Taylor & Francis
Taylor & Francis Group

TRANSPORT
ISSN 1648-4142 print / ISSN 1648-3480 online
2012 Volume 27(4): 373–382
doi:10.3846/16484142.2012.750622

PRIORITY BASED TAG AUTHENTICATION AND ROUTING ALGORITHM FOR INTERMODAL CONTAINERS RFID SENSOR NETWORK

Arūnas Andziulis[1], Rimantas Plėštys[2], Sergej Jakovlev[3], Danielius Adomaitis[4], Konstantin Gerasimov[5], Mindaugas Kurmis[6], Valdemaras Pareigis[7]

[1, 3, 5, 6, 7]Dept of Informatics, Klaipėda University, Bijūnų g. 17, LT-91225 Klaipėda, Lithuania
[2, 4]Dept of Computer Networks, Kaunas University of Technology, Studentų g. 50, LT-51368 Kaunas, Lithuania
E-mails: [1]arunas.iik.ku@gmail.com (corresponding author); [2]rimantas.plestys@ktu.lt; [3]s.jakovlev.86@gmail.com; [4]danielius.adomaitis@gmail.com; [5]gerakon@gmail.com; [6]mindaugask01@gmail.com; [7]valdevaldas@gmail.com

Submitted 26 January 2011; accepted 28 March 2011

Abstract. Intermodal containers transportation management has always been a serious issue among logistics worldwide companies where the application of secure mobile information technologies (e.g. radio frequency identification systems (RFID) and sensor networks) could significantly improve the current situation by sending managers all the needed transportation conditions information. In this paper, we have focused on improving managerial decision making method by introducing the expert system evaluation functionality in a common software solution CTRMS for additional ICT risks evaluation. The basic risks involved in transportation and the appropriate measures are introduced as well. The pre-defined RFID sensor network was used to develop an optimal tag authentication and routing algorithm where tags and reader authentication protocols were defined and based upon the highest security assurance and the reader to tag response time criterias. A Nearest Neighbor (NN) heuristic approach and a Priority setting method were used to address the problem of routing within the RFID sensor network between tags with the objective function of minimizing the data transfer time between tags with the highest priority values. Computational results also indicate that when the tags have the same level of confidence in the system, they can exchange information without any additional verification, so making the authentication protocol less time consuming and therefore more effective against other proposed protocols.

Keywords: complex information system, intermodal container, RFID sensor network, priority setting, expert system.

1. Introduction

Intermodal container monitoring is considered as the main problem among many major logistic companies worldwide, due to the high rate of containers fleet addition (see Fig. 1), so now even the basic intermodal container transportation (ICT) management becomes a very difficult problem for conventional methods and systems. That is why a more agile and secure solution needs to be proposed.

The application of modern software and mobile technologies (e.g. radio frequency identification systems (RFID) and sensor networks) in ICT management systems plays an important role in maximizing the performance of services, reduction of costs and risks of transportation. In addition to the increasing number of TEU containers, based just on Wal-Mart's mandate and that of the U.S. Department of Defense (US-DOD), the RFID tag market in the U.S. retail supply chain was $91.5 million in 2003, and was expected to be around $1.3 billion in 2008 (Piramuthu 2007). Therefore, any substantial research in the problem area may have a great economical impact on any logistics company in the field of ICT worldwide. While there is much literature about the intermodal transportation management (Thill, Lim 2010; Macharis *et al.* 2010; Ishfaq, Sox 2010; Macharis, Pekin 2009; Limbourg, Jourquin 2009; Kreutzberger 2008), comparatively little has been written about sensor based active and passive RFID technology implementation in ICT (Andziulis *et al.* 2010; Ngai *et al.* 2007), optimized information and expert systems usage in ICT management (Mikulėnas, Butleris 2010; Wen 2010; Dias *et al.* 2009).

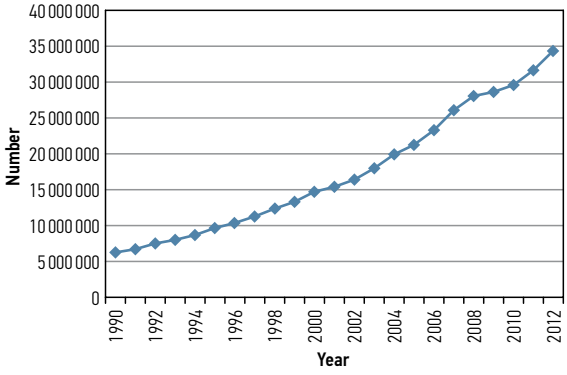

Fig. 1. End-year fleet size (data provided by the World Shipping Council – *http://www.worldshipping.org*)

The aim of this research is to describe a complex information system (CIS) for intermodal container management. System that consists of an RFID sensor network and software based solution. Also to propose a new secure tag authentication and routing algorithm in a container warehousing environment based on Priority settings and an expert system evaluation method that ensures seamless real time end-to-end tracking and cargo conditions visibility from global, to local level in intermodal transportation, a problem introduced by Ferrer *et al.* (2010). In addition, privacy and security issues play critical role in acceptance of RFID sensor network technologies by the general public, since most people are afraid of being monitored, tracked, watched etc. Although other technological means are already implemented and are in a widespread use by the same general public, some of the inherent properties of RFID tags render opportunities for suspicion including their low cost, physical size, privacy assessment etc.

2. Description of the Main CIS Functionality and the Basic Security Aspects

When creating a specific CIS it is very important to analyze the current situation from different perspectives, all the newest and the most promising systems, protocols and other algorithms available and to decide what can be done faster and safer, although the combination of different mobile and other information technologies in one CIS can be very difficult to implement (Kaya *et al.* 2009; Jedermann *et al.* 2006) due to the different standards used to gather, process and safely transfer data, where Knospe and Pohl (2004) specified the basic RFID communication protocols Table 1 and suggested future RFID technology development in the logistics research area.

