Applying Wireless Sensor Networks in Fire Fighting

Chunlei An and Andreas Timm-Giel

Institute of Communication Networks, Hamburg University of Technology,
Schwarzenbergstr. 95E, 21071 Hamburg, Germany
{chunlei.an,timm-giel}@tuhh.de

Abstract. Fire fighters often work in dangerous environments, therefore protection is essential. Nowadays fire fighters are equipped with different types of devices, each of which supplies a specific functionality. This paper studies the possibility of integrating some of these functionalities into one intelligent glove, which has a build-in sensor node. Merging different functionalities into one device will reduce the number of equipments that a fire fighter must carry. The concept of networking the intelligent gloves using Wireless Sensor Networks (WSNs) is validated by doing application requirements analysis, transmission range experiments, and performance evaluations of a dedicated routing protocol. Results show that the IEEE 802.15.4 based WSN can be applied in fire fighting scenarios.

Keywords: Wireless Sensor Networks, Fire Fighting.

1 Introduction

Wireless sensor networks play an increasingly relevant role in emergency and rescue scenario. Nowadays fire fighters use different equipment for different functionalities. Each fire fighter needs one communication unit to keep in contact with each other. This type of communication can be disturbed in noisy environments. Furthermore, each fire fighter also needs to carry a dead man alarm, which generates acoustic alarms when the fire fighter becomes incapacitated. One severe shortcoming of such a device is the limited alarming range. This means that only fire fighters who are close enough can be informed by the alarms, and it is also not reliable in noisy environments. In some cases the fire fighters have to risk their own safety for checking certain surroundings. This can happen when a fire fighter wants to open the door of a close room. Currently the fire fighters need to take off one of the gloves, and put the back of the hand close to the door for estimating the inner room temperature. This may be dangerous if the outside temperature is already high, or the fire fighter touches the door accidentally .

The GloveNet project [1] is funded by the German Federal Ministry of Eduction and Research (BMBF), and is targeting to solve the aforementioned problems. The main concept of this project is to explore the possibility of building a WSN using intelligent gloves, which have compact sensor modules integrated.

K. Pentikousis et al. (Eds.): MONAMI 2011, LNICST 97, pp. 386–395, 2012.

This module should provide alternatives to the functionalities mentioned before, so that the fire fighters can be better protected.

One example is using gestures as complement to the voice communications. Imagine that a fire fighter finds more than one wounded persons and needs assistance from his colleagues. He will ask for backup over the communication unit, and at the same time, he will also make a predefined gesture using his glove. This gesture signal will be transmitted to other fire fighters over the GloveNet. In this case, the other fire fighters will not miss the assistance requirements through the vibrational feedback from the gloves even in noisy environments.

This paper focuses on the data transmissions over the GloveNet. The rest of the paper is organized as follows: Section 2 presents the application requirement analysis; Section 3 and 4 explain transmission range study performed and the routing protocol design respectively; In Section 5 the performance of the proposed routing protocol is evaluated, and finally conclusions are drawn in Section 6.

2 Application Requirement Analysis

First of all, it is important to see whether the requirements from the application can be satisfied by the capability of WSNs. User studies and in depth analysis of the application scenarios show that it is required to read and transmit different specific parameters. Some of these parameters need to be checked periodically, e.g., the environmental temperature, the air pressure around the fire fighter, and the life sign of each fire fighter. From a communication network's point of view, this information is needed by the command post for monitoring the status of each fire fighter. Some other signals are not read regularly, but rather event driven, such as a predefined gesture.

Various standards are available for local area wireless communication. Table 1 lists some of the commonly used standards and their specifications. It is not difficult to see that 802.15.4 has several advantages over the other standards, such as relatively larger transmission range, low complexity and very low power consumption. Even though it has lower data rates, it still fulfills the application's requirements.

