ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2012. No. 3(119)*
ELEKTRONIKA IR ELEKTROTECHNIKA

SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
T 120
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Cargo Container Monitoring Data Reliability Evaluation in WSN Nodes

S. Jakovlev, A. Andziulis, V. Bulbenkiene
Klaipeda University, Department of Informatics Engineering,
Bijunu str. 17-206, LT-91225, Klaipeda, Lithuania, phone: +37064690756, e-mail: s.jakovlev.86@gmail.com
R. Didziokas, M. Bogdevicius
Klaipeda University, Mechatronics Science Institute,
Bijunu str. 17, LT-91225, Klaipeda, Lithuania, phone: +37046398693, e-mail: rimantas.didziokas@ku.lt
R. Plestys, R. Zakarevicius
Kaunas University of Technology, Department of Computer Networks,
Studentu str. 50-416, LT-51368, Kaunas, Lithuania, phone: +37037300368, e-mail: rokas.zakarevicius@ktu.lt

crossref http://dx.doi.org/10.5755/j01.eee.119.3.1371

Introduction to the problem area

Application of Wireless Sensor Network (WSN) technology for cargo container condition monitoring plays an important role in raising the efficiency of cargo transport operations [1]. In general, the container monitoring WSN consists of sensors inside the containers. Sensors constantly report on the transport conditions and transmit the information to the integrated network database. Such application has a lot in common with robotic movements' control [2] and other industry production processes [3] and therefore, may have the same stochastic process control methods applied to them to measure acquired data reliability. As an example: external climatic conditions have a decisive impact upon the climatic conditions inside containers (temperature fluctuations). External climatic conditions are in particular determined by the transport route, season, the time of day and the current weather.

The possibilities of container sensor errors, mechanical container and sensor system damage, and external non typical changes in the environment, that fall outside the cargo technological limitations, are considered not probable and are not taken into account in this paper. Thus, any sensor system error should be clearly visible during the primary node data analysis. Each individual WSN node can be defined by multiple sensor criteria depending on the area of application. It is obvious that constant analysis of all these criteria is not efficient in terms of computational time and system resources. In addition, the use of different sensors (further implied as parameters) in the system hardens the data analysis, as it includes application of different technologies. External non typical changes in the environment depend on the transport route, transport means and weather conditions, and therefore, are predictable. Mechanical container and sensor system damage is relatively random and should be of the primary concern. Sensor node hardware and containers receive additional physical damage during long transport operations. Failure to comply with standards and other external impacts can also cause undesirable measurement errors. Such additional impacts can cause nodes to malfunction and receive false or discard real data errors.

Nowadays, all general data reliability assurance mechanisms used within the networks require a lot of resources – increased data processing and transmission time. Therefore, other data analysis mechanisms are needed to be used, that enable data reliability evaluation of the WSN nodes and predicting false data occurrence. The assumption is made, that true data is evaluated as true container damage data and false data is evaluated as sensor system errors. Such functionality could be achieved by using intelligent middleware agents [4]. It would allow integrating the software and hardware (sensors) with the wide variety of security and reliability based applications that are currently available. It would also provide real-time event management through the use of intelligent programmed nodes for real-time processing of sensor signals. These signals could be converted into effective business information that would be used in cargo transportation enterprise environment.

The main characteristics of data reliability evaluation

The cargo container monitoring system includes two interconnected parts: the container itself and its built-in sensors. Container status data is generated by sensors that are the nodes of the WSN. The reliability of each WSN

node data is examined by evaluating the reliability of information it receives and transfers. Each cargo container can be in normal or defected state. The WSN network sensors can also be in normal state and provide correct information, or a in defected state thus providing false information. Data is considered to be reliable when they describe the actual state of a cargo container. Here the following probability statements are introduced: w – the probability to generate false data by a node; $\overline{w} = 1 - w$ - the probability to generate true data by a node; q – the probability that data is evaluated as false; $p = 1 - q$ – the probability, that data is evaluated as true.

Here the probability statements for cargo container state and sensor data transfer reliability evaluations are introduced: q_{BB} – the probability that the cargo is not damaged and the sensors indications are incorrect (false data is evaluated as false); q_{GB} – the probability that the node might have been damaged during the operational period and that the information is evaluated as false (true data is evaluated as false); p_{GG} – the probability that the cargo is truly damaged and the sensors indications are correct (true data is evaluated as true);

p_{BG} – the probability that the node is a malicious node and the information is evaluated as true (false data is evaluated as true).