The nowadays widespread use of modern mobile technologies has introduced a new challenge concerning the security aspect of the data being transferred. It became essential to design information systems to withstand external attacks as well as internal malfunctions in the system, and to rapidly recover from them. Such system infrastructure security is a serious issue, where Chen and Deng (2009) proposed a new RFID system authentication and encryption method to ensure security between tags and readers that not only reduces database loading, but also ensures user's privacy proving its feasibility for use in several applications and analyzing all the basic security viewpoints. Van Deursen and Radomirović (2009) investigated the security claims of a RFID authentication protocol and exhibited a flaw which has gone unnoticed in RFID protocol literature and presented the resulting attacks on authentication, intractability, and resynchronization resistance.

Kang *et al.* (2008) proposed a secure authentication protocol to provide information to an authorized user by applying recognition technology in an insecure communication channel even for the communication between the database and the initial reader in the RFID system.

Table 1. The main RFID ISO standards (ISO 18000 Air interface)

Standards/ISO	Specification
Part 3-1: (ISO 18000–3)	13.56 MHz for HF systems. Compatible with ISO 15693
Part 3-2: (ISO 18000–3)	Next generation RFID system in the same frequency band with higher bandwidth with up to 848 Kbit/s and faster scanning of multiple tags.
Part 4: (ISO 18000–4)	2.45 GHz systems: in mode 1 a passive backscatter system and in mode 2 a long range, high-data rates system with active tags (self powered).
Part 6: (ISO 18000–6)	A passive backscatter system in 900 MHz range band.
Part 7: (ISO 18000–7)	An RFID system with active transponders and long range in the 433 MHz band. Long ranges, high data transfer rate, concurrent read of less than a 100 items, cannot penetrate water or metals.

Container monitoring is considered as a major security issue in many countries where the application of new intermodal container transportation management technologies plays an important role in optimizing the performance, reducing the cost and risks of transportation.

On the other hand, similar variations of the RFID and sensor based CIS have already proven their direct value in the field of intermodal transportation (Lee, Chan 2009; Hsu *et al.* 2009).

At this point, the evaluation of the potential forecasted risks involved in risk cargo transportation is prioritized, thus providing a mobile cargo security assurance service. Here the automatic wireless reading of multiple RFID tags creates an enormous data flow that is potentially beneficial to the transport operation management, enabling improvements in the accuracy and speed of delivery promise.

At this point, the amount of information transferred and data links established at one point in time must be minimal to gain the best results possible. The basic functionality of the CIS consists of optimal communication between intermodal tagged containers and end-user software (see Fig. 2).

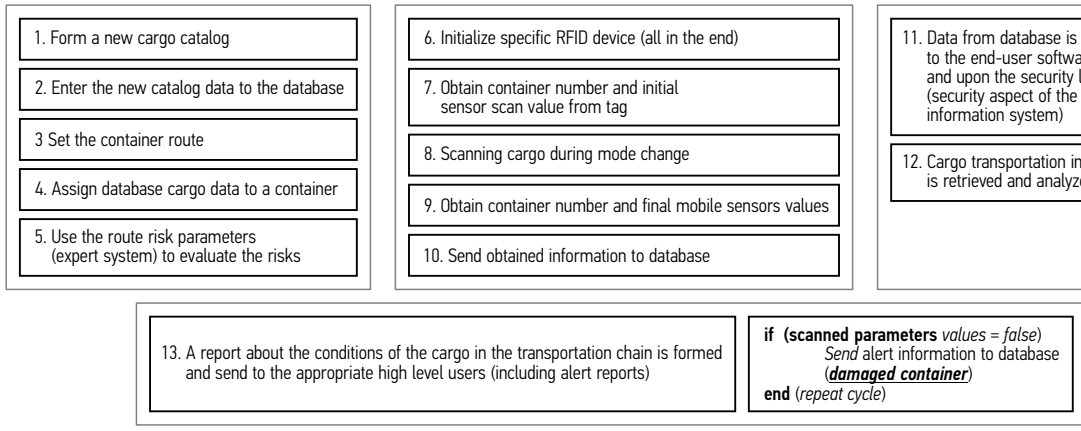

Fig. 2. Overall CIS functionality description

The approach is the use of active RFID tags joint with mobile sensors that are attached inside intermodal shipping containers. Sensor inside the container can report on the overall condition and integrity of the cargo during the whole transportation or on each check location, providing the needed security and safety assurance so important for managers during the whole transportation period.

Once the check is activated the transponder communicates with the RFID tags wired to sensors that measure changes in environmental variables, such as: temperature, humidity, vibration etc. In an alert situation, if a problem occurs during a cargo check or if the acquired RFID data indicates the probable cargo damage, then this action triggers other events, processes, SMS alerts or report notifications to occur automatically and to be sent to the end-user software. The amount of data to be sent to the end-user software is predefined by individual users' privileges.

Such safe precaution system would be capable of minimizing the time spent on cargo checks and would let the system automatically decide when to bother employees, thus minimizing the rate of data errors in the proposed CIS in a real time manner.

3. Description of the Single Round Protocol for Multiple RFID Sensor Network Tags

Most existing applications of RFID system tags are not secure, and can leak data about the cargo inside the containers. At this point it is possible to silently track/monitor the object without appropriate permissions. Some common types of attacks on RFID tags include: eavesdropping, replay attack, loss of data including DoS (denial of service) and message hijacking and other physical attacks.

Such problems that deal with tags and readers authentication are addressed by many authors worldwide (Piramuthu 2007) and many lightweight and secure to a reasonable extent algorithms and protocols have already been proposed. Nevertheless, there are still blind spots in the RFID technology that need additional attention (Dimitriou 2005). Such protocols address a specific scenario involving RFID tag applications, where simultaneous presence of two or more tags in a reader's field is to be proved (Saito, Sakurai 2005; Juels 2004). Notations used in this section:

- s, r, r_B, r_C: random l-bit (or k-bit) vectors;
- s_i, ID: tag identifier;
- h, H, G: hash functions —$\{0,1\}^l$ or $\{0,1\}^k$;
- V: verifier for MAC;
- MAC: Message Authentication Code;
- MAC_x $[m]$: MAC using secret key x on message m
- P_{BC}: proof B and C tags scanned simultaneously.