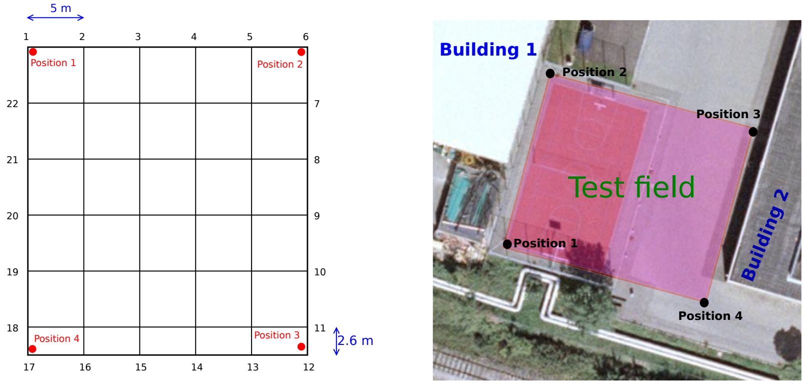
At the site of operation there is normally no wireless communication infrastructure (the existing one cannot be accessed or has been damaged). Due to this fact, a WSN working in multi-hop ad hoc [3] mode is required.

3 Transmission Range

In the previous section it has been proved that the application requirements can be fulfilled by the processing capability of a WSN, and the next question comes up is the transmission range of a sensor node. Is it actually possible to provide adequate coverage for the fire fighters? The answer is hardware dependent. In this paper the GloveNet sensor nodes use the radio frequency of 868 MHz, which

Table 1. Wireless standards comparison

	802.15.4	802.11	802.15.1	802.15.4a
Data Rate	20, 40 and 250 kbit/s	11 and 54 Mbit/s	1 Mbit/s	100-500 Mbit/s
Range	10-100m	50-100m	10m	<10m
Operating Frequency	868MHz	2.4 and 5GHz	2.4GHz	3.1-10.6 GHz
Complexity	Low	High	High	Medium
Power Consumption	Very low	High	Medium	Low



(a) Test field illustration with 22 predefined locations

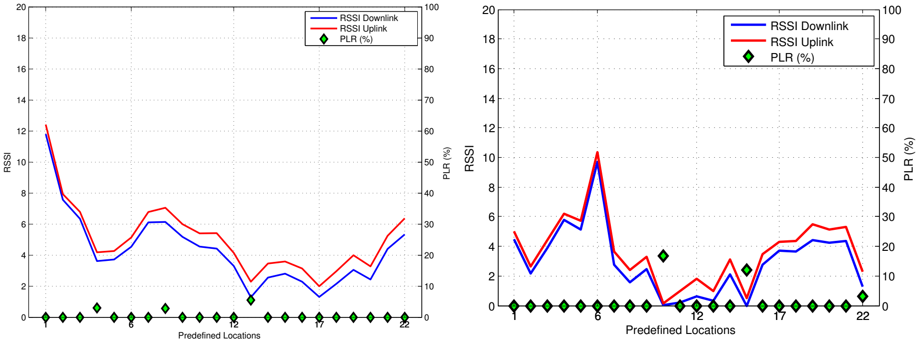
(b) Google map of the test field

Fig. 1. Test field for transmission range

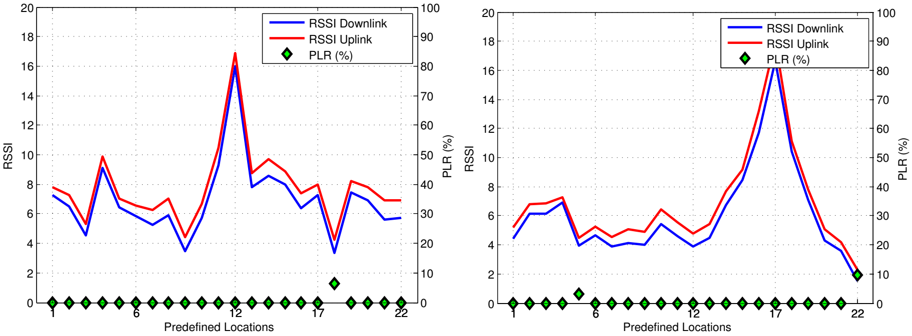
has lower data rate, but provides theoretically longer transmission range and less interferences than the commonly used 2.4 GHz frequency band.