The following statements are true:

$$p = p_{GG} + p_{BG},\ p \in (0,1), \quad (1)$$

$$q = q_{BB} + q_{GB},\ q \in (0,1), \quad (2)$$

$$p_{GG} + q_{GB} = 1 - w, \quad (3)$$

$$p_{BG} + q_{BB} = w,\ w \in (0,1), \quad (4)$$

$$p_{GG} + p_{BG} + q_{BB} + q_{GB} = 1. \quad (5)$$

The coefficients that define the relations among different data error probability cases are introduced in (6, 7, 8 and 9).

The relation of probability of true data being evaluated as false with the probability to generate true data is

$$\alpha = \frac{q_{GB}}{p_{GG} + q_{GB}} = \frac{q_{GB}}{1-w} = 1 - \frac{p_{GG}}{1-w},\ \alpha \in (0,1). \quad (6)$$

The relation of probability of false data being evaluated as true with the probability to generate false data is

$$\beta = \frac{p_{BG}}{p_{BG} + q_{BB}} = \frac{p_{BG}}{w} = 1 - \frac{q_{BB}}{w},\ \beta \in (0,1). \quad (7)$$

The relation of probability of true data being evaluated as true with the probability to generate true data is

$$\lambda = \frac{p_{GG}}{p_{GG} + q_{GB}} = \frac{p_{GG}}{1-w} = 1 - \frac{q_{GB}}{1-w},\ \lambda \in (0,1). \quad (8)$$

The relation of probability of false data being evaluated as false with the probability to generate false data is

$$\delta = \frac{q_{BB}}{p_{BG} + q_{BB}} = \frac{q_{BB}}{w} = 1 - \frac{p_{BG}}{w},\ \delta \in (0,1). \quad (9)$$

Additionally, the sum of all data error defining coefficients is

$$\alpha + \beta + \lambda + \delta = 1. \quad (10)$$

Evaluation of data defect levels

As mentioned previously, depending on many factors, data reliability evaluation is required. The reliability of data evaluation mechanism can be formulated as

$$\phi = 1 - \alpha - \beta,\ \phi \in (0,1). \quad (11)$$

The defect levels for WSN node k and the nearest WSN node k+1 are introduced below: Q_{INk} – is the defect level of the incoming data in node k (any node in the network), $Q_{INk} \in (0,1)$; Q_{OUTk} – is the defect level of data after the evaluation in node k, $Q_{OUTk} \in (0,1)$; Q_{INk+1} – is the defect level of the incoming data from node k which is transferred to the neighbouring node for potential evaluation, $Q_{INk+1} \in (0,1)$; Q_{OUTk+1} – is the modified defect level of data after the secondary evaluation in node $k+1$ (nearest node in the network), $Q_{OUTk+1} \in (0,1)$.

The defect level of the incoming data Q_{IN} is dependent on the technological aspects of the used hardware. The probability that data is evaluated as false in node k is

$$q = \alpha + \phi \cdot Q_{INk} = \alpha + (1 - \alpha - \beta) \cdot Q_{INk}. \quad (12)$$

The probability that data is evaluated as false in node k+1 is

$$q = \alpha + \phi \cdot Q_{INk+1} = \alpha + (1 - \alpha - \beta) \cdot Q_{INk+1}. \quad (13)$$

The defect levels of data after the evaluation at node k and k+1 can be expressed:

$$Q_{OUTk} = \beta \cdot \frac{Q_{INk}}{p} = \frac{p_{BG}}{w} \cdot \frac{Q_{INk}}{\alpha + (1 - \alpha - \beta) \cdot Q_{INk}}, \quad (14)$$

$$Q_{OUTk+1} = \beta \cdot \frac{Q_{INk+1}}{p} = \beta \cdot \frac{Q_{OUTk}}{p} = \frac{p_{BG}}{w} \cdot \frac{Q_{OUTk}}{\alpha + (1 - \alpha - \beta) \cdot Q_{OUTk}}. \quad (15)$$

In all cases, the defect level Q_{OUTk} is defined as Q_{INk+1} for the nearest node in the network during the data update process. This is done in order to check if the

acquired data is true or false.

Problem area definition and messaging technique

When node k receives the highly deviated sensor data it computes the problem area Ap and initiates the request and reply procedure. The nearest node $k+1$ is defined by its coordinates x, y, z in the problem area Ap. When node k sends the request message m_{Rt} through the WSN to the integrated network database, the nearest node k+1 receives that message and replies to node k by sending the reply message m_{Ry} (Fig. 1). The Integrated network database is used to store the request messages and main network messages m_S.