The idea is to ensure that the inputs to a tag are based on parameters that are necessary for the other tag, and to create dependence of the tags on each other so that they cannot be processed separately in the proof without the presence of the other tag. We assume that the reader authenticates itself with the back-end verifier before beginning the process of obtaining r from V as well as when returning P_{BC} at the end of the process. While generating a proof, when a transmission of interest fails to reach its intended receiver, the transaction is cancelled and started all over again with a fresh r from V, using a pre-defined time limit (Piramuthu 2007).

The proof is as follows: the addition of a random variable (r) sent to both the tags from the verifier through the reader. This helps to keep track of the time duration between the initial transmission from the reader to the B tag and final submission of P_{BC} for verification by the verifier. The random variable r is also used as seed for generating r_B and r_C by the tags; the MAC generated by T_C depends on both r and r_C. The use of r_B in generating m_C is crucial. Since r_B is generated and used internally in T_B for generating m_B as well.

Because r is generated by the verifier, the dependence on r for generating m_C adds yet another layer of protection against attacks; the fifth transmission in the proof is m_C instead of r_C. This helps in the generation of m_B; the use of m_C in generating m_B is crucial since T_B has to wait for T_C to generate m_C. Therefore, T_B's part of the proof cannot occur before T_C's part and T_C's part cannot happen independently since it too is dependent on input from T_B (r_B). T_B also generates r_B, which is kept internal; it is not received as input from an outside entity.

A possible extension would be to collapse the messages sent to tag T_C into the reader and let the reader generate m_{C_i} (i = 1, …, n here n is the number of tags of interest) values for each of the tags. Fig. 3 provides a description of the interactions between the reader and the i^{th} tag (T_i). The same r is transmitted by the reader to all n tags. In the end, P_A is evaluated based on the r_1, …, r_n, r, m_1, …, m_n values (Piramuthu 2007).

Ohkubo *et al.* (2003) considered a protocol that relied on two hash chains (G and H) to update a random identifier that is stored both in the tag as well as the system's database. The random identifier begins with s_1. When the reader sends a request to the tag, the tag computes $G(s_i)$ and sends it to the reader and then updates the identifier using the other hash function H (s_i+1 = $H(s_i)$). The backend database linked to the reader maintains pairs of (ID_k, s_1 k) where ID_k is the identifier and s_1 k is the initial secret information for tag k. After receiving the second message, the back-end database does an exhaustive search of hashed values to identify the tag (Piramuthu 2007).

This protocol assures privacy since the information sent by the tag is indistinguishable from a random value in a random oracle model. It also assures forward privacy because of the one-way hash functions. However, it is not protected against replay attacks. Avoine *et al.* (2005) propose a modification to this protocol to prevent replay attacks (see Fig. 4). The modified protocol uses a fresh challenge (r) sent by the reader, thus preventing replay attacks since the adversary cannot replay $G(s_i \oplus r)$ with a different r, here $\oplus$ is the XOR operator. The same technique could be used for each tag authentication in the RFID sensor network during the application of the tags routing algorithm, as it introduces a simple, fast and secure protocol.

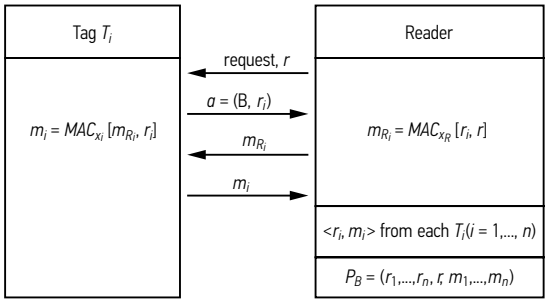

Fig. 3. Modified proof for more than 2 tags (Piramuthu 2007)

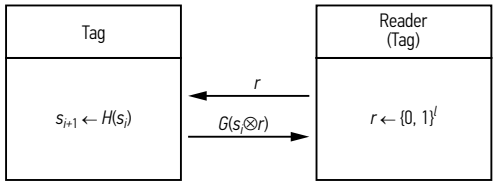

Fig. 4. Modified Tag (Reader) to Tag protocol (Ohkubo *et al.* 2003; Avoine *et al.* 2005); Piramuthu (2007) and Authors of the current paper)

4. RFID Sensor Network Security Based on Priority Settings

The rapid development of different mobile technologies raised the question of safe initial information detection during authentication and other routing algorithms (Adomaitis *et al.* 2010) used in the RFID sensor networks. Such services proved to be very effective in transport and logistics areas where precision and timeliness are very important.

In this case, the above mentioned services could be referred to as the main measurable parameters of the RFID sensor network Table 2 and the main ID requests (identification procedures).

Table 2. Risk factors

Risk factors	Risks considered
Temperature	+
Humidity	+
Ventilation	+/– (has impact on the temperature and humidity)
Vibration	+
Shrinkage/Shortage/Theft	–
Others…	…

The modeled services could be presented as: Service-1 as Temperature, Service-2 as Humidity, Service-3 as Vibration and Service-4 as the main RFID systems' functionality for the successful connection to the reader and to transfer of all the needed data. Basically, all CIS are designed to combine and control various portable IT devices in real time. Such would be the above mentioned RFID sensor network, where the applications of functional protection algorithms help to solve different security, privacy and authentication challenges.

All general cryptographic algorithms used within the system require a lot of system resources and in the end – decreased data transfer and analysis speed and overall security. On the other hand, it makes each service providing process safer by controlling each separate tags confidence level in the common RFID sensor network. Nevertheless, the use of mobile services is directly linked to service security assurance and in time error fix, which nowadays is not commonly applied in practice.

Modern CIS should include separate object state control for a more effective resource and service control included in the RFID sensor network model (Ahamed *et al.* 2009, 2010). One of the most beneficial and widely used IT proposals is the middleware, that would enable connection of various programs, computer systems, RFID sensor network and data transfer mechanisms control integration in one common ICT management system CTRMS. Despite all the advantages, there are still many flaws that need additional analysis.