A series of field experiments have been designed and carried out to see the actual performance of the radio transceiver and the antenna. Experiments were conducted in different environments. Due to the space limitation, here only the results taken from the open area will be shown and analyzed. Fig. 1 depicts the experiments. In this experiment four fire fighters stand at the four corners of the chosen area, and one fire fighter moves from position 1 (the upper-left corner), and go through all the predefined locations. At each location the mobile fire fighter stops and wait until the completion of the data transmission. This procedure is repeated by the mobile fire fighter at each location.

Results are shown in Fig. 2. Fig. 2a depicts the variation of the Received Signal Strength Indication (RSSI), as well as the Packet Loss Rate (PLR) between the mobile fire fighter and the fixed fire fighter standing at position 1. The results show the change of the link quality between a pair of fire fighters over distance. It can also be observed that at some positions the PLR is high even with relatively good RSSI, for instance at position 4 and 8. One possible reason



(a) Fixed node 1 (b) Fixed node 2



(c) Fixed node 3 (d) Fixed node 4

Fig. 2. RSSI and PLR between the mobile fire fighter and four stationary fire fighters

is that the experiment field is also partly surrounded by houses (as shown in Fig. 1b), which may add unexpected fading effects to the ongoing data transmission, hence impact the data reception. Similar behaviour can also be seen in the data collected between the mobile fire fighter and the rest three fixed fire fighters (see Fig.2b, 2c and 2d).

Much higher packets loss rates are observed in Fig. 2b. This is due to the instable connection between the antenna and the radio module on this sensor node, and it will be solved in the later produced sensor nodes.

Another thing to mention is that in all the four plots, the link quality of the uplink (from the fixed nodes to the mobile node) is better, or at least as good as that of the downlink (from the mobile node to the fixed nodes). This maybe is due to the fact that the mobile node gets power supply from the laptop, so that it has better reception than the battery powered fixed nodes. Further experiments are planned to verify this explanation.

Results of transmission range tests show that the links between sensor node pairs are symmetric, and a single hop transmission range of around 37.2 meter (diagonal of the experiments field) can be provided by the current sensor module. Larger coverage can be easily obtained by using multi-hop communication.

4 Routing Protocol

An overview of the routing protocols in WSNs is given in [7]. Most of the existing routing protocols in WSNs were designed to serve a certain purpose, and support to mobility was not a main concern. However, in fire fighting the move of the fire fighters leads to a frequent network topology change, and this requires the routing protocol to be able to handle network dynamics. A broadcasting based routing protocol, EMergency ROuting (EMRO), is proposed in [4] for the communication in fire fighting. Due to the nature of broadcasting, EMRO outperforms other traditional routing protocols in terms of mobility handling. However, it can only work with linear network topologies nicely, but has poor performance in non-linear network topologies.

Therefore a new protocol, Beacon Based Routing (BBR), is designed and implemented for GloveNet. This routing protocol is based on the distance vector algorithm [8]. This means that neighboring sensor nodes keep exchanging distance vectors until each of them finds a route to every other nodes in the network. The distance can be any metric, and here it is defined as the number of hops. Afterwards beacon messages are sent periodically for monitoring the routes' availability. A routing entry is considered invalid, if there is no beacon message being received from that specific neighboring node within a given time period. However, this approach can cause delay in broken link detection, which is heavily dependent on the aforementioned time period. Therefore, dynamic neighbor update and mobility detection are investigated, in order to get a broken link detected as soon as possible. These features are achieved with the help of continuous exchange of beacons.

