Computer Technology and Application 2 (2011) 530-538

Fraud Detection in Interoperable Information Systems

Saša Mladenović[1], Marko Rosić[1] and Maja Štula[2]

1. Computer Science Department, Faculty of Science, University of Split, Split 21000, Croatia

2. Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Split 21000, Croatia

Received: May 20, 2011 / Accepted: June 09, 2011 / Published: July 25, 2011.

Abstract: Interoperability is broad and complex subject being the most critical issue facing businesses that need to access information from multiple systems. The concept of unwanted interoperability can result in fault decision making based on counterfeit data produced by hostile interoperable system. Research in this paper is based on highway toll collection system analysis as representative of hierarchical heterogeneous systems where integration becomes more important than development due to the short time in disposal between the contract signature and implementation. Unwanted interoperability detect mechanism is presented using information collected from different information system levels.

Key words: Unwanted interoperability, hierarchical system, toll collection, fraud.

1. Introduction

The global market is trying to improve their competitiveness. Collaboration among companies, supported by flawless communication between respective systems and applications is identified as key factor in company success in ever changing global environment, strengthening partnership and business on the market [1]. Cooperation and partnership motivates companies to look for interoperability solutions. Interoperability is important subject of discourse in the last decade, and it will become even more important with the proliferation of collaboration between companies.

The paper is organized into six sections. Section 2 outlines interoperability definitions and scenarios including unwanted interoperability. Section 3 reviews and combines hierarchical approach to system modeling with complexity science. Section 4 presents highway toll collection system used as a case study for this research. Section 5 describes multilevel multidimensional approach used to detect fraud in highway toll collection system. Section 6 presents short conclusion on fraud detection in respect to presented case study. Finally software agents and multi agent approach is foreseen as methodology to further improve fraud detection making the whole business environment more secure.

2. Interoperability

Numerous interoperability definitions (emerged from scientific papers, reports [2-3], standards and official government documents in different countries [4-5]) are presented inside technology adoption curve [6] shown in Fig. 1.

It is obvious that different users are showing interest

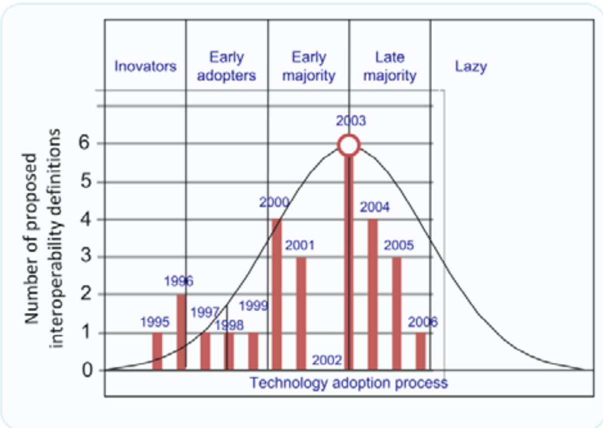

Fig. 1 Interoperability definitions adoption process.

Corresponding author: Saša Mladenović, Ph.D., research fields: artificial intelligence, toll collection system, knowledge management. E-mail: sasa.mladenovic@pmfst.hr.

for the interoperability field. That fact explains the increasing number of interoperability definitions. On the other hand decrease in definitions number is explained by reaching the maturity in the field.

From a pure technological point of view, interoperability is the ability of two or more information technology resources (hardware and/or communications devices or software components) to easily or automatically work together [7].

The Institute of Electrical and Electronics Engineers, (IEEE) Glossary defines interoperability as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [8].

Broadly speaking, interoperability is the ability of performing interoperation between two or more different entities (pieces of software, processes, systems, business units, etc.) [9]. The word “inter operate” implies that one performs operation for another system. If the system observed is a computer system than we can say that interoperability is the ability of two heterogeneous computer systems to function as one (together) and to give access to respective resources in reciprocal way. Once the set of systems has been identified, those systems can be modeled to evaluate the level of the interoperability that can be reached. Modeling heterogeneous computer systems is complex due to multilevel design of all but basic computer systems.