Although, modern solutions require not only the main functionality described at the highest level, but also all new services such as tags Priority settings that would allow identification and usage of each separate

system devices (later on indicated as RFID sensor network tags) Trust/reliability with the RFID sensor network in real time manner.

4.1. The Main Criterions that Affect the Service Providing System

Priority function control needs to store information that describes the confidence levels (0 to 1.0) and is dependent upon the each tags (containers) negative or positive impact history confidence level update rule. Information about the tags resource/service group is also a very important aspect and the overall such resource number in the system varies from separate tags resource available R_e (from 0 to 1.0).

Another important criterion is the information about the successfully accomplished service operations O_{sc} (from 0 to 1.0) that depends on the recommendations from other tags based upon successfully completed service providing operations (e.g. number). Also, a function algorithm is introduced to store all the information about the data transfer events for further deeper separate tag analysis.

Using the separate system modules, function algorithm database (*DB*) and the Priority set function, similar or the same Trust value tags are combined into separate groups for faster and safer resource/service exchange. Using the Priority set control rules, tags get all the information needed for a safe disconnect from the system. Such could be the disconnect time range control, where the resource/service provider disconnects only after a successfully implemented service, otherwise that tag is introduced to the harmful tag list, gets lower Trust level. That is how the systems reliability is assured, also providing the high level of confidence among all RFID sensor network tags and the main CIS and its software component CTRMS. That in turn, enables more effective and reliable service providing functionality.

4.2. Formulation of Mean Trust Values for Wireless Networks

Confidence control determines the confidence values and confident/reliable links with other tags of the system (network). The basic confidence value calculations are performed based on the service providing tags and their customers provided initial parameters. Confidence values are constantly calculated and updated within the system (network) between the tags, based on the history of the specific tag when it provides a service (Ahamed, Sharmin 2008).

After each new update all the newly calculated Trust values for all of the tags are formed into a report and sent to the main security providing, control section. The mean Trust values (Sharmin *et al.* 2006) can be calculated as (1):

$$t\left(SP,B\right)=\left(\sum_{i=1}^{n}S_i\cdot T\left(SP_i,B,x\right)\right)\Big/\sum_{i=1}^{n}S_i, \qquad (1)$$

where: *SP* – is the provider of the service; SP_i – is the (*i*) service of the provider tag; $t(SP, B)$ – is the mean *SP* Trust value for tag *B*; S_i – *i*-th service security level ($1<= S_i <= 10$); $T(SP_i, B, x)$ – is the reader *B* Trust value for service (*i*); $x(0.0 <= x <= 1.0)$ is the possible Trust value that can be acquired; *n* – is the number of services that link SP with tag *B*.

4.3. Formulation of Mean Priority Values for Wireless Networks

All the mean Priority values ρ are acquired by using the equation (2):

$$\rho\left(SP_m,n_p\right)=\left(\sum_{m=1}^{n}S_m\cdot\left(\frac{R_{ee}}{O_{sc}}\right)\cdot t\left(SP_m,n_p\right)\right)\Big/\sum_{m=1}^{n}S_m, \qquad (2)$$

where: R_e – are the used tag resources; O_{sc} – successfully completed operation; *n* – number of services, between *SP* and *B, C, D, ..., n*$_p$; $p(SP_m, n_p)$ – mean *SP* Priority values for tag n_p; $t(SP_m, n_p)$ – mean *SP* Trust value for tag n_p; S_m – *m* service security value.

5. Evaluations of the Transportation Conditions by an Expert System

Basically, the system can provide a way to minimize the foreseen cargo losses with the customer before the actual loss takes place. It also provides two-way mobile communication within a supply chain network that enables real-time analysis of the current transportation situation and forecast possibility by evaluating the route risk parameters.

Such route risk analysis is programmed as an expert system and presented as a graph of peaks and downfalls during the whole container transportation route, indicating each check location probability of being the point of higher risk then the point before and etc. Where each expert *T* support consists of knowing the exact statistical probability of the damage or loss in the containers and using that information to describe the risk situation with a formal value.

All the input data for the expert system can be split into 4 main groups:

- regional weather conditions at all check locations;
- each container evaluation model;
- transportation infrastructure model;
- additional expert support.

Expert system consists of an expert knowledge base and database as inputs to Inference engine. Inference engine consists of a neural network block. Where the expert knowledge base has the initial service risk parameter value range of $\varepsilon', \phi', \gamma' = \{1:9\}$, and finally the output parameter that consists of final service risk parameters ε, ϕ, γ *w*here an assumption was made that the initial and final service risk parameter variations are ε, ϕ, γ ={1:9} for easier expert risk percentage evaluation 1÷100% (at 10% step). The initial service risk probability ditributon for expert evaluation can be formulated for $W_1 \in (1,3]$, $W_3 \in (3,6]$ and $W_3 \in (6,9]$ and for each ε'_q, ϕ'_q, γ'_q value, formulated in an initial expert evaluation matrix, see Table 3, where *q* – is the number of experts.

There W_1 represents the low risk probability, W_2 represents the medium risk probability and W_3 repre-

sents the high risk probability used in the expert evaluation of the initial service risk parameters. The probability is derived from separate expert knowledge. It also should be noted, that one of the function components of the inference engine is that each separate check point must have a service risk parameter higher than the rest evaluations with $\overline{\varepsilon}' = \varepsilon$, $\overline{\phi}' = \phi$, $\overline{\gamma}' = \gamma$.

The neural network block adds sufficient advantages as it can update the knowledge base from the knowledge gained through several sessions of interaction with the system, its users and the introduced databases, thus decreasing the use of additional expert support. Such expert system functionality can be systemized and introduced as a separate instance for automatic expert values generation.

On the other hand, there is a problem of each expert having accurate knowledge base for the estimation of the risk possibility in the current check location or during the transportation period. Each new expert's evaluation should compensate the previous ones inaccurate estimations based on the standard deviation sums from those expert evaluations for each case, to seek the minimum value (3):

$$\min\begin{cases}\dfrac{1}{q-1}\displaystyle\sum_{u=1}^{q}\left(x_i' - \overline{x'}\right)^2; \\ \dfrac{1}{q-1}\displaystyle\sum_{u=1}^{q}\left(y_i' - \overline{y'}\right)^2; \\ \dfrac{1}{q-1}\displaystyle\sum_{u=1}^{q}\left(z_i' - \overline{z'}\right)^2. \end{cases} \tag{3}$$

Thus, it is possible to provide the neural network block with an additional check functionality, to see if the deviation is acceptable in the given region for any W_n.