4.1 Dynamic Neighbor Update

Dynamic neighbor update means that each node is aware of its immediate one-hop-neighbors at all times. To achieve this, all nodes are periodically sending out beacons. Based on the reception of these beacons, each node maintains a list of its direct neighbors.

Once a node detects a beacon from a previously unknown node, the receiving node will add the sending node to its own neighbor list. An entry in this dynamically created list contains the neighbor's address, the RSSI of the last received beacon, and a time to live (TTL) integer. The RSSI value is used for the mobility detection and the TTL value determines the lifetime of the connection as follows.

To detect the loss of a connection, a timer has been implemented, which is started periodically. Each time the timer expires, every entry of the neighbor list will be processed. First the TTL value will be decreased by one. If the TTL value is now equal to zero, the processing node will assume the connection to this node to be lost. It will therefore delete this entry from the neighbor list. The node will also change its routing entries and send out a lost message.

Every time a node receives the beacon of an already known neighbor it will search the according entry in the neighbor list and reset the TTL value to the default value. This will prevent this neighbor from timing out. Based on the above described method of maintaining a neighbor list, three parameters are considered critical for the duration of a connection: the TTL value, the amount of time it takes for the TTL timer to fire and the beacon sending frequency. These values have to be tuned so that a lost connection is detected as fast as possible, yet a few lost beacons should not result in a dropped connection.

4.2 Mobility Detection

Mobility Detection means that one node can detect if itself is moving or that other nodes are moving relatively to it. In this paper a method based on RSSI is implemented and tested. This method tracks the RSSI value of the nodes in the immediate neighborhood. This information is used to decide which nodes are moving relatively to the currently tracking node.

RSSI Based Mobility Detection. To detect if a neighbor is moving either towards or away from a node, the node uses the information from the neighbor list. It works in conjunction with the above described procedure. On reception of a packet the receiving node will check its neighbor list for the entry of the sender. If the sender is known, the RSSI value of the new packet will be compared to the previously saved value. Otherwise, it will be added to the list.

In the case that the RSSI value has decreased more than the specified threshold value, the neighbor will be assumed to be moving away. The TTL value for this neighbor will then be reduced, which effectively implies that the connection times out twice as fast. It has been chosen to halve the TTL value, but this has only been chosen for testing the concept and the value can probably be optimized further.

The parameters that influence the speed of a node movement detection by method are the frequency of sent beacons and the threshold value for the RSSI.

If the beacon frequency is too high, it could theoretically happen that the difference between any two consecutively measured RSSI values are always lower than the threshold, even if the node is moving. Yet this has not been observed in the simulations.

This method has been proven to work quite nicely in TOSSIM [5]. The reduction of the connection timeout then reduced the packet loss in simulation scenarios with moving nodes by about 10%.

5 Results Analysis

In this section the performance of the proposed routing protocol is evaluated through simulations. The TOSSIM simulator is used.

Various scenarios have been created, in order to evaluate different aspects of the routing protocol. In this paper two things are mainly concerned, namely the mobility handling and the transmission packet loss rate. Mobility handling is important, because in reality the fire fighters move will cause frequent change to network topology. The routing protocol must be able to detect the change and adapt itself accordingly. Packet loss rate is also studied using different network topologies, because this metric directly affects the reliability of the data transmission, hence the overall usability of the whole GloveNet project.

These two aspects are discussed in the following two subsections.

5.1 Mobility Handling

The mobility handling is tested separately due to the limitation of TOSSIM. Currently the TOSSIM simulator in TinyOS 2.x does not support mobility. However, this can be done manually by taking several snapshots to the whole simulation period. For the sake of simplicity, a line scenario is used here. This scenario includes five stationary nodes, and one mobile node (as depicted in Fig. 3). At the beginning the mobile node, in this case node n6, stays near node n0, therefore it has connection to n0 and n1. Considering the closer distance, the received power measured at n0 is set to -40 dBm, while the the one measured at n1 is -60 dBm. This is considered as the first snapshot of the network. In the second snapshot, node n6 moves to the position between n0 and n1. Both nodes receive the signal from n6 with -40 dBm. In the next snapshot, node n6 has moved close to n1. Now it has connections between n0, n1 and n2 respectively (as shown in Fig. 4c). Considering the relatively larger distance between n6 and n0, as well as n6 and n2, n0 and n0 have poorer reception (-60 dBm) than n1 (-40 dBm). In the fourth snapshot, node n6 reaches the position between n1 and n2. Here the connection between n6 and n0 is lost, whereas the signal reception at n2 is improved to -40 dBm. This process is repeated, until n6 stops besides n5 at the end.