Although diverse factors have to be taken into consideration, if reaching the goal means achieving interoperability between two systems, then it is certain that success depends on the desired interoperability level and scenarios like depicted in Fig. 2.

Example Fig. 2a represents interoperability inside the same system. This is the simplest interoperability case since in the system itself most probably common procedures, knowledge, reasoning and environment can be found.

Fig. 2b represents interoperability between two non identical but known systems. Since systems are not

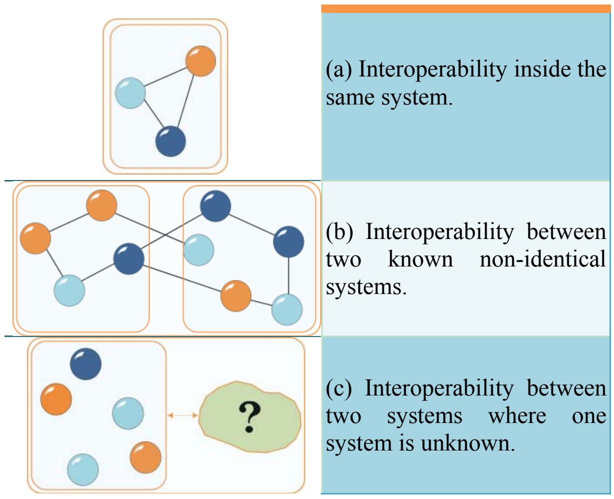

Fig. 2 Interoperability scenarios.

identical there is a concern that procedures and organization of two systems can be in confrontation. Communication subjects are supposed to be time invariant for the analysis purpose.

Case Fig. 2c differs from other cases described since one of the systems is unknown. This case describes the situation when one system is presenting information to anyone that needs it, but without prior agreement with other interested party.

Nature of the relationship established with the system can be collaborative or confrontational. We can differ between aggressive, passive, collaborative and cost focused systems [10]. Aggressive and passive systems are to be avoided in establishing the interoperability, therefore if the interoperability is established with such systems we will call it unwanted interoperability.

In an unwanted operational process one system tries to achieve advantage over the other system. Unwanted interoperability implies result based operations in which interoperability concentrates on the desired effects of the enemy system.

Let $S = \{s_1, s_2\}$ be a set of systems that have to achieve interoperability. Once the systems set S has been identified respective systems have to be modeled.

A system can be modeled using set of attributes $A=\{a_1, a_2, \ldots, a_n\}$ representing perspective and important features (size, shape, functions, element interfaces, etc.) of the system modeled.

Let interoperability mark describe what systems do to each other (i.e., two computers communicate, two firms trade, virus attacks). Than we can define system interoperability mark as a function which maps systems to a set of marks $A : S \rightarrow M$ where mark imply a interoperability type. An interoperability mark represents a pair (input, output) describing how systems achieve interoperability. Interoperability marks can be extracted from system description. It is to be noted that due to the fact that "s_1 interoperable with s_2" ≠ "s_2 interoperable with s_1 on the same level" interoperability marks are directional. Given a specific $s \in S$ and a set $a \subseteq A$ of system attributes describing s, then $c = a(s)$ is a chain of system states or instance of s, modeling s. To be able to compare two systems system instances have to be aligned with each other.

2. Complexity in System Modeling

As previously defined, system is made of any combination of interacting elements, which are themselves systems. Interacting elements can be people (person, group of people, organizations of people), intangible elements (methods, approaches, theories, software, processes, concepts, ideas), and tangible elements (computers, network devices, mechanical devices, sensors, vehicles) [11].

Element properties and interaction principles are not enough to deduce on properties of the whole system [12]. Additionally tendency exist to divide the science on "old" (appropriate for intrinsically simple systems), and the "new" complexity science [13]. One of "old science" properties is linearity. System is decomposed in elements and elements are analyzed. The system as a whole is defined as the sum of system elements. Most complex systems manifest both linearity and nonlinearity in composing subsystems. There are many definitions of complex system [14-15], but all agree that complex systems achieve missions, goals or functions through intricate interactions between elements. In such systems the whole is greater than the sum of the parts, not in metaphysical but in important objective sense, with system properties emerging.