Table 3. Expert evaluations matrix

Risk parameters	Expert evaluations				Mean values
	T_1	T_2	…	T_q	
ε'	W_1	W_1	…	W_n	$\overline{x'}$
ϕ'	W_2	W_2	…	W_n	$\overline{y'}$
γ'	W_3	W_3	…	W_n	$\overline{z'}$

6. Formulation of the RFID Sensor Network Routing Problem

The main objective of the routing problem is to minimize the data transfer time between tag to tag and reader to tag with the pre-defined tag authentication and priority based secure data transfer algorithm. When modeling such RFID sensor network in an interconnected warehousing environment it is sufficient enough to present only a separate containers line to be analyzed as a model. So the objective function for each separate containers line can be formulated as (4):

$$\min \sum_{y=1}^{n_p-1} c_y^p \cdot \rho\left(SP_m, n_p\right), \tag{4}$$

where: p is the number of the containers line and $n_p \in Z, Z \geq 0$ is the number of containers in a defined line; c_y^p and $C^p = \left\{c_y^p\right\}$ represents tags data transfer times, tag distance, between 2 scheduled containers later on signed as i (i = 1, …, n_p) and j (j = 1, …, n_p), $C^p = \left\{c_{ij}^p\right\}$, where C^P presents the finite set (n_p – 1) of available objective function tags data transfer times.

NN Heuristic for Solving the Tags Routing Problem. The Nearest Neighbor (NN) algorithm is simple heuristic for the solution of the tag routing problem via scheduling presented as a travelling salesman problem where Gutin *et al.* (2002) suggested that NN algorithms produce comparatively good solutions with known TSP. So the main routing algorithm is described by 6 main steps for each separate container (later on used only as tag) line:

1. Stand on an first current arbitrary tag e_β^p, $Q^p = \left\{e_\beta^p\right\}$, where Q^P is the finite set of available tags from the p containers line, where β represents the currently selected tag and (β + 1) represents the next tag not previously selected from Q^P, where any e_β^p is the first (second etc.) selected arbitrary tag from the p containers line. The first selection is made according to the nearest positioning to the reader and is defined by the minimum time for tag activation. As for other tags currently in line, the final activation is made only after the activation times are gathered and the minimum value is found. That way the ID of the tag is known and it gets the highest Priority value in the containers line (is the first arbitrary tags line activation tag).
2. Find the shortest arbitrary distance c_{ij}^p between tags i and j connecting the current tag and any previously unselected tag $e_{\beta+1}^p$.
3. Set current tag to $e_{\beta+1}^p$.
4. Mark e_β^p and $e_{\beta+1}^p$ as visited/activated.
5. Go to step 2 with the initial β to be β = β + 1. If all the tags are selected β = n_p, then terminate the algorithm.
6. The sequence of the selected tags is used vice versa for the routing of the transferred RFID sensor network data.

That way, it could be suggested that it is possible to get a near optimum objective function value with the given NN algorithm.

7. Computational Results

In section 7.1 the main Priority and Trust based simulation of the RFID sensor network is presented and in section 7.2 an expert system evaluation simulation is also presented based upon the statistical data analysis of the gathered weather conditions and cargo and container damage possibilities using the additional expert support.

7.1. Simulation of the Priority Settings Assessment

The main parameters which affect the service providing functionality are presented and respectively evaluated, thus it is possible to provide a high level of overall system reliability and sustain the best level of confidence between separate tags of the RFID sensor network. That in turn would allow fast and secure resource service exchange.

Based on the modeled tags locations in the system/network and the distances between them and the service provider (*SP*) Fig. 5, a notion is made that the acquired Trust values are decreased evenly. In this case, reader has the highest Trust value to tag *B*, which gives him the highest Trust value in the network because it is the first in the defined container line to be activated and work as a secondary network reader with each new tag working as a service provider to other tags in the network by means of a routing algorithm described in Section 6.

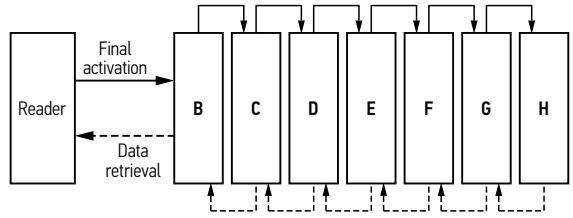

Fig. 5. Chosen RFID sensor network scheme

To determine the confidence level to each of the tag of the system/network and to assign the services and their availability level, the primary conditions (tag identification data) are introduced for each tag, to which tag *B* will provide its services (*SP*), see Table 4. Here *t* is the mean Trust value and $T(SP_i, B, x)$ for service all services are $x = 0.5$, exception is made for RFID identification with $x = 0.9$. All other tags have $x = 0.5$ assigned to them for sensors data and RFID identification services as $x = 0.3$.

To make the service providing system functionality more comfortable in use (tag friendly), the main priorities need to be determined. The tag with the highest Priority could use all the services and provide their own without programmable selection function.

Table. 4 Service-level security assessment of tags Trust values

Tags	Service provided (RFID network data transfers)				*t*
	Service-1	Service-2	Service-3	Service-4	
B	0.7	0.6	0.2	0.9	0.650
C	0.4	0.4	0.7	0.9	0.425
D	0.2	0.3	0.4	0.9	0.400
E	0.8	0.6	0.5	0.9	0.436
F	0.1	0.1	0.6	0.9	0.394
G	0.8	0.9	0.9	0.8	0.453
H	0.6	0.5	0.4	0.4	0.458

For that purpose, at present, 3 major service providing areas within the modeled network (tags B, C, D, E, F, G, H connected and sharing different services), based on the mean Trust values, where the 1st area (the highest 0.7÷1.0), the 2nd area (the middle 0.4÷0.7) and the 3rd area (the lowest 0.1÷0.4) that have effect on the service providing functionality to all of the system service tags.

