardware platform and nodes in enclosure. The nodes are equipped with push button and LEDs for user interface implementation. For example in the mobile node, alarms are triggered using a push button and LEDs indicate if the alarm is on and if help is on its way. The nodes also include various sensors and on/off actuator control.

mobile node consumes 30851 bytes of program memory (23%) and 2411 bytes of data memory (61%).

6. Experiments and Results

A full scale hospital security WSN was implemented for experiments and pilot deployment at the hospital. Before the pilot deployment, the network was experimented in an office environment. After this, the network was deployed and experimented at the hospital environment.

In both environments the network was experimented for reliability, network delay, and localization accuracy. Also, power consumptions of mobile and router nodes were measured. The localization accuracy and resilience results of our location resolver algorithm in the office environment are from our previous work [12].

A delay diagnostics application was implemented for the the reliability and network delay experiments. The application packets contained fields for cumulative delay on each node, the number of hops traversed by a packet, and a sequence number.

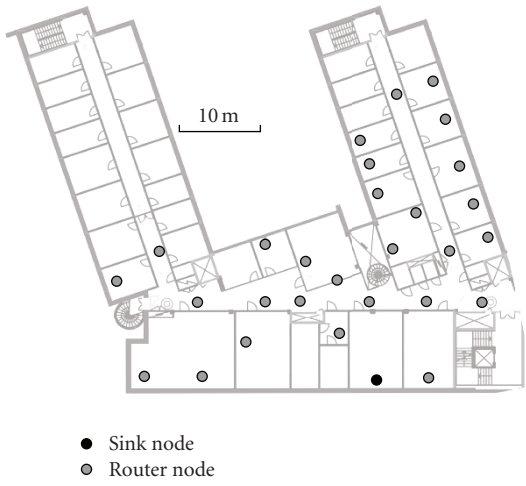


Figure 12: Network deployment at the office environment. Network included one sink node, while the router node amount varied from 2 to 28.

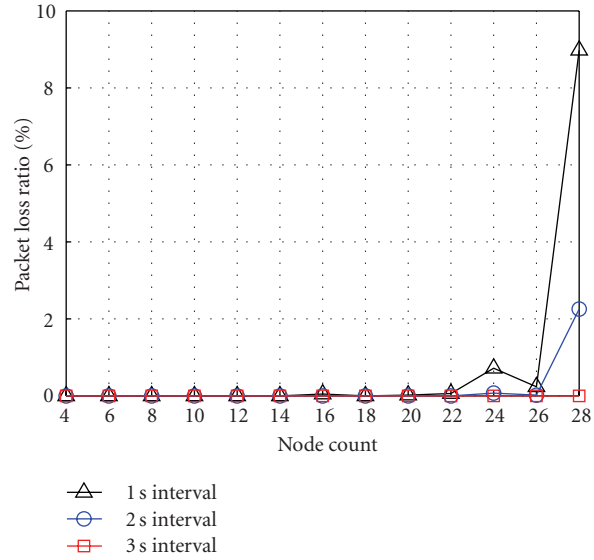


Figure 13: Average packet loss ratio as a function of node amount.

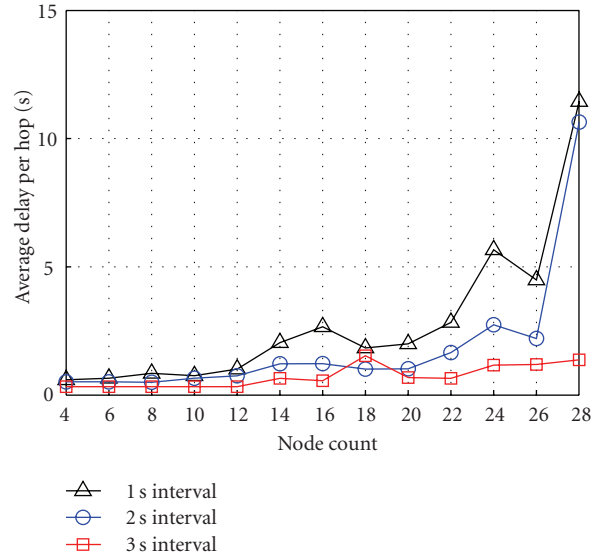


Figure 14: Average delay per hop as a function of node amount.

