Intelligent Containers Network Concept

Sergej Jakovlev[1], Audrius Senulis[2], Mindaugas Kurmis[1], Darius Drungilas[1] and Zydrunas Lukosius[1]
[1] *Informatics and Statistics Department, Klaipeda University, Bijunu str. 17, LT-91225, Klaipeda, Lithuania*
[2] *Engineering Department, Klaipeda University, Bijunu str. 17, LT-91225, Klaipeda, Lithuania*
{s.jakovlev.86, mindaugask01, dorition}@gmail.com, {audriussenulis, z.lukosius}@yahoo.com

Keywords: Wireless Sensors Network, Security, Intelligent Containers, Mobile Security, Communication.

Abstract: In this paper, a novel approach is presented to increase the security of shipping containers transportation and storage in container yards. This approach includes wireless sensors networks with programmable modules to increase the effectiveness of the decision support functionality for operators' onsite. This approach is closely related to the Container Security Initiative and is intended to deepen knowledge in the intelligent transportation research area. This paper examines an urgent challenge - secure of cargo transportation in containers, i.e., how quickly it is possible to detect dangerous goods in shipping containers without changing their tightness and hence rationally implements international security regulations all around the world. This paper contributes to the development of new approaches of shipping containers handling and monitoring in terms of smart cities and smart ports (for the development of the Smart Port initiative) for ports that have higher levels of security violations. This contribution is addressed as an informative measure to the general public working in the Information and Communications Technologies (ICT) research area.

1 INTRODUCTION

To combat illicit trafficking in maritime container transport, a good level of detection is essential, and should be approached with advanced data-driven or process-driven technologies. Although the process-driven technologies are done now with a large range of surveillance and active interrogation techniques, active sensors that register the threats during the transportation route and onsite might be an interesting supplement to the battle the rising threats. Data-driven characteristics will allow instantaneous recombination of all possible scenarios with a high certainty of risk detection under normal working conditions.

The analysis of scientific literature studying the intermodal terminal activity revealed that there are many models helping to improve the terminal's operational activity, however there are no models helping to determine which technology would be the most rational in the terminal for security (Chang et al., 2014). In the research of Alexandridis et al., 2017, they analysed the international shipping industry in order to improve the efficacy of risk diversification for shipping market practitioners, further security problems were addressed by Scholliers et al., 2016. Authors discussed the technological possibilities to improve the integrity of containers in port related supply chains. They suggested that the most plausible solutions are adding monitoring equipment, such as e-seals and tracking devices, monitoring the environment using cameras, improved gate processes and generating useful control information in the general security monitoring infrastructure, also discussed by McLay and Dreiding, 2012.

In this paper a discussion is made allowing the reader to generally understand the variety of technological solutions currently applied and to understand the importance of their integration in a common technological platform.

Regulations and standards proposed in the Container Security Initiative (Bullock et al., 2018) declare that the future of containerization depends heavily on the level of adoption of new technologies to increase cargo and processes security on all level and during the whole trip. CSI declared the development of an "Intelligent container" concept. This is how the "intelligence" in brought to the everyday containerized section of the global transport chain and the following CSI core elements are achieved: establish security criteria to identify

high-risk containers based on advance information, pre-screen containers at the earliest possible point, use ICT to quickly pre-screen high-risk containers and develop secure and "intelligent" containers.

Application of most modern mobile technologies plays an important role in maximizing the performance, reducing the costs and risks of intermodal containers transportation and raises the efficiency of other transportation services in the supply chain. WSN is a technology that can be very useful when it is used to acquire and dispatch collected data in wide areas. Usually, these networks consist of different types of nodes which are carrying different types of sensors along with computational devices. WSN can be visualised using active RFID system components currently used by several countries for port transport operations, where each network node is called a tag. These nodes transmit data through the network to some specific destination or the collecting tag (initiation node).

There is a wide range of literature concerning WSNs (Truong, 2015; Anurag & Christian, 2015). The large amount of publications revolves around different issues: fault tolerance (Sausen, 2010), scalability (Hoblos, 2010), sensor placement (Bulusu, 2001), caching and power consumption (Dimokas, 2011), data aggregation (Polastre, 2004) and data gathering (Krishnamachari, 2002). In some particular cases, a WSN can be also seen as a collection of different sensor nodes with intermittent connectivity, asymmetric bandwidths, long and variable latency and ambiguous mobility patterns. There are many studies that approach the problem of high connectivity in wireless networks.

