Son, V.Q., Wenning, B.-L., Timm-Giel, A. , Görg, C.: A Model of Wireless Sensor Networks using Context-Awareness in Logistic Applications. Proceedings of the 9th International Conference on Intelligent Transport System Telecommunications (ITST 09), pp. 2-7.

A Model of Wireless Sensor Networks using Context-Awareness in Logistic Applications

Vo Que Son, Bernd-Ludwig Wenning
Communication Networks
University of Bremen
Bremen, Germany
{son, wenn}@comnets.uni-bremen.de

Andreas Timm-Giel, Carmelita Görg
Communication Networks
University of Bremen
Bremen, Germany
{atg, cg}@comnets.uni-bremen.de

***Abstract*—Although Wireless Sensor Networks (WSNn) are designed to operate with low power consumption, much of the research in this field focuses on improving the efficiency of resource usage. In many scenarios, WSNs are configured to monitor and transmit the observed data periodically. This can lead to duplication of traffic in the network if most of the sensed data does not change over time under normal conditions. In this paper, a flexible context-aware model of Wireless Sensor Networks (WSNs) is presented for use in logistic contexts to reduce that unnecessary information. By being aware of contexts, WSNs know which information is significant to transmit. Generated traffic load and energy efficiency are considered to illustrate the advantages of the proposed context-aware model.**

Keywords: Logistics, Wireless Sensor Networks, routing, application, context-awareness

I. INTRODUCTION

With the development of digital electronics, low-cost, low-power, distributed processing sensor nodes have been proposed for use in a wide range of applications such as environmental monitoring, environment observation. Sensor nodes are electronic devices which typically contain sensors, a microcontroller, a radio communication chip and other peripherals. They can communicate with other nodes to form self-organizing WSNs. Featuring sensing, computation and communication capabilities, such as ad-hoc networking and distributed processing, WSNs allow telemetry, information collection and information management, which can be suitable for logistic applications. This can help to introduce a new logistic system which consists of intelligent logistic items that can autonomously control their transport processes.

There are many deployments of WSNs in different fields, for example, a sensor network in [1] is deployed by Harvard university to collect real data from Reventador, an active volcano in Ecuador, SensorScope [2] is used to monitor the environmental information in the I&C building on EPFL campus (Switzerland), or GlacsWeb [3] is designed to gather the data of glaciers autonomously at Briksdalsbreen in Norway. However, the sensor nodes are programmed with given tasks (usually data collection and network control tasks) and the intelligence of these nodes has not been taken into account because of complexity reasons. In addition, mobility of sensor nodes is also an important factor in a logistic transportation system, which needs to be considered in the WSN design.

Originating from the fact that WSNs have been deployed in smart containers [4] to collect the information of temperature, humidity or pressure of the good items, WSNs are becoming a promising technology for logistics. This requires that sensor nodes are attached to goods, shelves, Returnable Transport Items (RTIs) and containers to form a multi-hop sensor network. In addition, a container that is equipped with a WSN must have a gateway to bridge the information from its WSN to an external network (e.g. WLAN, UMTS) to make it accessible from outside.

In this paper, a context-aware model of WSNs is proposed to adapt to the collected environmental data. Moreover, this model does not eliminate the self organization goal of WSNs by building the context model in the application layer while using the proactive routing protocol in [5]. The context-awareness in the proposal is node centric. This comes from the fact that if each node is context-aware, the whole sensor network is also context-aware [6].

This paper is structured in 6 sections: section I is the introduction to the scope of this paper, and related work is discussed in section II. Section III describes the context-awareness in logistic applications. Simulation and implementation results are shown in section IV and V. Finally, conclusions are given at the end of this paper.