Based on the system mean confidence values, it is possible to obtain the mean *SP* Priority values for each separate tag and to use them to form the service Priority usage identification rule for each separate tag. Based on the mean Trust values the mean *SP* Priority values are found for each separate tag and thus each service use prerogative rule is defined, see Tables 5 and 6. It is also advised to store all the needed data from the separate modules of the system for better Priority control. Determining the mean *SP* Priority values for tags n_p, $\rho(SP_m, n_p)$ minimizes the reliable tag search time and space, this way providing continuous and safe data exchange.

Table 5. Initial conditions for the Priority value (criteria) calculations

Connected tags	Mean *SP* trust value for tag – $t(SP_m, n_p)$	Security Values of Services, S_m	Succesfully completed data transfer, O_{sc}	Used RFID tag resources, R_e
B	0.650	$S_1 = 2$; $S_4 = 10$	0.4	0.6
C	0.425	$S_1 = 2$	0.2	0.4
D	0.400	$S_1 = 2$; $S_2 = 3$; $S_3 = 2$; $S_4 = 10$	1.0	1.0
E	0.436	$S_1 = 2$; $S_4 = 10$	0.5	0.6
F	0.394	$S_1 = 2$; $S_4 = 8$	0.7	0.8
G	0.453	$S_1 = 4$; $S_4 = 9$	0.5	0.6
H	0.458	$S_1 = 2$; $S_2 = 2$; $S_3 = 4$; $S_4 = 10$	0.6	0.7

Table 6. Calculated network tags mean Priority values based on the provided services

Network tag	Service-1	Service-2	Service-3	Service-4	ρ
B	2	0	0	10	0.975
C	2	0	0	0	0.850
D	2	3	2	10	0.400
E	2	0	0	10	0.523
F	2	0	0	8	0.450
G	4	0	0	9	0.544
H	2	2	4	10	0.534

When allocating network tags by Priority levels, it is necessary to evaluate such aspects as resources and successfully performed data transfers (provided services).

Substantial errors may occur when these aspect are overlooked, which may lead to false priorities distribution and as a result false resource sharing between tags with different priorities levels. Such allocation of tags in the network can lead to systemic unreliability and false services providing system functionality, that has direct impact on the security (users privacy) of the provided services.

That is why the resource/service provider disconnects only after a succesfully implemented service, otherwise it is introduced to the harmful tags list and that in turn assures high level of systems reliability also provides high level of confidence among other RFID sensor network tags. There the numerical verification results suggest that when the tags have the same level of confidence in the system, they can exchange information without any additional verification, so making the authentication protocol less time consuming and therefore effectively manage data transfer speed within the network with a high confidence in the security of the data gathered data (see Fig. 6).

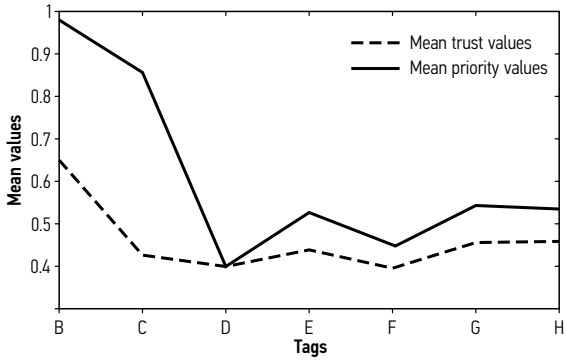

Fig. 6. Comparison of mean Trust and Priority values

7.2. Simulation of an Expert System Evaluation

With the given knowledge base update rule, the biggest risk possibility simulated by the expert system (see Table 7) was in the 5th check location (see Fig. 7) and proved to have the highest risk value with the cargo being damaged due to vibration (presented in Figs 8 and 9).

Such programmed expert evaluation is only possible for those risk factors that depend only on the above mentioned conditions, such as:

- regional weather conditions at all check locations (forecasted and statistics);
- each container evaluation model (forecasted and statistical;
- transportation infrastructure model (although, it has lots of limitations concerning human factor and any other unforeseen risks that cannot be evaluated or forecasted;
- additional expert support help (such expert support can be somehow incompetent with some arguable questions concerning transportation of risk cargo), where shrinkage, shortage and theft is a predicted factor for each region of the route and is evaluated using statistical data for a certain period of time and the use of additional expert support as well.

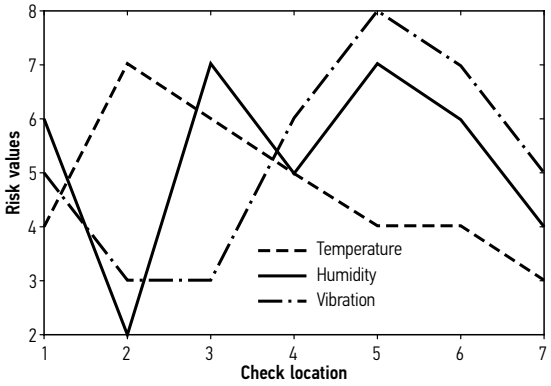

Fig. 7. Simulation of the expert system evaluation

Table 7. Simulated expert system evaluations

Measured risk factors	Modeled route check points						
	1	2	3	4	5	6	7
Temperature, γ	4	7	6	5	7	6	4
Humidity, ϕ	6	2	7	9	4	4	3
Vibration, γ	5	3	3	6	8	7	5

Active RFID technology provides the ability to automatically collect real-time cargo data without burdening employees and no operator intervention is required at that moment.

This provides company managers with an accurate up-to-the-minute picture of transportation processes and activities with a constant usage of update functionality of the CIS software component CTRMS (see Fig. 8).