Emergence refers to the arising of novel and coherent structures, patterns, and properties during the process of self-organization in complex systems. Emergent phenomena are conceptualized as occurring on the macro level, in contrast to the micro-level components and processes out of which they arise [16]. Fig. 3 shows a stack of lines assembled to form different structures. None of the parts (lines) has such property.

System model is representation of the real world and it is based on parts and relations between parts. Mathematical theory describing such system is called multilevel mathematical theory. Modeling method includes building of multidimensional elements bottom up from the lower level system elements set.

Discrete systems have (usually finite) sets of elements and (usually finite) sets of relationships between them. Relationships can be represented by networks in which the elements are represented by vertices and the relationships are represented by directed links.

A set can be any collection of objects, called objects' elements. Elements can be abstract or concrete. In this paper attention is restricted to finite sets, i.e., those sets whose elements can be counted from 1 to N, for some finite number N. A set X is well-defined if there is an operational procedure, P_x, for recognizing its elements.

The notation $P_x = True$ means that x passes the operational procedure P_x, in which case we say that x

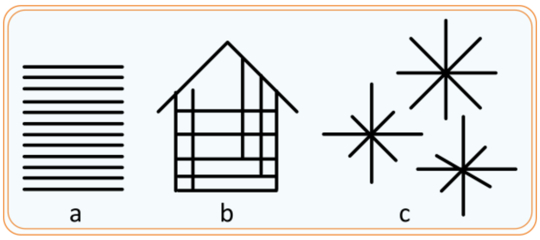

Fig. 3 Emergent properties of lines.

belongs to X. This is written: x belongs to the set X if x passes the operational procedure P_x $X = \{x| P_x(x)=True\}$. Each object can again be composed of parts.

Let P be the set of parts of an object W, then these parts have to be assembled into W under a relation R. We write $R : P \rightarrow W$ If P has two elements, x_1 *i* x_2 than we say that R is binary relation and we write $x_1 R x_2$, or $R(x_1, x_2)=True$. Generally, relation between n elements is called n-ary relation and denoted $R(x_1, x_2, \ldots, x_n)=True$. Although graphs and networks have powerful analytic power, there is essential disadvantage that they can represent only binary relations between pairs of things.

For example, consider three recognized parties in interoperability meeting, S_1, S_2 and S_3, agreeing on some subject in the interoperation process. This is not the same as they agreeing as three pairs having separate meetings. Thus, the combination $<S_1,S_2,S_3>$ is not the same as $<S_1,S_2>$ with $<S_1,S_3>$ with $<S_2,S_3>$, which can be written as $<S_1,S_2,S_3> \neq <S_1,S_2> + <S_1,S_3> + <S_2,S_3>$. Since $<S_1, S_2>$ is graphically represented by a line the natural generalization is to represent $<S_1, S_2, S_3>$ as a triangle, as illustrated in Fig. 4. The relationship of three parties having meeting together is a 3-ary relation, and this cannot be expressed in terms of 2-ary relation (binary relations).

Multidimensional polyhedra can be used as a mathematical representation of emergence (that is related with idea of multilevel systems), and therefore enable the definition of multilevel structure [17]. If vertices exists at one level then structures assembled from vertices, exist at a higher level. Thus the mapping from the set to the simplex moves up the hierarchy of representation from Level N to Level $N+1$. Fundamental diagram of multilevel systems is hierarchical cone presenting the assembly of vertices into a polyhedron. Euler circle (ellipse) as the base of the cone represents the set, and apex represents vertex and all together at a higher hierarchical level represent simplex. Assembly relation maps base set to a structure at a higher level in the representation (Fig. 5). Since the same set can be assembled in many different ways, the cone construction illustrates a many important options. Simplex is represented with set of vertices and relation that assembles vertices into structure. It's related notation is $<v_0, v_1, \ldots, v_n ; R>$.