II. BACKGROUND AND RELATED WORK

A sensor network is context-aware if it can use context to provide relevant information to the user, to other sensors or also to itself [6]. A lot of research on context-awareness has focused on two main fields: routing and applications. Gruteser et al. in [7] propose a Privacy-Aware Location algorithm which can prevent collection of privacy-sensitive data. In [8], some metrics (e.g. energy per packet, time to network partition) of Power-Aware routing are considered to prolong the lifetime of sensor nodes. The remaining battery charge of nodes is also taken into account as a routing metric in this research. Environmental Monitoring Aware Routing [9] uses a multiplicative combination of environmental conditions and other context criteria for routing, which can be useful in

978-1-4244-5347-4/09/$26.00 ©2009 IEEE

disaster scenarios such as forest fires. In [10], a model of WSNs awareness is also proposed using business rules at the node level which can be applied for logistic transportation.

Most of the above research is done in the area of routing, while the model presented in this paper is built in the application layer. The goals are following some key points:

- A proactive routing protocol should be used which can adapt to the changes of the network topology to support the mobility of goods items in logistics.
- A rule-based context model should be used because this model is simple enough to be implemented in resource-limited sensor nodes and demands little computing and storage requirements.
- Many environmental and external conditions such as surrounding temperature, location of nodes or connectivity between sensor network and infrastructure network should be supported.
- The contexts have to be easily programmable and the contexts are independent for each node.

III. CONTEXT-AWARENESS

A. *Context-awareness in logistics*

There are some contexts which should be considered in logistics. The context information can be obtained from some of the following sources:

- *Environmental conditions*: for example, the frozen food must be kept at a temperature of -20 °C. If the sensed temperature is higher than this threshold because of unknown reasons, nodes can trigger the alarms.
- *Security issues*: the goods packages or the container door can be secured by sensor nodes. If the security states are violated, the sensor nodes can send an alert message to inform about this event.
- *Location*: the location information is useful for the data collected, especially during the transportation time. The absolute location can be used to determine the position of the container, or the relative location can provide the position of each item inside the container. This information can be taken into account for context.
- *Long-distance connection*: a container using WSNs usually has a gateway to bridge the information between the WSNs inside the container and the outside network (e.g WLAN, UMTS). In case that there is no connection available to bridge because of the lack of coverage for example, sensor nodes should temporarily store the data to prevent information loss.
- *Timing*: time is also a source of context, especially in cases where some goods are sensitive with daylight. Seasons are also used for context based on timing.

B. *Model of context-awareness in WSNs*

In this section, a model is proposed to satisfy the previously mentioned issues. Figure 1 shows the architecture of the context-aware model. It has 5 parts with many blocks which are responsible for specific tasks.

1) Neighbour Management: builds and manages a neighbour table by using beacon broadcast. This part also applies enforcement and eviction policies to maintain entries in the neighbour table.

2) Routing: this part does the routing using the RSSI and MG information collected in the Neighbour Management part. The best neighbour node is selected based on the routing algorithm in [5].

3) Forwarding: this part checks the incoming packets coming from neighbour nodes to detect transmission loop problems. It also uses a cross-layer technique for loop detection.

4) Localization: the RSSI-based localization technique in [11] is implemented in this part to locate the positions of the sensor nodes.

5) Context-Aware: this part is in the main focus of this paper. It has several sub-parts:

- *Sensor*: all the internal and external sensors used by nodes for environment monitoring or other missions.
- *Rule database*: contains a set of pre-configured rules which are run to do corresponding actions for the contexts
- *Rule engine*: run all the rules retrieved from the Rule database to validate the data coming from sensors
- *Configuration*: contains the configuration for operation of sensor nodes.
- *Command identification*: is used to recognize the commands which can be used for updating rules, configuring the operation or retrieving the packets stored in Storage and other tasks.
- *Storage*: buffer the packets if necessary.