6.1. Experiments in Office Environment. The office environment includes typical office rooms covering an area of approximately 700 m^2. Most of the walls are wooden, but also few glass and steel walls exist. During the experiments, several WLANs and other WSNs were active producing interference to the experimented network communication.

6.1.1. Reliability and Network Delay. In the experiments, all nodes in the network sent packets with identical packet intervals which was varied according to scenario. The network included one sink node, while the router node amount varied from 2 to 28. The router nodes were added around the sink as depicted in Figure 12.

The network was experimented using one-, two-, and three-second packet intervals. Further experiments on longer packet intervals would have required significant increase to the node amount since the network did not get congested with the three-second interval even with the used maximum amount of nodes. Each interval and node count combination was measured for ten minutes.

The packet loss ratios for the experimental scenarios are plotted in Figure 13. With packet transmit interval of three seconds, there were no lost packets. With two-second transmit interval, there were no lost packets until the node amount of 28. For packet transmit interval of one second, the packet loss ratio started to increase with 26 nodes. Most likely the experienced packet losses with the one- and two-second packet intervals were caused by queue overflows due to the large amount of data, as three-second scenario did not suffer from missed packets.

Figure 14 shows the average delays per hop as a function of node amount. With packet transmit interval of three seconds, the average delay per hop ranged from 330 ms to 1.370 s. Same values with two-second transmit interval were 520 ms to 10.640 s. For packet transmit interval of one second, the delay range was from 600 ms to 11.450 s. The increase of hopwise delay with the three-second interval was quite static with no abrupt changes. The resulted network congestion with the smaller intervals and largest node counts caused more rapid increase in network delays. With the two-second packet interval, the delay started to increase more rapidly around 24 nodes, while the one-second packet interval caused a slight jump in delays at 16 nodes and faster delay increase at 24 nodes.

6.1.2. Localization Accuracy and Resilience. The localization experiments were performed with two test scenarios. Both scenarios covered the same floor area of approximately 700 m^2, but with a differing amount of anchor nodes. Scenario 1 consisted of 23 anchor nodes deployed in 21 rooms, one anchor node per room, and two in the hallway. Scenario 2 included 12 anchor nodes placed in 12 rooms,

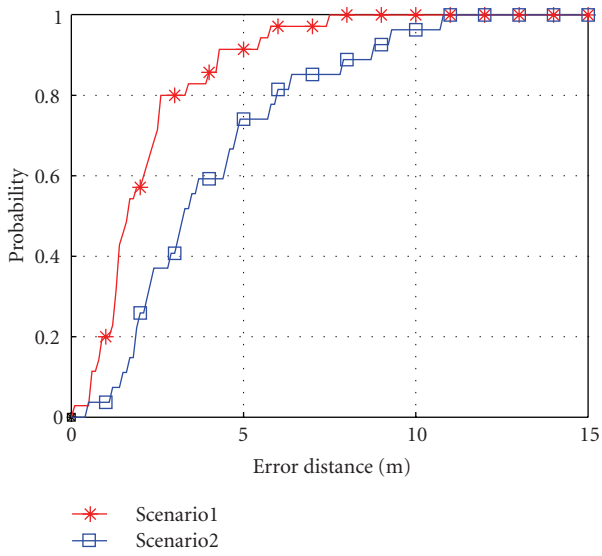


Figure 15: Cumulative distribution function results for point-based localization accuracies in Scenario 1 (23 anchor nodes) and Scenario 2 (12 anchor nodes).

approximately one anchor node in every other room. The anchor nodes were relatively evenly distributed in the covered area.