In multilevel systems structures are aggregated in new structures existing on higher level. Aggregation can be done in multiple ways. Assembling elements are composed into construct defined by relation between elements. To define different aggregations type, definition of assembling elements set and construct composition is required, taking into account different aggregation types. Assembling elements set T is defined as set of all available parts containing at least parts needed for system (object) assembly $T \supseteq D$.

Aggregation where all assembling elements are needed for construct to exist on the higher level is called *AND* aggregation and we can write:

$\forall d_i \in D\ \exists R_O : R : D \rightarrow O = True,\ O = <d_1, d_2, \ldots, d_i\ R_o> : d_i \in D\ \forall i>0,\ T \equiv D$, R_o construct assembly relation. *AND* aggregation creates new structures or constructs.

Aggregation for which one assembling element is enough for construct to exist on higher level is called *OR* aggregation and we can write:

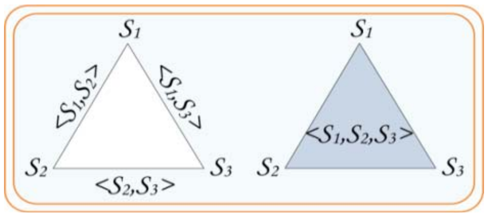

Fig. 4 Set of binary relations and ternary relation.

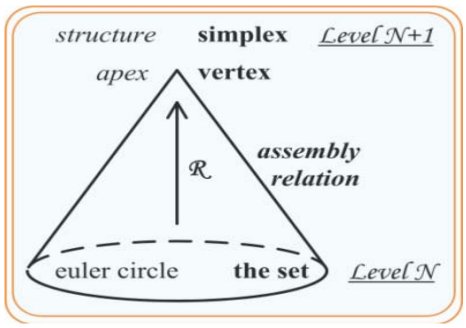

Fig. 5 Hierarchical cone.

$\forall d_i \in D\ \exists\ R_{O_i}: R: D \rightarrow O = True$, if there is at least one way to compose the object O.

When dealing with multilevel systems both aggregation types are expected to be used, therefore set of all possible solutions is defined as disjunction of conjunctions as depicted in Fig. 6 $O = \bigcup_i <d_1, d_2, \ldots, d_i; R_{O_i}> \ : \ d_i \in D\ \ \forall i>0,\ T\ \supseteq D,\ R_{O_i}$ assembly relation.

With introduction of different aggregations all prerequisites needed to model hierarchical heterogeneous systems that have to achieve interoperability are introduced. Highway toll collection system is representative of hierarchical heterogeneous system interoperating with other systems [18]. Since unwanted interoperability is the subject under consideration representative use case scenario has to be defined.

3. Highway Toll Collection System

Highway toll collection system (HTCS) is defined as a technology that allows electronic trace of toll payment regardless of payment method and user type. The goal of the system is to record the passage of a vehicle trough limited number of toll lanes, gate or plaza areas. HTCS relies on different technologies for vehicle identification, classification, positioning and authorization to determine if a vehicle is registered in a toll payment database. HTCS is composed of multiple system parts interacting together and creating a complex system. In countries like Croatia where highways are still in construction phase and number of toll stations and concessionaires are increasing [19], highway toll collection systems are evolving from manual trough stop-and-go to fast electronic toll collection system. Different technological solution to achieve required functionality can be used [20-22]. Technical solution depends on the required functionality. HTCS can be grouped based on payment method and service offered. Regarding equipment used on the toll lane we differ between automatic electronic toll collection (ETC) and manual

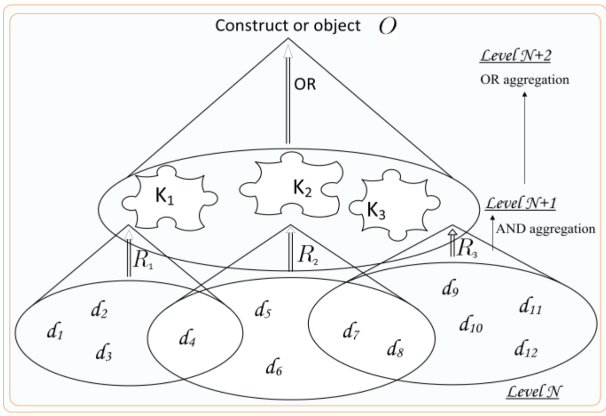

Fig. 6 Aggregations in multilevel system.