2 ANALYSIS OF AN INTELLIGENT CONTAINERS' NETWORK

From the middle-ages scientists tried to mimic the functionality of the surrounding nature by inventing new materials and machines. Computer systems are now control-ling various crucial aspects of our lives. Despite this scientific leap forward, many areas of engineering are still missing this innovative touch, mostly due to the lack of understanding of the benefits which can be derived from their full integration to solve the most obvious security problems. To adapt the intelligent container approach to the working conditions a new method is proposed to connect the intelligent containers to a network with the capability to perform computational tasks in different parts of the network (in nodes), much like in a living brain. A container yard can now be presented as a form of virtual brain for a certain computational activity. In a living brain, connection between neurons is made using nerve tissue.

Such connection can be done using simple cables. But this would pose serious problems to engineers and operators' onsite. A plausible solution is to use wireless communication technologies to connect all the computational neurons in the network. Such technology is called WSN. WSN in common applications use Ad-Hoc routing protocols.

Routing is meant to establish a proper connection among the nodes in the network. Such connections are fast and agile. In dynamic environments other routing protocols may also be applied. Each computational neuron can be presented as an individual container with the capability to compute certain amount of incoming sensor information and transfer it through the container network using wireless communication principles. But it is a tricky problem, because where one communication frequency is allowable in one country, others are not.

Neurons die and the brain is evolved by introducing new neurons and interconnections. New containers are introduced to the stack and to the network on a constant basis. Wireless sensor networks or WSNs are networks of autonomous sensors aimed at monitoring physical or environmental conditions and pass their data through the network to some locations or data sinks. Every node has a radio transmitter and a limited source of energy. Energy consumption is not essential in this research as larger batteries may be equipped in these conditions and may be used for years to come without any recharge. It is possible to use a combination of several routing protocols or a unique protocol divided among several inner networks for each individual case. However, there exists paradigm that does not allow the full and effective integration of this technology. That is the direct communication.

At some point, using a direct communication protocol, each sensor sends its data directly to the base station without additional data improvement at each node. If the base station is far away from the nodes, direct communication requires a large amount of resources from each node and the final result may contain information errors. When communication is done in a container yard, then due to the working environment constraints, this procedure becomes virtually impossible. Signal reflections will take

place when using ISO certified standards for communication within the port environment. Additional information errors in the messages will result in additional message replies and resends. This will take time and no guarantees are given whether the final result will be positive.

New regulations will have to take place. One of the solutions is to use a globally certified high frequency ZigBee standard. Although this high frequency standard will make transmission of information to the initiation node (sink) complicated, it is designed to be used in industrial environments by using the minimum-transmission-energy routing protocol. In this protocol, data is sent to the base station through intermediate nodes. Nodes act as routers for other nodes and transmit their data by adding their own data packets. Additionally, this data can be modified at each node separately and resent. In other words, it is possible to correct the data at each container node if this functionality is programmed. Each node then can receive data from several nodes around it at the closest distances and make assumptions about the security of its contents and the surrounding area. Specific hardware and software tools should be used to reach this goal. Additional middleware will programmable agent logic must be introduced. Intelligent agents will act as decision support actors for operator's onsite and the managers responsible for the transport chain activities indicating possible detected threats. Each node's computational power can be used to assess the problem using specific algorithms (agent logic).

These algorithms may be programmed as smart software agents in the network and etc. The problem still remains how to select each individual node in the network of containers. Which sensors data is essential and valuable and how many intelligent containers with sensors are required to fully cover the container yard, these are the main problems faced in this research. The placement of the sensors in the container can be optimized. Unnecessary nodes can be put to sleep. Sleep functionality is optional and can prove to be a useful toll in saving energy. Sleeping procedure is installed in many industrial WSN systems.