In Scenario 1, a total of 35 test locations was recorded. The test locations included at least one test location per room and six test locations in the hallway. In two of the rooms four additional test locations per room were used in order to find out how small changes in real locations affected the localization result. Scenario 2 had 27 test locations, including one test location per room (total of 21 test locations) and six test locations in the hallway.

For point-based accuracy evaluation, the bounding box center point was chosen as the resolved location for every test point. Then, absolute Euclidean distance between the real location and the estimated location was calculated. The resulting CDFs for Scenario 1 and Scenario 2 are illustrated in Figure 15. In Scenario 1, 25% of the estimated locations were within 1.3 m of the real location, 50% within 1.7 m, 75% within 2.6 m, and 90% within 4.3 m. For Scenario 2, the corresponding 25th, 50th, 75th and 90th percentile values were 2.0 m, 3.3 m, 5.8 m, and 8.8 m, respectively.

Room-level precision is given as a percentage of times the localized node room is determined correctly. When analyzing the experiment data, it was noted that the middle point of the bounding box correlated with the room the real location was situated in very well. When using bounding box middle point as the room determination criteria, the room was estimated correctly 89.7% of times in Scenario 1 and 52.4% of times in Scenario 2.

The localization system resilience against anchor node failure and incomplete data was analyzed comparing the localization performance of the two test scenarios, Scenario 2 having approximately half the anchor node amount of Scenario 1. In order to make qualitative comparison between the two test scenarios, the point-based accuracy values of Scenario 2 were normalized to the case of 23 anchor nodes. That is, the values were multiplied by $12(anchor nodes)/23(anchor nodes)$. The original and normalized values are presented in Table 1.

Table 1: Comparison of point-based accuracies for Scenario 1 and Scenario 2.

Percentile	Point-based accuracy [m]			
	Scenario 1		Scenario 2	
	Original	Normalized	Original	Normalized
25th	1.3	1.3	1.9	1
50th	1.7	1.7	3.2	1.7
75th	2.6	2.6	5.8	3
90th	4.3	4.3	8.8	4.6

As can be observed from Table 1, the normalized point-based accuracy values show a similar trend, but in Scenario 2 the accuracy deteriorates slightly faster than in Scenario 1. This can also be determined by comparing the shapes of the curves in Figure 15.

The ability to infer correct room decreased from 89.7% to 52.4% when changing from Scenario 1 to Scenario 2. This means that room level precision decreased by 41.6% as anchor node amount was reduced by 47.8%.

The comparison of the two test scenarios shows that the localization performance correlates with the amount of anchor nodes. The performance degradation is more or less linearly dependent on the anchor node amount. Thus, the algorithm can be considered to be resilient. As long as there is radio coverage over the localized area, the presented algorithm shows resilience against anchor node failure and incomplete data.

6.2. Experiments at the Hospital. The deployment at the hospital unit is depicted in Figure 16. The unit covers an area of approximately 1300 m^2. The deployment includes nine sink nodes, 41 router nodes, and 12 mobile nodes.

The experiments included a total of 44 alarms triggered in the rooms and the corridors of the deployment area. All the alarms were registered in the WSN server. Thus, the reliability of the alarms was 100%. 90% of the alarms were localized to the correct room, and all were localized within two rooms (correct or the neighboring room).

The delays are illustrated in Figures 17 and 18. 95% of the alarms packets were forwarded in under 2.3 s and 97% under 3.2 s. Actually, as Figure 18 demonstrates, only one packet was forwarded in over 3.2 s. The minimum delay was 0.8 s, and the maximum was 9.7 s.

6.3. Node Power Consumption. The measured router node power consumption is static and independent of the network activity. Average router node power consumption is 72 ± 1 mW. This gives a 138-hour lifetime expectation using 2000 mAh power source which is a conservative estimate for two AA batteries. This suggests that for long-term deployments, the routers should be equipped with big enough batteries or be mains powered.