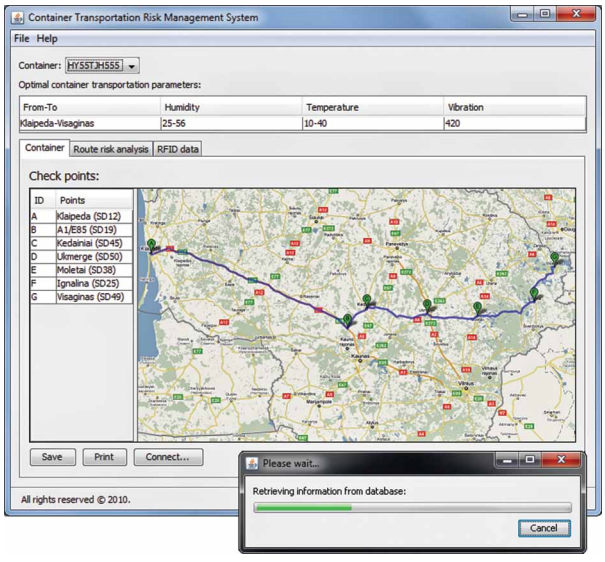

Fig. 8. Initial route description and the main parameters update function (initial database with all the statistical data)

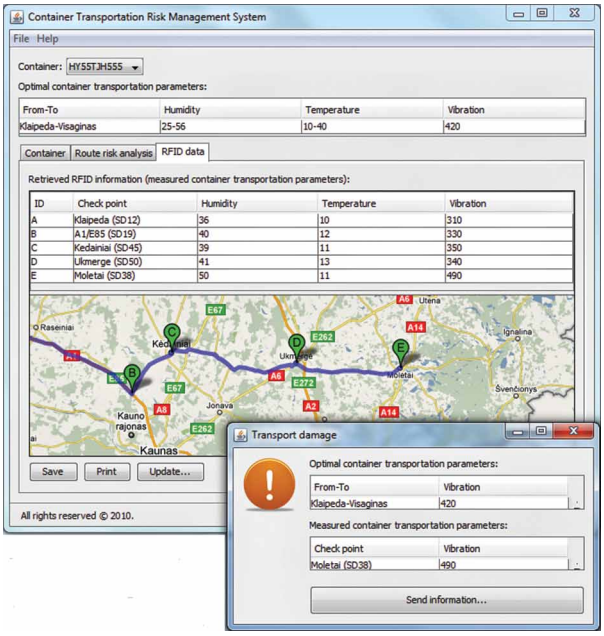

Fig. 9. CTRMS simulation

This in turn, allows them to respond to developing problem situations in a timely manner (see Fig. 9).

Conclusions were validated at a simulated case study in Lithuanian region with 7 check locations specified: including weather conditions at a specific time interval.

8. Conclusions and Future Work

First of all, we have focused on improving managerial decision making method by introducing the expert system evaluation functionality in a common software solution CTRMS for additional ICT risks evaluation, also to be used as an interface for the common CIS. At this point, managers are introduced to the basics of identifying the risks involved in transportation and take appropriate measures in real time manner. Secondly, a pre-defined RFID sensor network was used as a basis for the development of an optimal tag authentication and routing algorithm. Tags and reader authentication protocols were defined based upon the highest security assurance and the reader to tag response time criterias where a simple NN heuristic approach and a Priority setting method were used to address the problem of routing within the RFID sensor network between tags with the objective function of minimizing the data transfer time between tags with the highest priority values (tag response, data retrieval and transfer sum time). Finally, as Ferrer *et al.* (2010) stated, the proposed CIS full integration will only be successful if all the system users can trust it. The benefits derived from the use of RFID and sensor technologies have to outweigh the privacy concessions of many general and less effective ICT management systems.

Future work includes proposed CIS full application in Klaipėda University student project 'Intelligent Train Control System'.

Acknowledgement

The authors would like to thank project MOBAS 'The development of information environment for mobile and wireless services' (Nature and Technology Science Committee at the Lithuanian Science Council, Nr. AUT–03/2010) for the financial support while writing and publishing the manuscript.

References

Adomaitis, D.; Bulbenkienė, V.; Andziulis, A. 2010. Design and integration of software tools for control of services and resources in TI systems, in *16th International Conference on Information and Software Technologies* IT2010. *Research Communications*, 21–23 April 2010, Kaunas, Lithuania, 29–32.

Ahamed, S. I.; Li, H; Talukder, N.; Monjur, M.; Hasan, C. S. 2009. Design and implementation of S-MARKS: a secure middleware for pervasive computing applications, *Journal of Systems and Software* 82(10): 1657–1677. http://dx.doi.org/10.1016/j.jss.2009.03.020

Ahamed, S. I.; Haque, M. M.; Hoque, E.; Rahman, F.; Talukder, N. 2010. Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments, *Journal of Systems and Software* 83(2): 253–270. http://dx.doi.org/10.1016/j.jss.2009.09.040

Ahamed, S. I.; Sharmin, M. 2008. A trust-based secure service discovery (TSSD) model for pervasive computing, *Computer Communications* 31(18): 4281–4293. http://dx.doi.org/10.1016/j.comcom.2008.07.014

Andziulis, A.; Jakovlev, S.; Adomaitis, D.; Steponavičius, R.; Kurmis, M.; Pareigis, V. 2010. Integration of Information System Models in Intermodal Container Transportation Systems, in *Transport Means – 2010: Proceedings of the 14th International Conference,* 21–22 October 2010, Kaunas, Lithuania, 127–130.

Avoine, G.; Dysli, E.; Oechslin, P. 2005. Reducing Time Complexity in RFID Systems, in *Selected Areas in Cryptography: 12th International Workshop, SAC 2005*, August 2005 Kingston, Canada, 291–306.