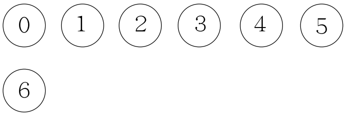
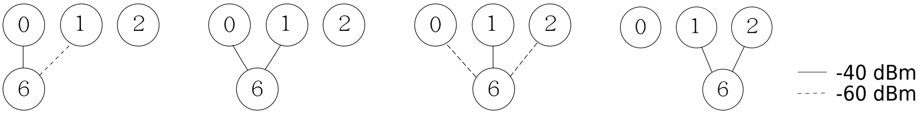


Fig. 3. Line topology of 7 nodes

In the simulation the mobile node is supposed to move at the speed of 1.5 meter per second, which is the fast walking speed of human being [6]. The distance between each pair of adjacent stationary nodes is 15 meters, therefore



(a) Snapshot 1 (b) Snapshot 2 (c) Snapshot 3 (d) Snapshot 4

Fig. 4. Snapshots of network topology

the mobile node needs 10 seconds to travel from one node to the next nearby node. Three snapshots are taken over this period of time (as depicted in Fig. 4a, 4b, and 4c), so it is reasonable to say that the mobile node stays at each snapshot for around 3.3 seconds. So has the simulation time been controlled.

Besides the aforementioned mobility detection algorithm, there are two more parameters, which have impact on broken link detection, namely the maximum time to live (MAX_TTL), and the length of each time to live period (TIMER_PERIOD_TTL). Table 2 shows different parameter settings and their impact to the broken link detection efficiency. “Time to detection” refers the time needed for the algorithm to detect a broken link.

Table 2. Testing results for a node moving along a line

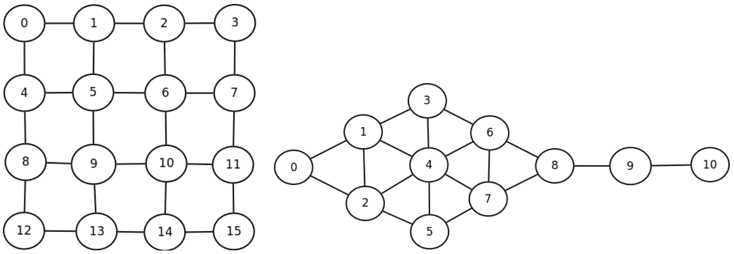
MAX_TTL	TIMER_PERIOD_TTL (ms)	Time to detection (s)
8	1000	5.088
6	1000	3.792
8	500	2.074
6	500	1.322

The maximum amount of time needed for detecting a broken link can be calculated as MAX_TTL*TIMER_PERIOD_TTL. The observed average of “Time to detection” is upper bounded by this value. The smaller the value of MAX_TTL and TIMER_PERIOD_TTL, the faster a broken link can be found.

The simulation results show that the proposed routing protocol can handle mobility inside the network, and furthermore, the performance can be improved by fine tuning the related parameters.

5.2 Packet Loss Rate

To study the performance of the proposed routing protocol in terms of packet loss rate, simulations are run using various network topologies. As it has been stated in the previous section, one of the main motivations for creating a new routing protocol is that EMRO can only deal with linear topology. So the focus of this section is to benchmarking the performance of the proposed routing protocol against EMRO using several nonlinear network topologies. In this paper two of them are chosen for the explanation, namely the four by four grid topology and the diamond topology (see Fig. 5).