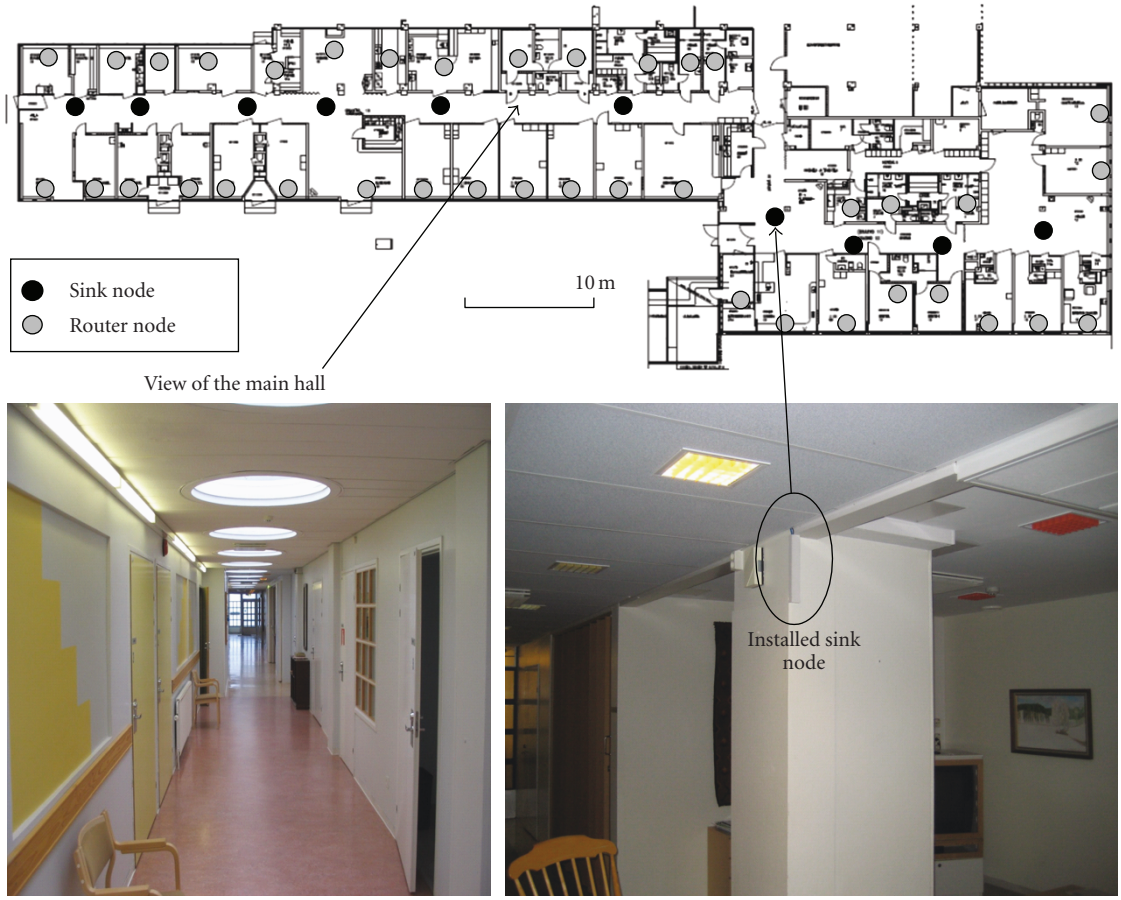


Figure 16: Network deployment at the hospital unit. The deployment includes 9 sink nodes, 41 router nodes, and 12 mobile nodes.

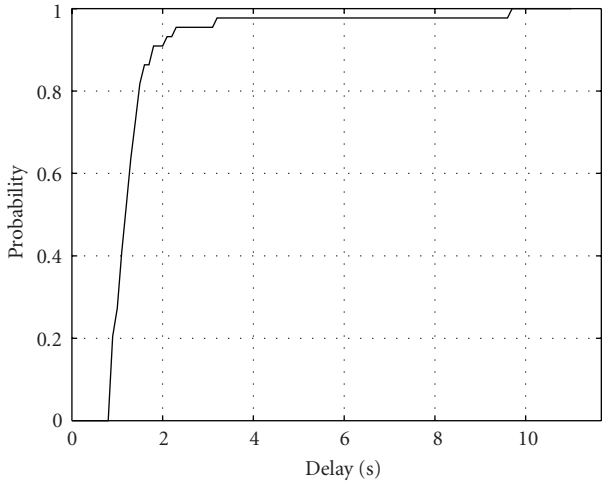


Figure 17: Test alarm delay CDF.