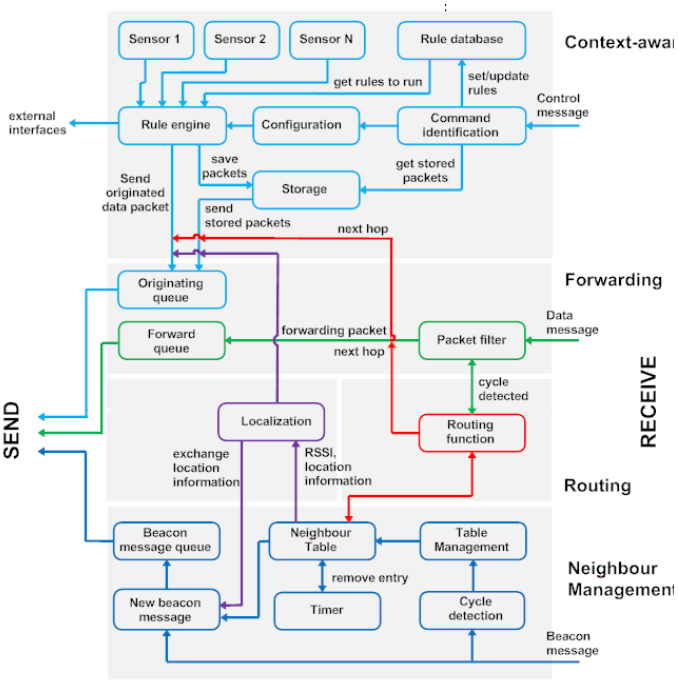


Figure 1: Architecture of proposed model

C. *Format of conditional rule*

A compact format for context rules shown in Figure 2 is proposed, which can be applied in context sources mentioned previously.

Figure 2: Format of rule

In this context rule there are the following fields:

- *ID* (6 bits): the unique number identifies the rule in the rule set. Hence, nodes can have many rules describing the contexts.
- *Sensor Type* (4 bits): is used to determine which sensor will be used in this rule. The table 1 shows the values of this field.

TABLE 1
VALUES OF SENSOR TYPE FIELD

Sensor Type	Value	Meaning
NO_SENSOR	0	If the sensor node has no sensor
TEMPERATURE	1	If the testing sensor is Temperature
HUMIDITY	2	If the testing sensor is Humidity
LIGHT	3	If the testing sensor is Light
INVOLTAGE	4	If the testing sensor is Internal Voltage (battery level or CPU temperature)
	5-15	Reserved for future use

* The testing sensor is the sensor generating the data which needs to be applied by the current context-aware rule

- *Condition* (3 bits): the logical condition is used to verify the validation of checking packets. The configuration of this field is shown in Table 2.

TABLE 2
LOGICAL CONDITION OF RULE

Condition	Value	Meaning
IN_RANGE	0	If the checking value is in range [Min..Max]
GREATER	1	If the checking data value of the checking packet is greater than Max
LESS	2	If the checking value of the checking packet is less than Min
OUT_OF	3	If the checking value of the checking packet is out of range [Min..Max]
NO_GW_CONNECTION	4	If there is no connection between the Gateway and infrastructure networks
GW_CONNECTED	5	If the Gateway connected to any infrastructure network
	6-7	Reserved for future use

* The checking value is the data which needs to be validated by the context-aware rules. The checking packet is the data packet which contains the checking value

- *Min* (16 bits), *Max* (16 bits): the minimum and maximum values which are combined with the *Condition* field. These values are the ADC values after the context interpretation.
- *Action* (3 bits): the corresponding action will be run if the *Condition* is true. Some pre-defined actions are shown in Table 3.

For example, a food package needs to be kept under the temperature in the range [0..4]°C during the transportation. Any value of the monitored temperature out of this range has to be reported. If sensor motes are used in this scenario, the context rule can be set as following:

IF TEMPERATURE OUT_OF [0…4] °C THEN SEND_PACKET

Because sensor nodes usually only understand raw ADC values (12 bits or 16 bits), the user meaning value (e.g. [0..4] °C) must be converted to ADC values.

The rule size is only 6 bytes so the limited-memory of sensor nodes can have many rules to describe contexts.

TABLE 3
VALUES OF ACTION FIELD

Sensor Type	Value	Meaning
DO_NOTHING	0	Do not apply any actions with the current packet
SEND_PACKET	1	Send the checking packet to the next-hop
STORE_PACKET	2	Store current packet to memory
	3-7	Reserved for future use

D. Context Interpretation

In order to reduce the computation at the sensor nodes, the contexts have to be described at the user side by defining a set of conditional rules which need to be applied for those contexts. After that, these rules will be translated into the rule format that the sensor node can understand using the numeric values in Table 1, 2, 3 and the format in section III.C. The translation is carried out by user-designed software.