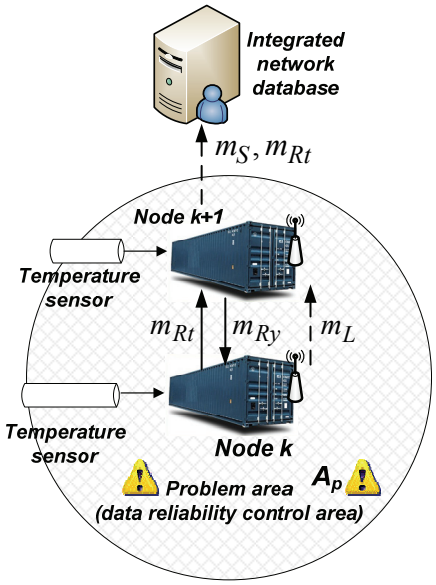

Fig. 1. Cargo container monitoring system diagram

The initial request message m_{Rt}, sent from node k, and reply message m_{Ry}, sent from node $k+1$ at time t, are described as:

$$m_{Rt} \in Rt : (Sc, k, \{t, Ap\}, C), \quad (16)$$

$$m_{Ry} \in Ry : (Sc, k+1, \{t, x, y, z\}, C), \quad (17)$$

here Ap – problem area defined by the node k; Rt – set of messages sent from node k; Ry – set of messages sent from node $k+1$; Sc – security mechanism; C – message content.

When the node k+1 is found, the local data update process is initiated. It is defined by the appropriate network infrastructure and is used by the set of network nodes K in data reliability evaluation. The data update message, sent from node k to node $k+1$, is described as

$$m_L \in L : (Sc, \{k, Q_{INk}, Q_{OUTk}, M, Tr, \{t, x, y, z\}\}, C), \quad (18)$$

here L – set of messages sent from node k; k – the initial node identification number; M – node k parameter deviation; Tr – time of data reliability evaluation.

The main network message m_S is formed in node k+1 and transferred via the pre-defined route. It is stored in the real-time communication integrated network database (Fig. 1). The message is described as

$$m_S \in S : \begin{pmatrix} Sc, \{k, Q_{INk}, Q_{OUTk}, M, Tr, \{t, x, y, z\}, Ap\}, \\ \{k+1, Q_{INk+1}, Q_{OUTk+1}, M, Tr, \{t, x, y, z\}\}, C \end{pmatrix}. \quad (19)$$

Here S – a set of main messages m_S sent from the problem area Ap.

Simulation results

The simulations have been performed for evaluating the functionality of data reliability evaluation mechanism. The initial simulation parameters have been chosen, that would be closely related to real technological parameters (Table 1). The initial parameters of network nodes are determined as identical for both experimental nodes with the same α, β, p and w values, where $Q_{INk} = 0.06$.

Table 1. Parameter values for WSN nodes k and k+1

No.	α	β	p	w
1	0.0206	0.8500	0.9800	0.0300
2	0.0207	0.7800	0.9750	0.0350
3	0.0208	0.7000	0.9700	0.0400
4	0.0209	0.6667	0.9650	0.0450
5	0.0211	0.6000	0.9600	0.0500
6	0.0212	0.5455	0.9550	0.0550
7	0.0218	0.5000	0.9500	0.0600

The dependencies of defect levels on their probabilities detect false are presented in Fig. 2. The results indicate that when probability q_{BB} (the cargo is not damaged and sensor indications are incorrect) is reaching the zero value, both defect levels increase in correlation with each other.

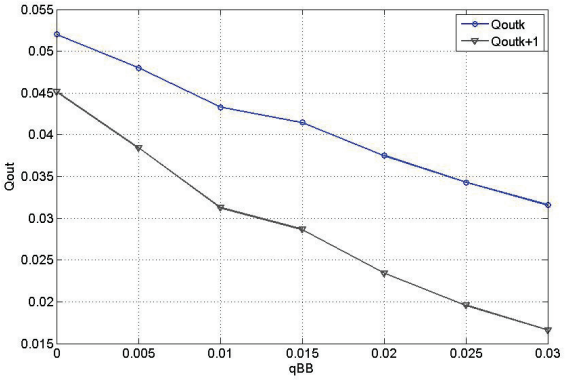

Fig. 2. Comparison of defect levels at nearby nodes

Therefore, the higher the possibilities to detect the false data in node k during the initial evaluation, the lower are defect levels on the outcome of both k and k+1 nodes. An assumption is made that such sensor indication is done in node k. Corrupt data is considered questionable by the middleware agent and therefore data reliability (data defect levels) are calculated. In the example, the nearest node $k+1$ compare the received information with its own sensor indication values. If the temperature sensor indications match, then the secondary positive evaluation is done and the main message m_S is formed. It is considered that weather conditions may have changed rapidly and are

affecting the cargo of containers with WSN nodes k and $k+1$ in the problem area Ap. Simulation results indicate that the cargo container is really damaged and the defect level of data from node k is decreased dynamically. The increment or decrement threshold of such defect level should be defined individually for each separate case.