lane, while defining mixed lane as a combination of automatic and manual lane. In this way the architecture of the HTCS has been simplified. To understand better the automatic ETC implementation problem it is enough to point out the tourists charging problem. Tourists may possess on board unit (OBU), required for user identification, purchased from one highway authority. They expect OBU to be valid on all toll highways they can access, regardless the highway authority or country. Without interoperability it is not possible to use one OBU and drive trough highways operated by different toll operators. One option is to let visitors/tourists drive for free or to make them purchase vignette. Vignette system is the time-proportional lump sum system that becomes uneconomic and inefficient due to the rapid expansion of the motorway networks. The system is not suitable for operating, maintaining, and reconstructing. Travelers are dissatisfied with having to purchase vignettes valid for several hundred kilometers and often several days and weeks in order to travel just a section of the motorway, like recently observed in the case of Slovenia. For transit or tourist destination country, like Croatia, none of the proposed solutions is acceptable. Taking into account specific situation in Croatia, mixed toll collection system is used. When using manual toll collection part of the system, the operator is minimizing the risk of letting the driver pass trough without payment. However, since the HTCS is complex a new requirement like interoperability can cause new unwanted functionality to emerge, resulting in fraud. The proposed solution is to use information collected from different system levels to detect unwanted interoperability therefore detecting possible fraud. Unwanted interoperability occurs when an opponent system achieves interoperability with target system with intention to send faulty information or to prevent the target system to operate as designed. To be able to detect weak points in the system, system has to be described and then modeled. Most interesting process for highway operators is the exit lane level, payment process described in Fig. 7. Since payment is authorized by external entity three other points are sorted out as potential weak points (marked with target icon). During the vehicle detection there is a possibility to affect the process in a way to declare nonexistent vehicle. From the part/whole point of view, the declaration is part of the same system, done by the toll collector, therefore representing unwanted interoperability in the same system. This kind of unwanted interoperability is interesting during the system design and implementation but less after that. After vehicle detection it is necessary to classify the vehicle since the price list depends on the vehicle class. This process, as previous one recognizes the possibility for toll collector to declare the vehicle class. Again interoperability is realized between components of the same system. Finally, during the payment process price list for the vehicle class detected or declared is applied based on the entry point information. Entry point information is extracted from the information stored on the entry ticket.

Entry ticket can be physical (paper ticket) or electronic (OBU) with data encoded on it. Entry ticket usually contains data like: date and time when vehicle entered the road network, entry point identifier, additional data about the vehicle (vehicle class, numeric license plate, color, number of axles etc.), ticket issuer identifier, etc.

Only part of the data (entry point identifier and date and time) is usually used on the exit lane for during the payment process. To be able to process data from the physical or electronic entry ticket, exit lane has to be interoperable with the system producing it.

Without achieving the interoperability on the entry ticket level there is no possibility to base the toll on the distance traveled.