E. Context programming

Because the contexts can change at any time, the rules must have the flexibility of being programmable to adapt to these changes. For the best, they can be programmed at any necessary time. Although the proposed model supports the rule programming at compilation time, it also supports the remote rule programming by sending commands (in control messages) to reconfigure the set of rules which describe the contexts. These control messages are implemented by using a dissemination technique as in [12] which is not only for programming context rules but also for other configuration purposes.

IV. COMPUTER SIMULATION

A container with 20 packages equipped with sensor nodes is used for 6 hours simulated time. The container also has a gateway to connect with the IP network and it is assumed to be transported to the destination. During the transportation, the connections between sensor nodes inside the container are always established because of the routing protocol. However, the connection between the gateway and the IP network may be disconnected because of the coverage. Each sensor node is powered by 2 AA batteries with the capacity of 2800 mAh [13]. The monitoring temperature is reported every 10 seconds if nodes use the normal operation mode. Nodes can be configured with normal or context operation mode. For evaluation, all data packets are monitored and logged at the gateway. The scenarios are simulated in TOSSIM [14]. However, the routing parameters are not discussed in this paper.

A. *Scenario 1: Environmental condition context-awareness*

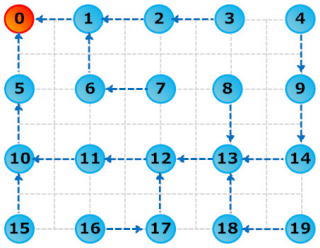
After booting, thanks to the routing protocol, the connectivity of network is built (shown in figure 3). Node 7 and node 18 are configured with context-aware operation mode while others use the normal operation. The temperature variations of these nodes are shown in figure 4 and 5 (the dash lines). The context-aware rule is used in node 7:

IF TEMPERATURE GREATER THAN 35 (°C) THEN SEND_PACKET (1)

and in node 18:

IF TEMPERATURE IN_RANGE [35..50] (°C) THEN SEND_PACKET (2)

Figure 3: The topology of 20 nodes network. Node 0 is the gateway and the others transmit their packets to the gateway using multi-hop communication. Each node not only transmit its packets but also forward packets coming from the neighbours.



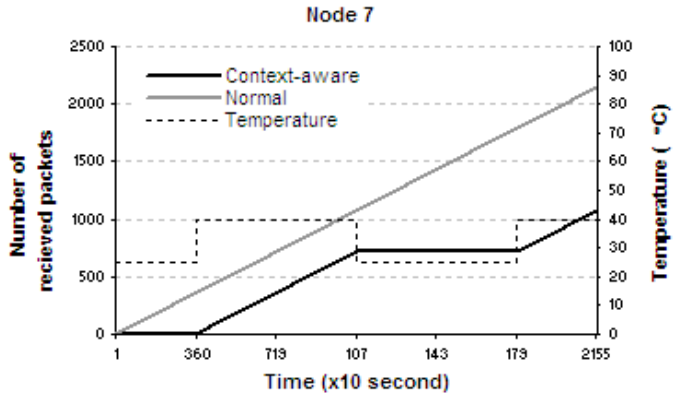


Figure 4: Temperature template and the number of received packets generated by node 7. The context of node 7 is that if the monitoring temperature is greater than 35 °C then the node will send the packets.

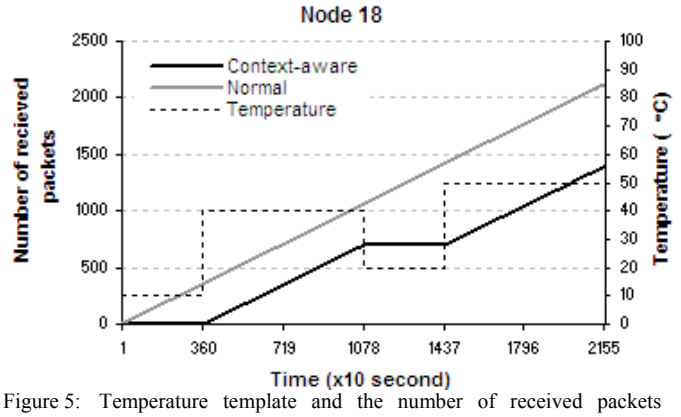


Figure 5: Temperature template and the number of received packets generated by node 18. The context of node 18 is that if the monitoring temperature is in the range [35..50] °C then the node will send the packets.