(a) 4x4 grid topology (b) Diamond topology

Fig. 5. Non-linear network topologies for PLR evaluation

In the four by four grid network node n0 is sending data to n15, and in the diamond topology n0 is transmitting packets to n10. In both cases the other intermediate nodes are just behaving as relays.

Results in Table 3 show that the proposed routing protocol outperforms EMRO in both cases. The difference is more obvious in the four by four grid network. This is because EMRO is a broadcasting based algorithm, and in this case many intermediate nodes, especially those in the middle of the grid, try to forward the copies of the same data message. This introduces unnecessary medium access contention, hence leads to the loss of packets.

Table 3. Performance comparison against EMRO in non-linear network topologies

(a) 4x4 grid topology

Data Loss Rate		
	EMRO	BBR
Run 1	38.7%	1%
Run 2	37.6%	0.2%
Run 3	38.4%	0.1%
Average	38.2%	0.43%
Stdev	0.57%	0.49%
95% CI	(36.82%, 39.65%)	(0, 1.66%)

(b) Diamond topology

Data Loss Rate		
	EMRO	BBR
Run 1	3.6%	0.2%
Run 2	3.9%	0.5%
Run 3	3.2%	0.1%
Average	3.6%	0.27%
Stdev	0.35%	0.21%
95% CI	(2.69%, 4.44%)	(0, 0.78%)

In both cases the lower limits of the 95% confidence interval for BBR are set to 0. This is because that the small sample size (three simulation runs) leads to negative lower limits, which are meaningless in terms of percentage.

6 Conclusions and Future Work

This paper studies the feasibility of applying WSN to fire fighting. The idea is to create a network of smart gloves, each of which has a sensor node integrated. First of all the requirements from the application have been analyzed. The conclusion from the analysis is that IEEE 802.15.4 based WSN is capable to fulfill the application's requirements. As the next step, experiments have been designed and conducted to see the transmission range of the designed sensor modules. Results show that a single sensor module can cover the area around it with the radius of around 37 meters. Large coverage can be achieved by using multi-hop communication. An dedicated routing protocol using distance vector has been implemented and evaluated. It is proved able to handle the network dynamic, which is mainly caused by the movement of fire fighters. Moreover, this routing protocol outperforms the EMRO protocol in coping with more complicated network topologies. Concluding all the previous steps, it is safe to say that IEEE 802.15.4 based WSN is a suitable technology for fire fighting scenarios.

Due to the limitation of the TOSSIM simulator, the network mobility is only evaluated in linear topology. In the future the proposed routing protocol will be tested in real testbeds, so that the mobility handling in more complicated network topologies can be evaluated.

Acknowledgement. The GloveNet project is funded by the German Federal Ministry of Education and Research (BMBF). Thanks to IMSAS, MRC from the University of Bremen, the fire fighting team of Reutlingen, Wuerth Elektronik GmbH, Binder Elektronik GmbH, and W+R GmbH.

References

1. GloveNet Project, `http://www.mrc-bremen.de/glovenet`
2. TinyOS: Open Source Operating System, `http://www.tinyos.net`
3. Corson, S., Macker, J.: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, Internet Engineering Task Force (January 1999)
4. An, C., Timm-Giel, A., Goerg, C.: Virtual Sensor Network Lifeline for Communications in Fire Fighting Rescue Scenarios. In: 70th Vehicular Technology Conference, Alasga, pp. 1–5 (2009)
5. TinyOS Tutorial: TOSSIM, `http://docs.tinyos.net/index.php/TOSSIM`
6. Carey, N.: Establishing Pedestrian Walking Speeds. ITE Student Chapter (2005)
7. Al-Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: a survey. J. IEEE Trans. on Wireless Communications 11(6), 6–28 (2004)
8. Kurose, J.F., Ross, K.W.: Computer Networking: A Top-Down Approach, 5th edn. Addison Wesley, Boston (2009)