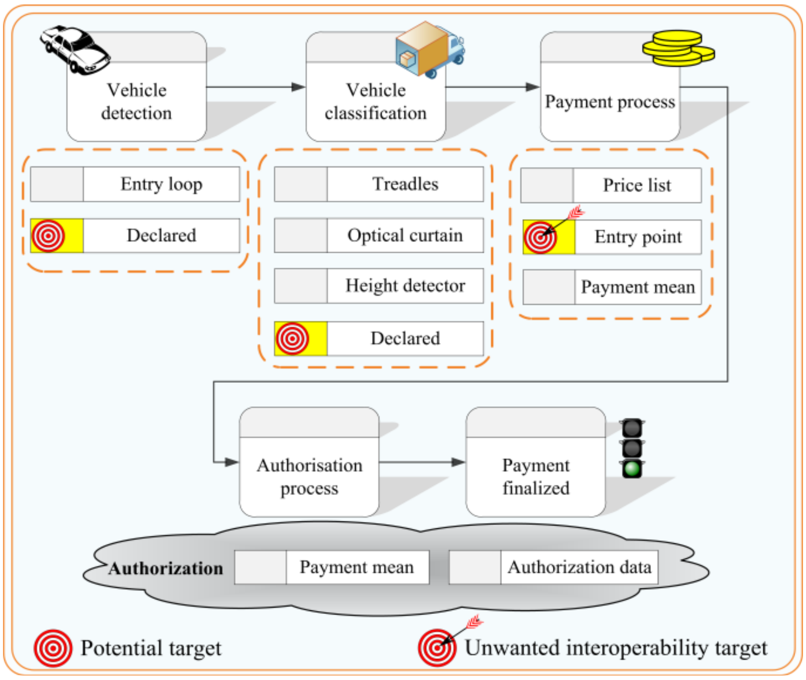

Fig. 7 Exit lane level payment process.

4. Fraud Detection

Entry ticket can be produced by known or unknown system. Known system is the one recognized as a friendly system; therefore the interoperability achieved is characterized as wanted. Unknown system can be anyone not registered as friend; therefore the interoperability achieved is characterized as unwanted. In our use case of highway toll collection system, interoperable entry ticket is produced by unknown enemy system. Regardless of the way and intention of the entry ticket production, our goal is to detect unwanted interoperability without changing the existing system. Hypothesis is that data arriving from different levels of the highway toll collection system can be used to detect the fraud caused by the emergence of unwanted interoperability. The HTCS is modeled respecting multilevel approach in Fig. 8. Elements depicted are for the illustration purpose only representing only parts of elements available on the respective level. The experiment consisted in analyzing information available to systems wanting to achieve interoperability with the HTCS. It is out of the scope of this paper to deal with security issues related to documentation availability.

Experiment consisted in production of multiple entry tickets on system defined as the one wanting to accomplish unwanted interoperability (enemy).

The ticket has been successfully processed on the unchanged exit lane. Successful processing of entry ticket produced by the enemy system is defined as fraud. Next step in the process was finding the counterfeited entry ticket by using multilevel approach. Simplest check was to compare information about number of vehicles entering the system per entry point, with number of vehicles exiting the system arriving from the same entry point (in the same time period). Number of vehicles per plazas is aggregated value existing on the level *N+1* and calculated based on the