From figure 4 and 5, it can be seen that node 7 and 18 strictly follow the pre-configured rules. The number of packets sent by these node (red lines) increase if the conditions (1) (2) are true. Comparing with the number of packets received by the gateway in the case when context rules are not used (the gray line), the load reduces significantly (from approximate 2000 packets down to about 1000 packets in figure 4).

B. *Scenario 2: Connection context- awareness*

Now, node 13 is also set to run in context mode. The connection between gateway and IP network is also depicted by a dash line shown in Figure 6: the container can connect to IP network in the first 3 hours, and is disconnected in the last 3 hours. The other nodes in network are aware of the disconnection by receiving a command from the gateway.
The context rule of node 13 is configured:

IF GW_CONNECTED THEN SEND_PACKET (3)

It can be shown in Figure 6 that the sensor node 13 only sends the packets when the connection is available. This is indicated by the increase of received packets (the black line).

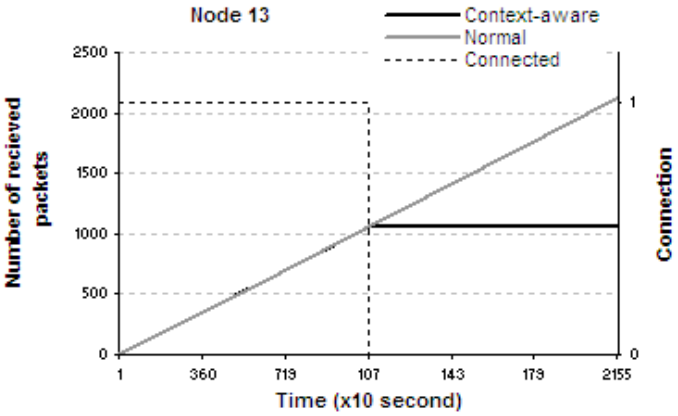


Figure 6: Temperature template and the number of received packets generated by node 13. The context of node 13 is that if the connection between the gateway and the IP network is available, then the node will send the packets.

C. *Scenario 3: Generated traffic*

In order to have a deeper view on the traffic of the whole network, all 20 sensor nodes are configured in normal operation and in context operation with the same context setting as in Scenario 1 (the same temperature template and the same context rule). Because the nodes only send packets in 3 hours (when the rule matches), so the total traffic generated in the network also reduces half. Moreover, reduction of traffic in each node also leads to the decrease of multi-hop load for the other nodes which is responsible for forwarding packets. Table 4 shows the number of sent packets in all scenarios.

TABLE 4
GENERATED TRAFFIC (PACKETS)

Scenario		Context-aware (packets)	Normal (packets)	Reduction (%)
1	Node 7	**1073**	2147	~ 50%
1	Node 18	**1391**	2121	~ 35 %
2	Node 13	**1052**	2121	~ 50%
3	Network	**19889**	39950	~ 50%

Theoretically, the generated traffic reduction is equal to rate of total time when the context rules are matched over the total running time of each node. This factor is also shown in the Table 4 with the same values. Hence, the definition of context

from users is very important because it can affect the efficiency of the network.

D. Scenario 4: Energy consumption

Using PowerTOSSIM-z [15] in the simulation for energy analysis, each node in the 20 nodes network consumes about 149 mAh during 6 simulation hours at the sampling rate of 10 seconds. Hence, at the sampling rate of 15 minutes, it can be easily calculated that the sensor nodes can operate in approximate 400 days if the battery has the capacity of 2800 mAh if the characteristic of self-discharging in batteries is neglected.