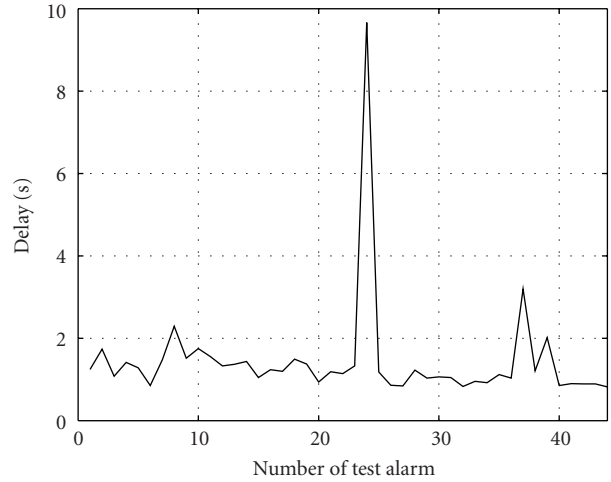


Figure 18: Delays for individual test alarms.

For the mobile nodes, the measurements were conducted using varying access cycle lengths of 1/4, 1, 4, 16, and 32 s. The power consumption ranges from 550 μW to 4500 μW. The estimated mobile node lifetime using the 2000 mAh power source is between 3 and 26 months with the used access cycle values. The mobile node lifetime does not double when the access cycle is doubled, because the sleep mode power consumption of the mobile node is not zero.

Table 2: Comparison of the hospital security WSN and related work against the user requirements.

	User Requirements					
Protocol	Wireless mobile nodes	Room-level localization	Reliability	Delay	Network lifetime	Installation and maintenance
Hospital security WSN	Yes	Yes	High	Low	Long	Easy
Random-access MAC protocols	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	Short	Easy
Scheduled contention-access MAC protocols	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	Medium for static nodes Short for mobile nodes	Easy
TDMA-based MAC protocols	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	Long for static nodes Short for mobile nodes	Easy
SPEED	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	MAC-dependent for static nodes Short for mobile nodes	Easy
MMSPEED	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	MAC-dependent for static nodes Short for mobile nodes	Easy
RPAR	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	MAC-dependent for static nodes Short for mobile nodes	Easy
Akkaya and Younis [22]	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	MAC-dependent for static nodes Short for mobile nodes	Easy
GRAB	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	MAC-dependent for static nodes Short for mobile nodes	Easy
Pothuri et al. [20]	Yes	Possible (e.g., with our algorithm)	Depends on implementation	Medium to high	Short	Easy
Sniper detection system [24, 25]	No	No	Not documented	Low		

6.4. Hospital Security WSN and Related Work: Comparison against the User Requirements. In this section, we compare the hospital security WSN and the related work against the presented user requirements. The comparison is summarized in Table 2.

All the related MAC protocols make wireless mobile devices possible. However, as shown in [12], the power consumption of the mobile nodes is high reducing network lifetime. The related MAC protocols incur medium to high channel access delays. In the random-access MAC protocols, the channel access delay is increased due to the long preambles. In scheduled contention-access and TDMA-based MAC protocols, a dedicated time slot has to be waited and allocated before transmission.

SPEED, MMSPEED, and RPAR make routing decisions reactively. This increases communication delay as route discovery and setup take place during the data forwarding procedure. The routing protocols presented by Akkaya and Younis [22], Pothuri et al. [20], and the GRAB protocol are proactive and can achieve low delays if paired with a MAC protocol presenting low channel access delays.