2.1 Data Communication Method

The foremost idea of the integration of the WSN and middleware agent approach is to ensure the collective security of the entire network in terms of data security within the information flow for the transport chain. To achieve this goal, an improved method of Jakovlev et al., 2012 is proposed that incorporates both network and hardware units, along with the computation power of each node in the network. It is done to increase the collective security of the entire network of containers. In a container yard each intelligent container performs its own evaluation of the situation. Accuracy of these measurements is questionable and requires further analysis. Each container manages an area in a 3-D space where each intelligent container can ask the neighbouring container for assistance in data confirmation and sensor work time efficiency optimization. As mentioned previously, nodes can use large power supplies and storage units inside the containers. To increase data and autonomous process visibility in transport chain, integrated database should be used to store and reallocate useful information. To achieve the security goal, a specific messaging technique is required. 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 (see figure 1). When node k sends the request message m_{Rt} through the network to the local data storages in nodes and the integrated network database, the nearest node k+1 receives that message and replies to node k by sending the reply message m_{Ry}. The local data storages are used to store the request messages and main network messages m_S. with the appropriate information regarding the sensor data. Integrated network database is used to store the final message m_S. The initial request message m_{Rt}, sent from node k, and reply message m_{Ry}, sent from node k+1 at time tm, are described as (1) and (2):

$$m_{Rt} \in Rt : (Sc, k, \{t, Ap\}, C), \tag{1}$$

$$m_{Ry} \in Ry : (Sc, k+1, \{t, x, y, z\}, C). \tag{2}$$

Here: Ap is the problem area defined by the node k, Rt is the set of messages sent from node k, Ry is the set of messages sent from tag $k+1$, Sc is the security mechanism and C is the 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. The data update message, sent from node k to node $k+1$, is described as (3):

$$m_L \in L : \left(Sc, \begin{Bmatrix} k, Q_{INk}, Q_{OUTk}, \\ M, Tr, \{t, x, y, z\} \end{Bmatrix}, C \right). \tag{3}$$

Here: L is the set of messages sent from tag k, k is the initial node identification number, M is node k parameter deviation, Tr is the time of data 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. The message is described as (4):

$$m_S \in S : \begin{pmatrix} Sc, \begin{Bmatrix} k, Q_{INk}, Q_{OUTk}, M, Tr, \\ \{t, x, y, z\}, Ap \end{Bmatrix}, \\ \begin{Bmatrix} k+1, Q_{INk+1}, Q_{OUTk+1}, \\ M, Tr, \{t, x, y, z\} \end{Bmatrix}, C \end{pmatrix}. \quad (4)$$

Here: S is the set of main messages m_S sent from the problem area Ap. Each message content C must include all the general information regarding the sensor parameters monitored by each individual node on demand by its neighbour. Each message content C must include all the general information regarding the sensor parameters monitored by each individual node on demand by its neighbour.

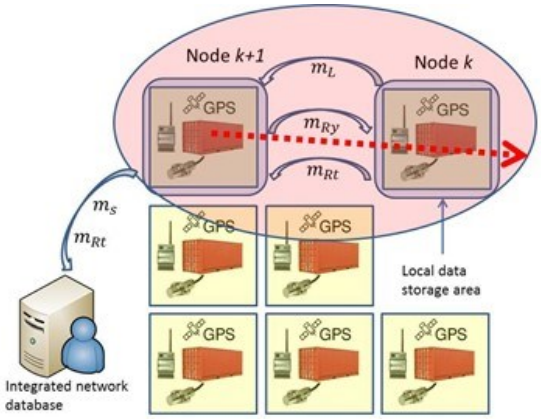

Figure 1: Intelligent container connectivity scheme.

This message must contain the accuracy of its estimation. Accuracy areas within a problem area of the container are spherical in every direction from the initial container k (see figure 2). Each message content C can be different, because various sensors and their manufacturers are used by different nodes. Their standardization requires them all to have standard output possibilities. This is still a problem that may not be solved at the near future. Each message can computed specifically for the network. Therefore, an additional security mechanism can be placed not in the message heading but in the message itself. The key for the message encoding is distributed by the operating company in the network of containers onsite using a simple network system coding principle with a single container during its unloading procedure.

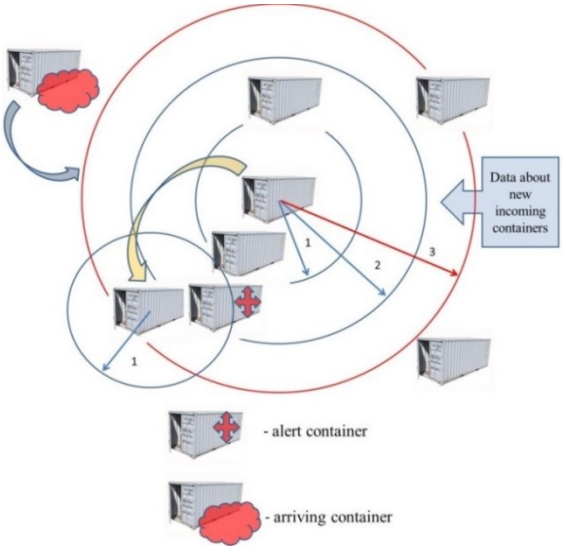

Figure 2: Accuracy area description for the container network.