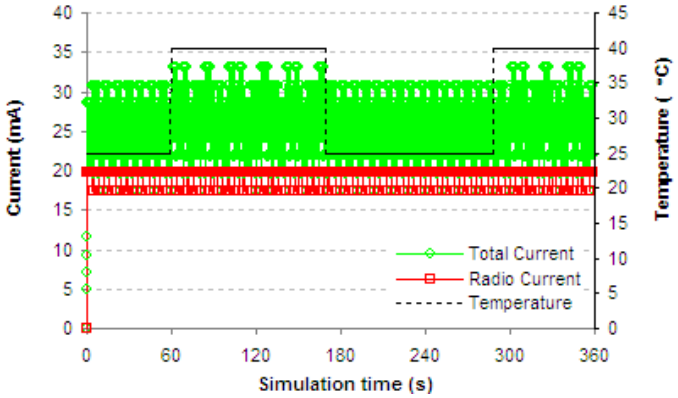


Figure 7: The current in node 1 during the 6 minutes of simulated time.

For a deeper investigation on energy consumption in nodes, a 2 nodes network is used because the forwarding traffic is not considered here. In this scenario, node 0 is the receiver and node 1 the transmitter. Node 1 uses the context rule (1) with the surrounding temperature variation in Figure 7 (the dash line). The total current in node 1 shown in Figure 7 is about 33 mA when the context rule is matched. And the simulation also shows that about 4600 mJ is consumed in 6 simulation minutes if context mode is used instead of 4700 mJ in normal mode.

V. Implementation

A. Description of Test bed

To measure the efficiency of context-awareness in a live sensor network, a 22 nodes network is set up using TelosB motes. TelosB uses a CC2420 radio chip for wireless communication, a TI MSP430 MCU with 10kB RAM for processing, and sensors (Hamamatsu S1087-01, Sensirion SHT11) [16]. The nodes run TinyOS [17], a real-time operating system. Each sensor node is configured to sample the environmental conditions (temperature, humidity and light) every 4 seconds. The data packets are logged at the gateway in 6 hours for analysis. The protocol described in [5] is used at the routing layer for data transmission. Low Power Listening (LPL) [18] and Packet Link Layer (PLL) [19] are also implemented to increase the efficiency and the reliability.

B. Configuration and measurements

After initializing the network, the connectivity of nodes is built based on the routing protocol. Figure 9 shows the topology in the test-bed. All of the rules are sent to the nodes at the beginning of the measurement by using software that is designed for collecting the packets, configuring the nodes and measuring parameters as well.

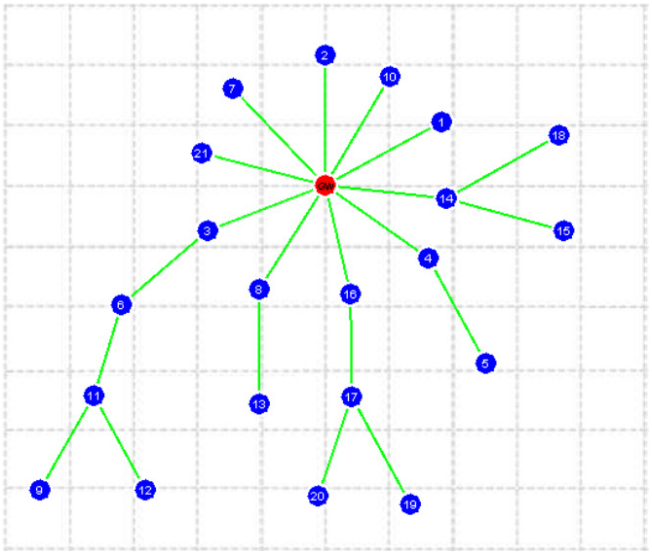


Figure 8: Test-bed network topology captured by the software. The red circle is the gateway and the blue ones are the sensor nodes with IDs inside.

Node 13 is set to operate in context mode. It uses a context rule:

IF TEMPERATURE GREATER THAN 38 (°C) THEN SEND_PACKET (4)

The surrounding temperature of this node is manually controlled over time. Node 19 is also configured with the rule:

IF LIGHT LESS THAN 20 (LX) THEN SEND_PACKET (5)

And the light shining to the sensor node is also manually adjusted. All the other nodes use normal operation.