All the related routing protocols form a flat topology where all nodes are assigned equal roles or functionality. This reduces the lifetime of mobile nodes as also they need to perform routing. Routing requires fresh neighborhood information resulting in frequent energy-consuming neighbor discoveries. Furthermore, in [20] two different power level radios are used increasing also the energy consumption of static nodes.

In general, room-level localization could be achieved using the related protocols and, for example, the localization algorithm presented in this paper. Reliable data transmission could also be implemented in the related protocols using, for example, link level acknowledgements. As all the related protocols are designed for WSNs, they are autonomous in nature making installation and maintenance easy.

The WSN-based sniper detection and localization system [24, 25] does not consider node mobility. Thus, mobile node room-level localization is also absent. In an experimental scenario of 56 nodes and 4 sinks, an average latency of 2 seconds was experienced giving low communication delay. However, more accurate results including path length, maximum delays, or reliability are not reported. The prototype achieved only 12-hour lifetime with four AA batteries.

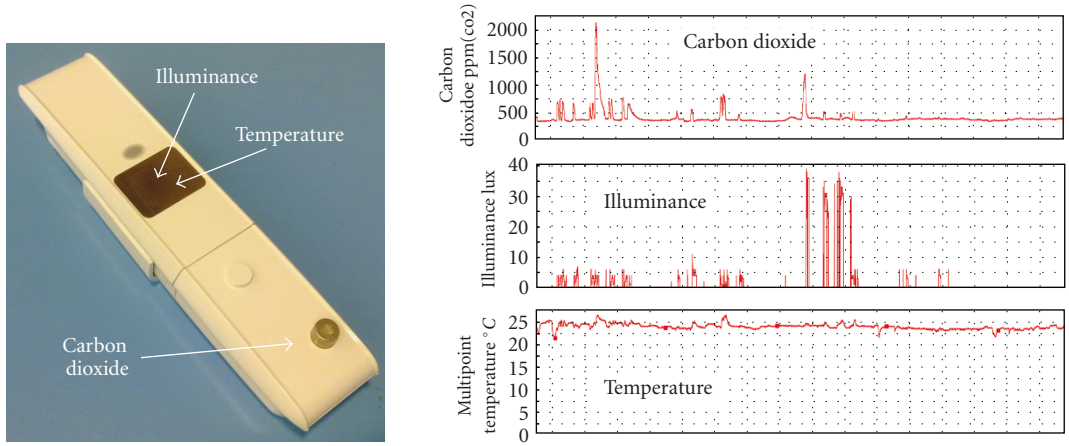
As demonstrated in this paper, the hospital security WSN meets all the presented user requirements. The design provides scalability and different QoS levels. Critical data is forwarded reliably and with low delays. Possibility for various measurements is included without decreasing the reliability and delay performance.

7. Hospital Security WSN Application Space

Using the various sensors and actuator control of the hospital security WSN nodes, a vast number of applications can be implemented with the same network and hardware. The main application domains include physiological measurements and patient monitoring, asset management and logistics, and building automation, security, and energy conservation.

(i) *Physiological Measurements and Patient Monitoring.* The condition of patients can be monitored with physiological measurements, such as temperature and pulse. The measurements can be augmented with patient location information. Also, the devices used to measure and localize patients can be used as wireless nurse call buttons.

(ii) *Asset Management and Logistics.* Localization enables the tracking of key personnel and equipment. Machines and products can be tracked continuously to optimize logistics management.



(a) (b)

Figure 19: Examples of possible measurements using the hospital security WSN.

(iii) *Building Automation, Security, and Energy Conservation.* Motion detectors and magnetic switches on doors and windows can be used to detect unauthorized access to buildings. Localization and mobile nodes enable access control. The power and water consumption, temperatures, ventilation, and lighting of a building can be monitored and controlled. Figure 19 illustrates few examples of monitoring applications.