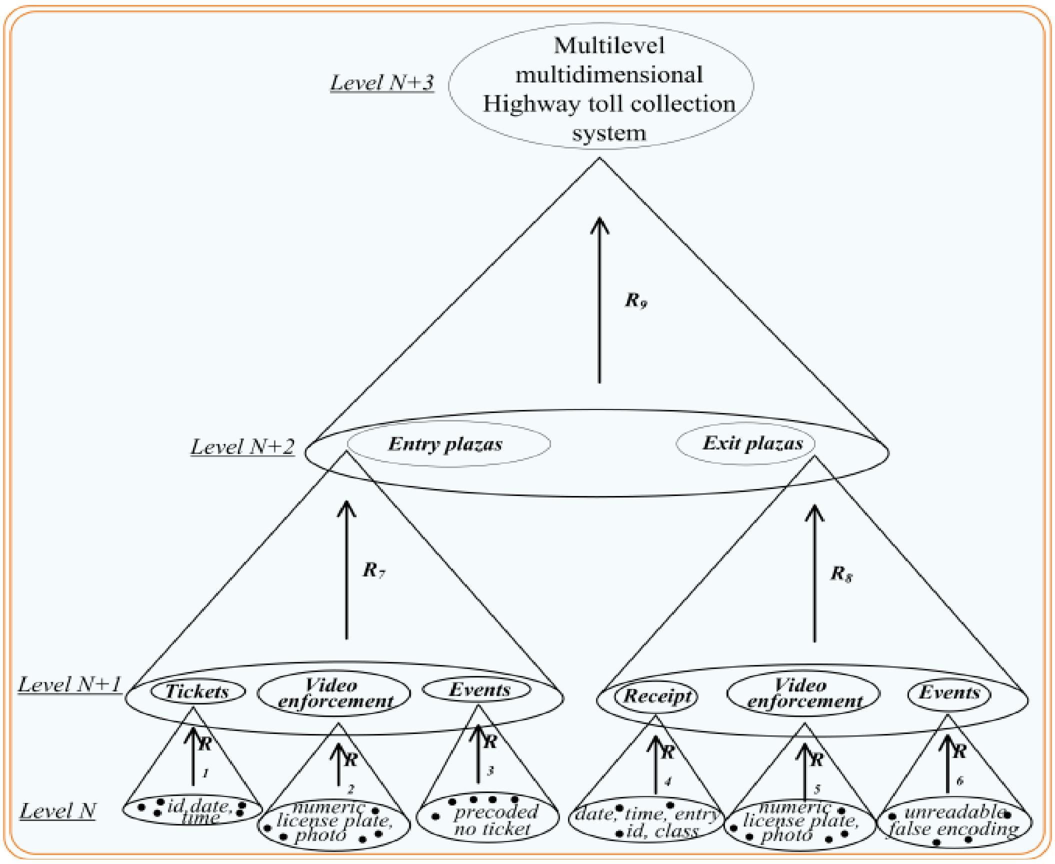

Fig. 8 Multilevel multidimensional HTCS.

values existing on the level *N*. Indication of potential unwanted interoperability was discrepancy in those numbers. Next step was to pair up entry ticket identifiers arriving from entry and exit plazas on the level *N+3*. For singleton entry tickets further investigation was required. If entry ticket identifier was part of the entry but not of exit plazas information set, for the system, it meant that vehicle never left the system. If on the contrary entry ticket identifier was part of the exit but not of entry plazas information set, for the system, it meant that vehicle never entered the system. If entry ticket identifier has been found in the respective information set multiple times, it meant that the same vehicle entered or exited the system multiple times. When some of the anomalies mentioned have been detected, further investigation was done by comparing photos taken for the respective entry ticket on entry and exit plaza. If photos taken were different it was concluded that unwanted interoperability has been detected.

Comparison of part of data available on different system levels is presented in Fig. 9.

Of course many more comparison rules may be defined to detect unwanted interoperability, depending on the system under consideration. Procedures on the lane level like checking the entry ticket consistency, numeric license plate comparison, maximum travel time and other procedures could be implemented. The goal was to show that even without additional restrictions unwanted interoperability can be detected.

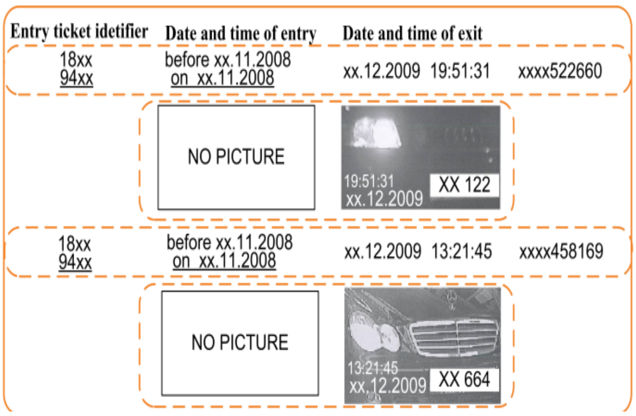

Fig. 9 Comparison of different system level data.

5. Conclusions

In the world with interconnection tendency in everyday life, it is to expect more requirements for interoperability between systems. Unwanted interoperability is a threat to all systems willing to interoperate. This research has shown that applying multilevel approach there is no need to restrict systems interoperability in order to defend it from intruders. During the design process by using multilevel modeling and complexity procedures to detect intruders can become part of implementation ensuring better protection against unwanted interoperability. In the HTCS use case, human agent has been used to detect unwanted interoperability resulting in fraud. However, software agents [23] and multi agent approach [24] can be used on top of existing hierarchical heterogeneous systems eliminating the need to spend considerable amount of time to detect potential fraud. Moreover by eliminating human factor systems can exchange information about procedures applied for fraud detection, making the whole business environment more secure.