Figure 9 and 10 depict the real temperature and light collected at the gateway and the number of received packets as well. These show that the context-rules work well in the given contexts. Figure 11 also shows the generated traffic comparison of nodes. It is clear that the nodes using context rules (node 13, 19) send less traffic than nodes using normal operation (e.g. node 11). The generated traffic of node 13 and node 19 is reduced by approximately 46% and 51% compared with the traffic generated by node 11.

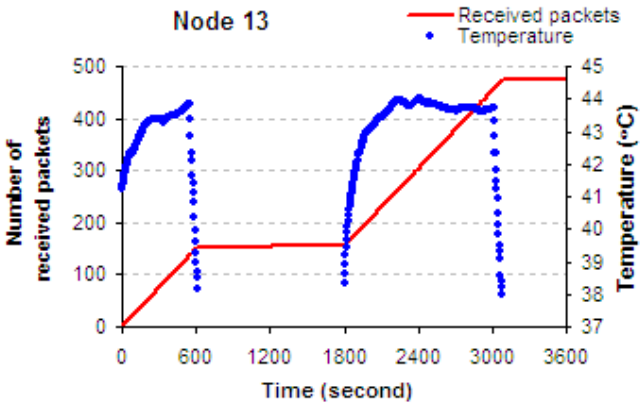


Figure 9: The number of received packets increases when the context rule is matched (temperature is greater than 38 °C)

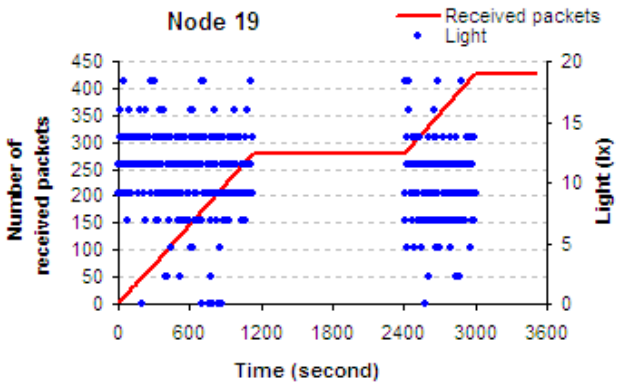


Figure 10: Similarly, if the light is less than 20 lx, then packets will be sent to the gateway.

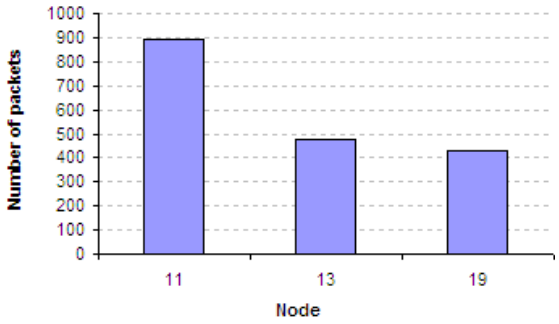


Figure 11: Comparison of generated traffic of nodes. Node 11 operates in normal mode and node 13, 19 use context mode.

However, only the originated traffic of each node is in the focus of this paper, not the traffic created by data forwarding, because the number of hops through which the packets travel can change over time due to the routing. However, if the generated traffic of the original node reduces, it also leads to a reduction of the total traffic in intermediate nodes (forwarding nodes). Hence, the total load in the network will decrease afterwards.

VI. Conclusion and Outlook

With the proposed model, it is believed that the items equipped with WSNs are becoming more intelligent. They not only know their locations, the conditions of surrounding environments, but also react with corresponding activities or communicate with other similar entities to send data. By being aware of their context, these sensor nodes can be easily used for many flexible targets in logistic scenarios to increase the communication as well as energy efficiency. Synergy between sensor nodes can be considered in the future to enhance the communication efficiency. Each sensor node not only uses its own context-awareness, but also interacts with others to improve the information quality. Location information can be taken into account for contexts as well.