8. Conclusions

In this paper, a novel WSN design called hospital security WSN was presented. The paper included the user requirement specification, design and implementation, and hospital pilot deployment and experiments. The user requirements consisted of wireless devices with room-level localization, reliable low-latency alarming, long network lifetime, and ease of installation and maintenance. With the hospital security WSN, personnel can send wireless alarms in threatening situations, receive acknowledgements telling that help is on its way, make various environmental and physiological measurements, and use actuators.

The hospital security WSN utilizes a heterogeneous communication topology including sink, router, and mobile nodes. The router nodes have a high-duty cycle, and they form a multi-hop network for low-latency data forwarding to sink nodes. The mobile nodes have low-duty cycles and are highly energy-efficient.

A full scale pilot network was implemented for deployment and experiments. The network consists of real resource constrained WSN nodes communicating in the 2.4 GHz frequency band. The network was experimented in two places: first in an office environment and after this in the hospital environment. Currently the pilot network is in use at the hospital unit.

The experienced delays were in the range of seconds, and message forwarding reliability was 100% until network became highly congested. Room-level localization accuracy was reached. The mobile nodes reached power consumption ranging from 4500 μW to 550 μW when their access cycle was varied from 1/4 s to 32 s. These values indicate lifetime of several months to years even when used with small batteries.

Currently we are extending the deployment also to another unit at the hospital. The future work includes the integration of more physiological signal measurements, such as EKG, to the hardware platform. Also, protocol enhancements, such as delay prediction and optimization of router node energy consumption, will be investigated.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] D. Culler, D. Estrin, and M. Srivastava, "Guest editors' introduction: overview of sensor networks," *Computer*, vol. 37, no. 8, pp. 41–49, 2004.

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[4] Y. Li, C. S. Chen, Y. Q. Song, and Z. Wang, "Real-time QoS support in wireless sensor networks: a survey," in *Proceedings of the 7th IFAC International Conference on Fieldbuses & Networks in Industrial & Embedded Systems (FeT '07)*, pp. 373–380, 2007.

[5] M. Kohvakka, M. Hännikäinen, and T. D. Hämäläinen, "Ultra low energy wireless temperature sensor network implementation," in *Proceedings of the 16th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '05)*, vol. 2, pp. 801–805, September 2005.

[6] M. Kohvakka, M. Hännikäinen, and T. D. Hämäläinen, "Wireless sensor network implementation for industrial linear position metering," in *Proceedings of the 8th Euromicro Conference on Digital System Design (DSD '05)*, vol. 2, pp. 267–275, IEEE Computer Society, Washington, DC, USA, 2005.

[7] M. Kuorilehto, J. Suhonen, M. Kohvakka, M. Hannikainen, and T. D. Hämäläinen, "Experimenting TCP/IP for low-power wireless sensor networks," in *Proceedings of the 17th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06)*, pp. 1–6, September 2006.

[8] J. Suhonen, M. Kohvakka, M. Hännikäinen, and T. D. Hämäläinen, "Design, implementation, and experiments on outdoor deployment of wireless sensor network for environmental monitoring," in *Proceedings of the 6th International Workshop on Architectures, Modeling, and Simulation (SAMOS '06)*, vol. 4017 of *Lecture Notes in Computer Science*, pp. 109–121, Samos, Greece, July 2006.

[9] M. Kuorilehto, J. Suhonen, M. Hännikäinen, and T. D. Hämäläinen, "Tool-aided design and implementation of indoor surveillance wireless sensor network," in *Proceedings of the 7th International Workshop on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS '07)*, vol. 4599 of *Lecture Notes in Computer Science*, pp. 396–407, Samos, Greece, July 2007.

[10] M. Kohvakka, M. Hännikäinen, and T. D. Hämäläinen, "Wireless sensor prototype platform," in *Proceedings of the 29th Annual Conference of the IEEE Industrial Electronics Society (IECON '03)*, vol. 2, pp. 1499–1504, Roanoke, Va, USA, November 2003.