This is done autonomously nowadays using e-Seal technology. Distance between nodes can be estimated in the WSN using the received signal strength indicator parameters RSSI (Wanga, 2009).

2.2 Description of the Accuracy Area

A special accuracy area parameter is used. Accuracy areas are designated spaces with dynamic environment where connection is possible by calculating the minimum SNR. Firstly, the accuracy area is calculated and nodes are discovered. Sensors data and parameters are sent for inspection to the initiation node. The networking time parameter tn, spent for both routing, accuracy area initiation and sensors parameters data retrieval operations, is provided. The computation time tc spent by the initiation container k includes: time spent for inner data file transfer, time spent for comparison to analyzed data from inner sensors and time spent to other sensors from outer containers. Further communication between more than 100 nodes can prove to be a difficult problem for an error increase in geometrical progression. Therefore, it can be assumed that the communication problem or tc can be minimized by decreasing the number of containers in the accuracy area, decreasing the range

of the accuracy areas or simply avoiding using too many containers for communication.

As an example, this intelligent containers network can be used to detect radioactive isotopes (dirty bombs) in all stored containers. Additional sensors data fusion technique like DAI-DAO can be programmed within the agent logic to partially deal with the communication problem by eliminating additional noise in the sensors readings and optimizing the overall detection time (Jakovlev et al., 2017).

By utilizing a sensors data fusion technique for radiation monitoring on short distances, detection time or threshold can be shorten in comparison to using all individual containers data separately by individual nodes. Data can be acquired and tested for accuracy along with the decrease in the estimation time, when only 1 additional communication is done for each separate accuracy area. This can prove to be the best solution. Each container can perform its own evaluation of the surrounding area at any given time and thus shorten the overall inspection time for the whole network. Ladder approach can be applied to deal with this problem as well. Figure 2 demonstrates how communication with only one container (*k* to *k+1*) in the highest accuracy area can lead to estimation of the whole container yard. Depending on the statistical background of the evaluation, each statistical area or alert area can be distinguished simply by estimating the distances between containers or any other well-known and computable onsite parameter. In this case, distance value can be used as a unique parameter, because it incorporates both signal strength indicator values and indicates the nearest neighbors in the network. In addition, background noise estimations and the deployed sensors density values must be known as well. Each message must contain this crucial information. The problem still exists - which parameters are vital for the working stability and security. This problem can be formulated as a rucksack problem. Each new accuracy area in *3-D* space can be formulated as (5):

$$Accurasy\_area_H = f(d(m_L, m_S)). \quad (5)$$

Messages can also include other estimations: accuracy of background noise estimation for each individual sensor and initial threshold time for the estimation of true detection time. Risk levels of the container can be estimated by different decision support systems, like the Automated Targeting System (ATS). Evaluation of the risk level can be used to estimate the accuracy area as well. Its initial value can be transferred through the network to the initiation node. Then the accuracy area can be evaluated taking into consideration the importance of the specific container. Further risk level assumptions are made within the initiation node. The final decision is made by the node to increase the accuracy area to perform additional evaluations of the risky container. These parameters may vary differently for each individual container. If no pre-determined risk is assessed by the ATS, then the priority of each node in the stack is the same. Each individual accuracy area H can be separated in-between other areas by a default value of 5%. (i.e. 0…100% with a 1…5% step). This principle is applied when a certain degree of accuracy is computed by the smart agent using the data defect levels.

The container accuracy area evaluation method includes two interconnected parts: the container itself and its built-in sensors. The reliability of each WSN node data is examined by the smart agent and the reliability of the information is examined. The decision support functionality work as an expert system within a node that provides decision about the truthfulness of the monitored container status. They include the following suggestions: each container can be in normal or defected state and network sensors can also be in normal state and provide correct information or in a defected state thus providing false information. Data is considered to be reliable when they describe the actual state of container.