Aknowledgement

This research is partially funded by the German Research Foundation (DFG) within the Collaborative Research Centre 637 ”Autonomous Cooperating Logistic Processes: A Paradigm Shift and its Limitations" (SFB 637) at the University of Bremen, Germany.

References

[1] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, M. Welsh, "Deploying a Wireless Sensor Network on an Active Volcano," IEEE Internet Computing, March 2006, Vol. 10, no. 2, pp. 18-25

[2] T. Schmid, H. Dubois-Ferrière, M. Vetterli, “SensorScope: Experiences with a wireless building monitoring sensor network”, in Proceedings of the Workshop on Real-World Wireless Sensor Networks, Stockholm, Sweden, June 2005

[3] P. Padhy, K. Martinez, A. Riddoch, H.L.R. Ong, J. K. Hart, “Glacial Environment Monitoring using Sensor Networks”, in Proceedings of the Workshop on Real-World Wireless Sensor Networks, Stockholm, Sweden, June 2005

[4] R. Jedermann, C. Behrens, R. Laur , W. Lang, “Intelligent Containers and Sensor Networks Approaches to apply Autonomous Cooperation on Systems with limited Resources”. In Understanding Autonomous Cooperation & Control in Logistics – The Impact on Management, Information and Communication and Material Flow. Springer, Berlin, 2007, pp. 365-392

[5] V.Q. Son, B.L. Wenning, A. Timm-Giel, C. Görg, “A Model of Wireless Sensor Networks using Opportunistic Routing in Logistic Harbor Scenarios”, in Proceedings of 2nd International Conference on Dynamics in Logistics, Bremen, Germany, August 2009, pp 214-223

[6] Q. Huaifeng , Z. Xingshe, “Context aware sensornet”, in Proceedings of the 3rd international workshop on Middleware for pervasive and ad-hoc computing, Grenoble, France, November 2005, pp. 1-7

[7] M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald, “Privacy-aware location sensor networks”, in Proceedings of the 9th conference on Hot Topics in Operating Systems, Bekerley, USA, 2003, pp. 28

[8] S. Singh, M. Woo, C. S. Raghavendra, “Power-aware routing in mobile ad hoc networks”, in Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Texas, USA, 1998, pp. 181-190

[9] B.L. Wenning, D. Pesch, A. Timm-Giel, C. Görg, “Environmental Monitoring Aware Routing in Wireless Sensor Networks”, IFIP International Federation for Information Processing, Toulouse, France, September 2008, Volume 284/2008, pp. 5-16

[10] M. Marin-Perianu, N. Meratnia, M. Lijding, P. Havinga, “Being Aware in Wireless Sensor Networks”, in Proceedings of the 15th IST Mobile & Wireless Communication Summit, Capturing Context and Context Aware Systems and Platforms Workshop, Myconos, Greece, June 2006,

[11] V.Q. Son, B.L. Wenning, A. Timm-Giel, C. Görg: “Localization using Opportunistic Routing in Wireless Sensor Network for Logistics”, in Proceedings of the ASOR2009 Conference, Queensland, Australia, 2009

[12] P. Levis and G. Tolle: Dissemination of Small Values – TEP 118, available at www.tinyos.net

[13] Energizer EN91 Datasheet, available at www.energizer.com

[14] P. Levis, N. Lee, M. Welsh, D. Culler, “TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications”, in Proceedings of the First ACM Conference on Embedded Networked Sensor Systems, Los Angeles, USA, November 2003, pp. 126-137

[15] E. Perla, A. Catháin, R. Carbajo, M. Huggard, C. Mc Goldrick: “PowerTOSSIM z: Realistic Energy Modeling for Wireless Sensor Network Environments”, in Proceedings of the 3nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, Vancouver, British Columbia, Canada, pp. 35-42

[16] TelosB Datasheet – available at www.xbow.com.

[17] TinyOS – www.tinyos.net

[18] J. Polastre, J. Hill, D. Culler, “Versatile low power media access for wireless sensor networks”, in Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore, USA, November 2004, pp. 95- 107

[19] D. Moss, P. Levis, “Packet Link Layer”, TEP127, available at www.tinyos.net