[11] M. Kohvakka, T. Arpinen, M. Hännikäinen, and T. D. Hämäläinen, "High-performance multi-radio WSN platform," in *Proceedings of the 2nd International Workshop on Multi-Hop Ad Hoc Networks: From Theory to Realityn (REALMAN '06)*, pp. 95–97, ACM, May 2006.

[12] V. A. Kaseva, M. Kohvakka, M. Kuorilehto, M. Hännikäinen, and T. D. Hämäläinen, "A wireless sensor network for RF-based indoor localization," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 731835, 2008.

[13] M. Kohvakka, J. Suhonen, M. Kuorilehto, V. Kaseva, M. Hännikäinen, and T. D. Hämäläinen, "Energy-efficient neighbor discovery protocol for mobile wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 1, pp. 24–41, 2009.

[14] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 95–107, ACM, Baltimore, Md, USA, November 2004.

[15] 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, pp. 493–506, 2004.

[16] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN)*, IEEE Std. 802.15.4, 2003.

[17] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Personal Communications*, vol. 7, no. 5, pp. 16–27, 2000.

[18] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: a stateless protocol for real-time communication in sensor networks," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems*, pp. 46–55, May 2003.

[19] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 6, pp. 738–754, 2006.

[20] P. K. Pothuri, V. Sarangan, and J. P. Thomas, "Delay-constrained, energy-efficient routing in wireless sensor networks through topology control," in *Proceedings of IEEE International Conference on Networking, Sensing and Control (ICNSC '06)*, pp. 35–41, April 2006.

[21] O. Chipara, Z. He, G. Xing et al., "Real-time power-aware routing in sensor networks," in *Proceedings of the 14th IEEE International Workshop on Quality of Service (IWQoS '06)*, pp. 83–92, June 2006.

[22] K. Akkaya and M. Younis, "An energy-aware QoS routing protocol for wireless sensor networks," in *Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCSW '03)*, p. 710, IEEE Computer Society, Washington, DC, USA, 2003.

[23] F. Ye, G. Zhong, S. Lu, and L. Zhang, "GRAdient broadcast: a robust data delivery protocol for large scale sensor networks," *Wireless Networks*, vol. 11, no. 3, pp. 285–298, 2005.

[24] G. Simon, M. Maróti, Á. Lédeczi et al., "Sensor network-based countersniper system," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 1–12, November 2004.

[25] P. Volgyesi, G. Balogh, A. Nadas, C. B. Nash, and A. Ledeczi, "Shooter localization and weapon classification with soldier-wearable networked sensors," in *Proceedings of the 5th International Conference on Mobile Systems, Applications and Services (MobiSys '07)*, pp. 113–126, June 2007.

[26] "TinyOS hardware platforms," 2009, http://www.tinyos.net/scoop/special/hardware.

[27] M. Maróti, "Directed flood-routing framework for wireless sensor networks," in *Proceedings of the 5th ACM/IFIP/USENIX International Conference on Middleware (Middleware '04)*, vol. 3231 of *Lecture Notes in Computer Science*, pp. 99–114, Springer, 2004.

[28] L. G. Roberts, "Aloha packet system with and without slots and capture," *ACM SIGCOMM—Computer Communication Review*, vol. 5, no. 2, pp. 28–42, 1975.

[29] J. Syrjarinne, *Studies of modern techniques for personal positioning*, Ph.D. dissertation, Tampere University of Technology, Tampere, Finland, March 2001.

[30] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Computer Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[31] A. Savvides, H. Park, and M. B. Srivastava, "The n-hop multilateration primitive for node localization problems," *Mobile Networks and Applications*, vol. 8, no. 4, pp. 443–451, 2003.

[32] T. Parker and K. Langendoen, "Refined statistic-based localisation for ad-hoc sensor networks," in *Proceedings of IEEE Global Telecommunications Conference Workshops (GLOBECOM '04)*, pp. 90–95, Dallas, Tex, USA, November-December 2004.

[33] "SOAP Version 1.2 W3C Recommendation," 2007, http://www.w3.org/TR/soap12-part1/.