Chen, C.-L.; Deng, Y.-Y. 2009. Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection, *Engineering Applications of Artificial Intelligence* 22(8): 1284–1291. http://dx.doi.org/10.1016/j.engappai.2008.10.022

Dias, J. C. Q.; Calado, J. M. F.; Osório A. L.; Morgado, L. F. 2009. RFID together with multi-agent systems to control global value chains, *Annual Reviews in Control* 33(2): 185–195. http://dx.doi.org/10.1016/j.arcontrol.2009.03.005

Dimitriou, T. 2005. A lightweight RFID protocol to protect against traceability and cloning attacks, in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005 SecureComm 2005*, 5–9 September 2005, Athens, Greece, 59–66. http://dx.doi.org/10.1109/SECURECOMM.2005.4

Ferrer, G.; Dew, N.; Apte, U. 2010. When is RFID right for your service?, *International Journal of Production Economics* 124(2): 414–425. http://dx.doi.org/10.1016/j.ijpe.2009.12.004

Gutin, G.; Yeo, A.; Zverovich, A. 2002. Traveling salesman should not be greedy: domination analysis of greedy-type heuristics for the TSP, *Discrete Applied Mathematics* 117(1–3): 81–86. http://dx.doi.org/10.1016/S0166-218X(01)00195-0

Hsu, C.-I.; Shih, H.-H.; Wang, W.-C. 2009. Applying RFID to reduce delay in import cargo customs clearance process, *Computers and Industrial Engineering* 57(2): 506–519. http://dx.doi.org/10.1016/j.cie.2008.02.003

Ishfaq, R.; Sox, C. R. 2010. Intermodal logistics: the interplay of financial, operational and service issues, *Transportation Research Part E: Logistics and Transportation Review* 46(6): 926–949. http://dx.doi.org/10.1016/j.tre.2010.02.003

Jedermann, R.; Behrens, C.; Westphal, D.; Lang, W. 2006. Applying autonomous sensor systems in logistics – combining sensor networks, RFIDs and software agents, *Sensors and Actuators A: Physical* 132(1): 370–375. http://dx.doi.org/10.1016/j.sna.2006.02.008

Juels, A. 2004. 'Yoking-proofs' for RFID tags, in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004*, 14–17 March 2004, Bedford, MA, USA, 138–143. http://dx.doi.org/10.1109/PERCOMW.2004.1276920

Kang, S.-Y.; Lee, D.-G.; Lee, I.-Y. 2008. A study on secure RFID mutual authentication scheme in pervasive computing environment, *Computer Communications* 31(18): 4248–4254. http://dx.doi.org/10.1016/j.comcom.2008.05.006

Kaya, S. V.; Savaş, E.; Levi, A.; Erçetin, Ö. 2009. Public key cryptography based privacy preserving multi-context RFID infrastructure, *Ad Hoc Networks* 7(1): 136–152. http://dx.doi.org/10.1016/j.adhoc.2007.12.004

Knospe, H.; Pohl, H. 2004. RFID security, *Information Security Technical Report* 9(4): 39–50. http://dx.doi.org/10.1016/S1363-4127(05)70039-X

Kreutzberger, E. D. 2008. Distance and time in intermodal goods transport networks in Europe: a generic approach, *Transportation Research Part A: Policy and Practice* 42(7): 973–993. http://dx.doi.org/10.1016/j.tra.2008.01.012

Lee, C. K. M.; Chan, T. M. 2009. Development of RFID-based reverse logistics system, *Expert Systems with Applications* 36(5): 9299–9307. http://dx.doi.org/10.1016/j.eswa.2008.12.002

Limbourg, S.; Jourquin, B. 2009. Optimal rail-road container terminal locations on the European network, *Transportation Research Part E: Logistics and Transportation Review* 45(4): 551–563. http://dx.doi.org/10.1016/j.tre.2008.12.003

Macharis, C.; Van Hoeck, E.; Pekin, E.; Van Lier, T. 2010. A decision analysis framework for intermodal transport: comparing fuel price increases and the internalisation of external costs, *Transportation Research Part A: Policy and Practice* 44(7): 550–561. http://dx.doi.org/10.1016/j.tra.2010.04.006

Macharis, C.; Pekin, E. 2009. Assessing policy measures for the stimulation of intermodal transport: a GIS-based policy analysis, *Journal of Transport Geography* 17(6): 500–508. http://dx.doi.org/10.1016/j.jtrangeo.2008.10.004

Mikulėnas, G.; Butleris, R. 2010. An approach for constructing evaluation model of suitability assessment of agile methods using Analytic Hierarchy Process, *Elektronika ir Elektrotechnika – Electronics and Electrical Engineering* (10): 99–104.

Ngai, E. W. T.; Cheng, T. C. E.; Au, S.; Lai, K.-H. 2007. Mobile commerce integrated with RFID technology in a container depot, *Decision Support Systems* 43(1): 62–76. http://dx.doi.org/10.1016/j.dss.2005.05.006

Ohkubo, M.; Suzuki, K.; Kinoshita, S. 2003. Cryptographic approach to 'privacy-friendly' tags, in *RFID Privacy Workshop@MIT: November 15, 2003*. Available from Internet: http://rfidprivacy.media.mit.edu/2003/papers/ohkubo.pdf

Piramuthu, S. 2007. Protocols for RFID tag/reader authentication, *Decision Support Systems* 43(3): 897–914. http://dx.doi.org/10.1016/j.dss.2007.01.003

Saito, J.; Sakurai, K. 2005. Grouping proof for RFID tags, *Proceedings of the 19th International Conference on Advanced Information Networking and Applications* (AINA 2005). Vol. 2, 621–624. http://dx.doi.org/10.1109/AINA.2005.197

Sharmin, M.; Ahmed, S.; Ahamed, S. I. 2006. An adaptive lightweight trust reliant secure resource discovery for pervasive computing environments, in *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*. 13–17 March 2006, Milwaukee, WI, USA, 258–263. http://dx.doi.org/10.1109/PERCOM.2006.6

Thill, J.-C.; Lim, H. 2010. Intermodal containerized shipping in foreign trade and regional accessibility advantages, *Journal of Transport Geography* 18(4): 530–547. http://dx.doi.org/10.1016/j.jtrangeo.2010.03.010

Van Deursen, T.; Radomirović, S. 2009. Security of RFID Protocols – a case study, *Electronic Notes in Theoretical Computer Science* 244: 41–52. http://dx.doi.org/10.1016/j.entcs.2009.07.037

Wen, W. 2010. An intelligent traffic management expert system with RFID technology, *Expert Systems with Applications* 37(4): 3024–3035. http://dx.doi.org/10.1016/j.eswa.2009.09.030