The defect levels for WSN node *k* and the nearest WSN node *k+1* are introduced: 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, $Q_{INk+1} \in (0,1)$ and Q_{OUTk+1} is the modified defect level of data after the secondary evaluation in node *k+1* (nearest node in the network), $Q_{OUTk+1} \in (0,1)$. 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 to be used further in the estimation of the trustworthiness of the containers and accuracy area. The full evaluation of the accuracy area can be rewritten as (6):

$$Accurasy\_area_H \sim Q_{OUTk+1} \cdot 100. \quad (6)$$

In this method, each intelligent container can provide its own observation according to the requirements that are coded within the middleware agent. Each container node can compute its crucial parameters and then ask for other nodes to do the same. A step-by-step solution is presented (figure 3).

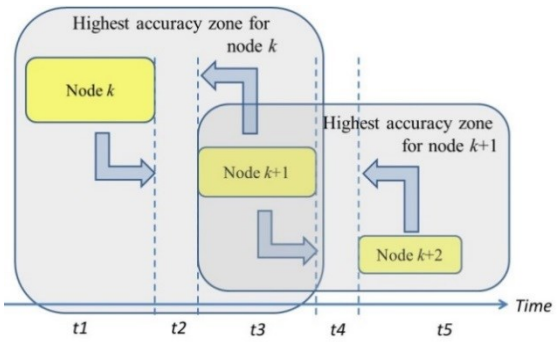

Figure 2: Overview scheme of the step-by-step solution.

One may notice that it is not an optimal solution. In this case *t2* and *t4* describe the networking time for the communication and messaging, *t1*, *t3* and *t3* are the computational times. Then the sum of the computational and the networking time values can be presented as $t_{Step} = t_1 + t_2 + t_3 + t_4 + t_5$. In this case, information acquisition for node *k* is done in a step-by-step manner. This step-by-step method can be changed according to the network activity. Each network node can acquire all the needed information in advance, process and store it locally. The proposed method can be used to avoid data loss in the network, when many nodes are talking to each other simultaneously. This could crash the entire network if a suitable synchronization protocol is not adapted. An obvious solution would be to integrate both methods into a single procedure. Monitoring of the environment can be done simultaneously to decrease the total detection time in the entire network and messages routing in the network can be done step-by-step at a local accuracy area pre-determined using the same principle for each neighbour. In figure 4, a different approach is presented.

This simultaneous network nodes activity method shows that in time $T_{Sim} = t_1 + t_2 + t_3$, information can be gathered more quickly, taking into account all the other actions related to time taken for sensor data manipulation by the agent, network routing and data transmission. Simultaneous messages retrieval can also trash the network and make it unstable.

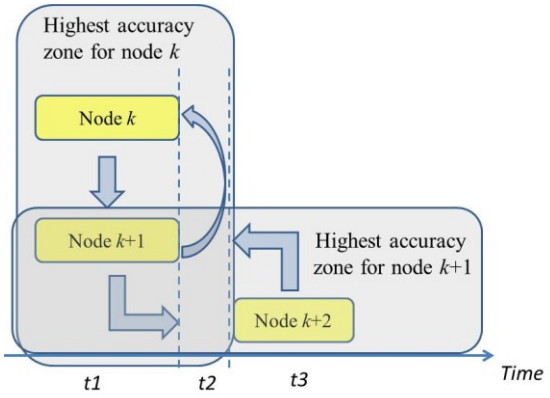

Figure 4: Overview scheme of the simultaneous network nodes activity.

3 CONCLUSIONS

In this proposed method, each node performs a local decision support based on the prediction of the background noise, estimation of the accuracy of the estimation and its surrounding area. The estimation of the required data sample size for the initial communication is a serious mathematical and computational problem, because each individual scenario requires a different statistical analysis approach for computing data reliability. The integration is possible only when there all necessary standardization tasks are finished and the system is widely used throughout the transport chain. This innovation must be taken into consideration not only by a single port authority, but by the whole global transport chain.

Therefore, any intelligent container knows the exact info it needs to know at the most appropriate moment and predict its neighbour's possible deviations in the monitored spectrum. This functionality is already implemented in some E-Seal systems. As briefly mentioned previously, application of intelligent systems plays an essential role in achieving the optimality goal of security in many countries of the world. These networking technologies can be applied in both in container yards, trucks, trains and ships to connect each individual container in a common network.