The problem area is described as data reliability evaluation area. The same computations can be made to any node in the WSN, if it is situated closely or in the same area as the node k, which defect level Q_{INk+1} is used in the evaluations.

Conclusions

The presented work describes the possible application of process quality control method for data reliability evaluation of WSN nodes. The novel statistically based data reliability evaluation concept has been created. It could be used in intellectual agent development for the evaluation of data that is being transferred throughout the Wireless Sensor Network (WSN). Such network enables instant collection of data from sensors located in cargo containers. The proposed data reliability evaluation mechanism enables real-time detection of data defects, thus helping during decision making processes in cargo transportation enterprise environment. The use of such data quality evaluation in WSN is directly linked to reliability assurance and useful in predictive maintenance of maritime cargo transportation systems.

Acknowledgement

The authors would like to thank the project LLIV-215 "Cross-border DISCOS. JRTC Extension in Area of Development of Distributed Real-Time Signal Processing and Control Systems" for the support while writing and publishing the manuscript.

References

1. **Oztekin A., Pajouh F. M., Delen D., Swim L. K.** An RFID network design methodology for asset tracking in healthcare // Decision Support Systems. – Elsevier, 2010. – No. 49(1). – P. 100–109.
2. **Bielskis A. A., Ramašauskas O.** Detection of Signal Data Alternations by Forward Chaining XPS // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 2(74). – P. 45–48.
3. **Container Handbook.** – GDV die Deutschen Versicherer, 2010. – 1500 p.
4. **Adomaitis D., Bulbenkienė V., Jakovlev S., Pridotkas G., Andziulis A.** Mobile services providing devices rating based on priority settings in wireless communication systems // Communications in Computer and Information Science, – Springer, 2011. – No. 188(1). – P. 1–8.

Received 2010 11 08
Accepted after revision 2012 01 12

S. Jakovlev, A. Andziulis, V. Bulbenkiene, R. Didziokas, M. Bogdevicius, R. Plestys, R. Zakarevicius. Cargo Container Monitoring Data Reliability Evaluation in WSN Nodes // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 3(119). – P. 91–94.

The application of state-of-art mobile technologies in cargo container transportation monitoring systems (ex. Sensor networks) is possible only after assessing the reliability of data transfer. Data reliability depends on how accurately container state is evaluated by sensors and sensor reliability itself. Four probability values are introduced that define the states of damaged and undamaged containers and evaluate the generation of true and false data. The formats of messages that are being sent to the integrated network database are described. The definition of data defect level is introduced and used to evaluate the aggregate state of a node, consisting of a container and a sensor. The dependences of defect levels on the probabilities to detect false data at nearby nodes in the problem area have been derived. It enables real-time detection of data defects, thus helping during decision making processes in cargo transportation enterprise environment. Ill. 2, bibl. 4, tabl. 1 (in English; abstracts in English and Lithuanian).

S. Jakovlev, A. Andziulis, V. Bulbenkienė, R. Didžiokas, M. Bogdevičius, R. Plėštys, R. Zakarevičius. Krovinių konteinerių stebėjimo duomenų patikimumo įvertinimas belaidžio jutiklių tinklo mazguose // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 3(119). – P. 91–94.

Naujas mobiliąsias technologijas jūrinių konteinerių transportavimo stebėjimo sistemose (pvz., sensoriniuose tinkluose) galima taikyti tik įvertinus perduodamų duomenų patikimumą. Duomenų patikimumas priklauso nuo to, kaip tiksliai sensoriai įvertina konteinerių būklę, taip pat ir nuo jų pačių sensorių patikimumo. Naudojamos keturios tikimybės, įvertinančios pažeisto ir nepažeisto konteinerio būsenas, taip pat teisingų ir klaidingų duomenų generavimą. Aprašyti pranešimų, siunčiamų į integruotą tinklo duomenų bazę, formatai. Įvedama defekto lygio sąvoka, kuria apibūdinama mazgo, sudaryto iš konteinerio ir sensoriaus, bendra būsena. Gautos defekto lygio priklausomybės nuo klaidingų duomenų atpažinimo tikimybės probleminėje srityje. Tai leidžia aptikti duomenų klaidas realaus laiko sąlygomis ir greičiau priimti sprendimus krovinių transportavimo įmonėse. Il. 2, bibl. 4, lent. 1 (anglų kalba; santraukos anglų ir lietuvių k.). Il. 2, bibl. 4, lent. 1 (anglų kalba; santraukos anglų ir lietuvių k.).