References

[1] J. Greenfield, K. Short, Software factories: assembling applications with patterns, models, frameworks and tools, in: Companion of the 18th Annual ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages and Applications, ACM, 2003, pp. 16-27.

[2] E. Morris, L. Levine, C. Meyers, System of systems interoperability (SOSI): final report, Technical Report, Carnegie Mellon University, 2004.

[3] M. Kasunic, W. Anderson, Measuring systems interoperability: challenges and opportunities, Technical Note, Carnegie Mellon University, 2004.

[4] T.C. Ford, J.M. Colombi, S.R. Graham, D.R. Jacques, A survey on interoperability measurement, in: D.S. Alberts (Ed.), Adapting C2 to the 21st Century, 12th International Command and Control Research and Technology Symposium, Gateways, 2007, p. 3.

[5] V.R. Hrvatske, Uredba o informacijskom sustavu zaštite okoliša, Narodne Novine, Jun. 2008.

[6] E.M. Rogers, U.E. Medina, M.A. Rivera, C.J. Wiley, Complex adaptive systems and the diffusion of

innovations, The Public Sector Innovation Journal 10 (2005) 1-26.
[7] H. Lueders, Interoperability and Open Standards for eGovernment Services, in: Proc. of 1st Intern. Conf. on Interoperability of Enterprise Software-Applications, Switzerland, 2005.
[8] IEEE and I.O.E. & E. Engineers, IEEE Standard Computer Dictionary: a Compilation of IEEE Standard Computer Glossaries: 610, Inst of Elect & Electronic, 1991.
[9] F.B. Vernadat, Interoperable enterprise systems: principles, concepts, and methods, Annual Reviews in Control 31 (2007) 137-145.
[10] C. Verstraete, Partner Relationships: Confrontation, Collaboration, or Both? Stamford: Collaborative Product Development Associates, LCC, 2005.
[11] M. Couture, Complexity and chaos-State-of-the-art; overview of theoretical concepts, Technical Memorandum, DRDC Valcartier TM 2006-453, Canada: Minister of National Defence, 2007.
[12] H.A. Simon, The Sciences of the Artificial, 3rd ed., The MIT Press, 1996.
[13] W.R. Ashby, An Introduction to Cybernetics, Chapman & Hall London, 1956.
[14] H.A. Simon, The Sciences of the Artificial, 2nd ed., The MIT Press, Cambridge, Mass, 1981.
[15] J. Johnson, Can complexity help us better understand risk, Risk Management 8 (2006) 227-267.
[16] J. Goldstein, Emergence as a construct: history and issues, Emergence 1 (1999) 49-72.
[17] J. Johnson, Hypernetworks in the Science of Complex Systems, Imperial College Press, 2011, pp. 364-375.
[18] S. Mladenović, M. Štula, D. Stipaničev, Highway toll collection information system redesign, in: Proceedings of KOREMA, Automation in Transportation, Zagreb, Ploče, Hrvatska, Sarajevo, Bosna i Hercegovina, 2009, pp. 52-55.
[19] Z. Pribanić, G. Knežević, G. Šepuka, Road toll collection in the Republic of Croatia with a special emphasis on interoperability, in: ASECAP Study & Information Days, Pula, Croatia, 2006, pp. 336-346.
[20] L. Klein, Sensor Technologies and Data Requirements for ITS, Artech House, Boston, London, 2001.
[21] G. Hanaoka, T. Nishioka, Y. Zheng, H. Imai, An optimization of credit-based payment for electronic toll collection systems, IEICE Trans. Fundam Electron. Commun. Comput. Sci. E83-A (2000) 1681-1690.
[22] W.H. Lee, B.S. Jeng, S.S. Tseng, C.H. Wang, Electronic toll collection based on vehicle-positioning system techniques, in: IEEE International Conference on Networking, Sensing and Control, 2004, pp. 643-648.
[23] J.M. Bradshaw, Software Agents, MIT Press Cambridge, MA, USA, 1997.
[24] J. Ferber, Multi-Agent Systems: an Introduction to Distributed Artificial Intelligence, Addison-Wesley, 1999.