Future work includes research on the impact of delays, errors and other uncertainties on the communications protocol, its application in laboratory environment and in practice using research grant described below.

ACKNOWLEDGEMENTS

Authors would like to thank EU funded Research project “Ateities autonominis žaliasis uostas: naujo konteinerių krovos metodo ir sistemos prototipo sukūrimas“ (Nr. 01.2.2-LMT-K-718-01-0081) for the support while writing and publishing the manuscript.

REFERENCES

Chang, C.H., Xu, J., Song, D.P. 2014. An analysis of safety and security risks in container shipping operations: A case study of Taiwan, *Safety Science*. Vol. 63, p. 168-178.

Alexandridis, G., Sahoo, S., Song, D.W., Visvikis, I. 2017. Shipping risk management practice revisited: A new portfolio approach*, Transportation Research Part A: Policy and Practice*, In press, corrected proof. https://doi.org/10.1016/j.tra.2017.11.014.

Scholliers, J., Permala, A., Toivonen, S., Salmela, H. 2016. Improving the Security of Containers in Port Related Supply Chains, *Transportation Research Procedia*. Vol. 14, p. 1374-1383.

McLay, L.A., Dreiding, R. 2012. Multilevel, threshold-based policies for cargo container security screening systems, *European Journal of Operational Research*. Vol. 220(2), p. 522-529.

Jane A. Bullock, George D. Haddow, Damon P. Coppola. 2018. 7: Transportation Safety and Security. Book chapter. *Homeland Security (Second Edition)*, ELSEVIER. p. 169-188.

Truong, T.T., Brown, K.N., Sreenan, C.J. 2015. Multi-objective hierarchical algorithms for restoring Wireless Sensor Network connectivity in known environments, *Ad Hoc Networks*. Vol. 33, p. 190–208.

Anurag, S., Christian, W.O. 2009. Performance comparison of particle swarm optimization with traditional clustering algorithms used in self-organizing map. *International Journal of Computational Intelligence.* Vol. 5(1), p. 32–41.

Sausen, P.S., Spohn, M.A., Perkusich, A. 2010. Broadcast routing in wireless sensor networks with dynamic power management and multi-coverage backbones. *J. Inform. Sci.* Vol. 180(5), p. 653–663.

Hoblos, G., Staroswiecki, M., Aitouche, A. 2000. Optimal design of fault tolerant sensor networks. *IEEE International Conference on Control Applications*, pp. 467–472.

Bulusu, N., Estrin, D., Girod, L., Heidemann, J. 2001. Scalable coordination for wireless sensor networks: self-configuring. *International Symposiumon Communication Theory and Applications*, p. 1-6, Ambleside, UK.

Dimokas, N., Katsaros, D., Tassiulas, L., Manolopoulos, Y. 2011. High performance, low complexity cooperative caching for wireless sensor networks. *J. Wirel. Network.* Vol. 17(3), p. 717–737.

Polastre, J., Hill, J., Culler, D. 2004. Versatile low power media access for wireless sensor networks. *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, p. 95–107.

Krishnamachari, L., Estrin, D., Wicker, S. 2002. The impact of data aggregation in wireless sensor networks. *22nd International Conference on Distributed Computing Systems Workshops*. p. 575 – 578.

Wanga, X., Bischoffa, O., Laura, R., Paula, S. 2009. Localization in Wireless Ad-hoc Sensor Networks using Multilateration with RSSI for Logistic Applications. *In: Proceedings of the Eurosensors XXIII conference*. *Procedia Chemistry*. Vol. 1, p. 461–464.

Jakovlev, S., Andziulis, A., Bulbenkienė, V., Didžiokas, R., Bogdevičius, M., Plėštys, R., Zakarevičius, R. 2012. Cargo Container Monitoring Data Reliability Evaluation in WSN Nodes. *Electronics & Electrical Engineering,* Vol. 3(119), p. 91-94.

Jakovlev S., Kurmis M., Drungilas D., Lukosius Z., Voznak M. 2018. Multi-sensor Data Fusion Technique to Detect Radiation Emission in Wireless Sensor Networks. *AETA 2017 - Recent Advances in Electrical Engineering and Related Sciences: Theory and Application,* Lecture Notes in Electrical Engineering, Vol. 465, p. 135-144.

.