Multi-agent Platform for Security Level Evaluation of Information and Communication Services

Grzegorz Kołaczek

Institute of Informatics, Faculty of Computer Science and Management,
Wroclaw University of Technology,
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
Grzegorz.Kolaczek@pwr.wroc.pl

Abstract. The paper presents an original multi-agent approach to security level evaluation in service oriented systems for telecommunication sector, especially for providers of communication and information services. The platform is built from the following elements: user interface which has been used to select and configure the mode of operation of the analytical algorithms implemented within the platform; inter-modules interfaces which are used to supply the algorithms with appropriate datasets and to provide the user the results of analysis; analytical services which are responsible for security level evaluation and finally data repositories. The platform provides the security evaluation functionality as a web service according to Security as a Service (SaaS) model. This way of providing security assumes that the analytical methods are implemented independently from the evaluated objects and can be provided to any requesting subject as web services. The paper presents the architecture of the platform and the provided functionalities. Finally, the example scenario of the security level evaluation has been demonstrated and discussed. The presented platform for security level evaluation is an integral part of the comprehensive solution called PlaTel which has been designed for management and execution of information and communication services.

1 Introduction

The telecommunication market has always been 'service oriented'. This means that from early beginning changes in the telecom sector have been motivated by changes in an offered set of services (service-driven). To provide an end user high level quality services, telecom operator must for each service: design the architecture, define the cooperation between the existing components with the application of communication protocols, standardize the content and steering messages exchange. This way of providing new services is relevant to International Telecommunication Union (ITU) recommendation. ITU prepared the three step procedure for modeling telecommunication systems which includes: the description of provided for end user functionality, the architecture definition, the interdependencies and protocols definition [1,2,3].

The changes in telecom sector driven by changing technology and users expectation started in eighties. Then appeared the idea of *Intelligent Network* (IN) which was

N.T. Nguyen et al. (Eds.): *Adv. Methods for Comput. Collective Intelligence*, SCI 457, pp. 107–116.
DOI: 10.1007/978-3-642-34300-1_10

the first approach to programmable and reconfigurable telecommunication systems. The idea of IN has been extended by International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to iterative approach of Intelligent Network Conceptual Model (INCS). Although the growing number of implementations and wildly accepted standards the IN and INCS have not reached the expected level of interest. This motivated the next phase of changes in telecommunication systems in the nineties (Figure 1). Then several new application programming interfaces (API) for telecommunication systems have been developed, e.g. Parlay, 3rd Generation Partnership Project (3GPP), Open Service Architecture or Java API for Integrated Networks (JAIN). Finally, the simplified version of Parlay specification (Parlay/OSA – Parlay X) has been approved as the standard API for telecommunication services. The main assumption of Parlay X are as follows: service intelligence is separated from signalization, service intelligence can be moved outside the telecommunication network, the connection between a service logic and telecommunication network is defined by API. Additionally Parlay X uses the elements known from classic web systems such as Extensible Markup Language (XML), Universal Description, Discovery and Integration registry (UDDI), Web Services Description Language (WSDL) and Simple Object Access Protocol (SOAP) [4].

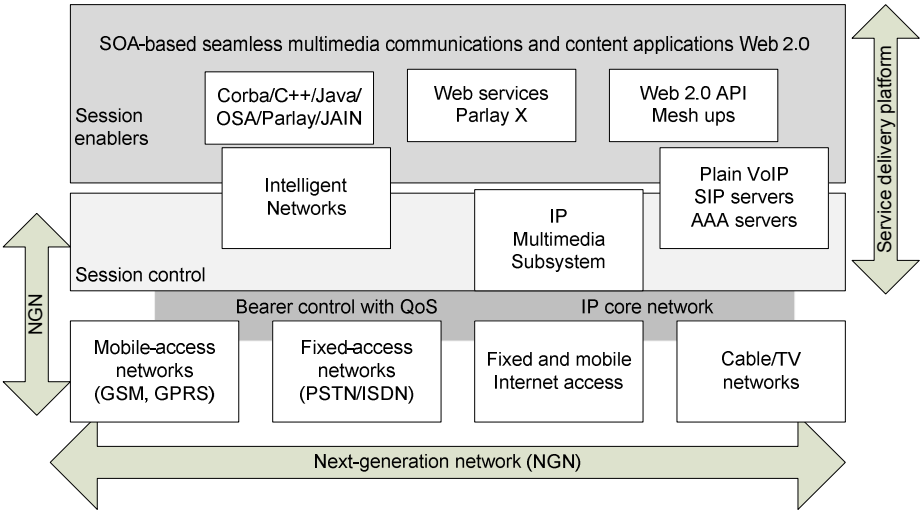

Fig. 1. Layered architecture of SOA-based ICT systems

Next section presents general overview of PlaTel – universal platform for management and execution of information and communication services. The third section describes the architecture and functionalities of security level evaluation module of PlaTel. This section is summarized by an example of practical application of the proposed framework in the task of security level evaluation in telecommunication systems. The last part of the paper contains conclusions and the further work.

2 Universal Platform for Management and Execution of Information and Communication Services

The universal platform for management and execution of information and communication services – PlaTel – has been developed to integrate several layers of abstraction on the way of providing intelligent communication and computational services. PlaTel offers complementary support in business processes management and execution for all type of users (e.g. telecomm services providers, end users or telecomm operators).

PlaTel has been developed in accordance with Service Oriented Architecture (SOA) paradigm. This means that PlaTel is a set of loosely coupled services constitute a set of basic functionalities provided as separate modules. There are a few basic modules which are responsible for: business process and organization modeling (PlaTel-O and PlaTel-P), service composition (PlaTel-U), mapping of communication-based requirements (PlaTel-K), execution environment management (Platel-R), security evaluation (PlaTel-W). Each of the modules may act independently using its own execution environment and input data. However, the maximum synergy can be achieved when all modules interact with each other. Combining several well know as well as originally developed methods of knowledge processing makes PlaTel an original collective intelligence tool for management and execution of information and communication services. In such case, the entire business process can be supported by PlaTel from the stage of the business process definition through the services composition, mapping them to the communication and computational resources and executing, till the evaluation of the final effect in terms of security and quality of services[5].

2.1 Security Problems and Security Level Evaluation of Communication and Information Services

PlaTel-W is a type of security monitor for the service-oriented systems which evaluates the level of security on the basis of detection of the anomalous patterns in network traffic or other characteristic values of the services available in the system [6]. In this paper we consider a service-oriented data exchange system. The generic system's architecture that is monitored with PlaTel-W has been depicted in Figure 2. It consists of services that have been composed (PlaTel-U) requested by user and which are intended to implemented a particular business process (PlaTel-P). After composition, the services are mapped on set of available services using the computational and communication requirements (PlaTel-K). Finally, services are executed (PlaTel-R). The execution of the services is monitored and all relevant data are collected in PlaTel repositories. Data from repositories are available for all PlaTel modules and allows for constant composition, mapping, execution, etc. improvement. PlaTel-W uses collected data to evaluate security level of the executed services and specially to find some anomalies in service execution which may be related to security breaches.

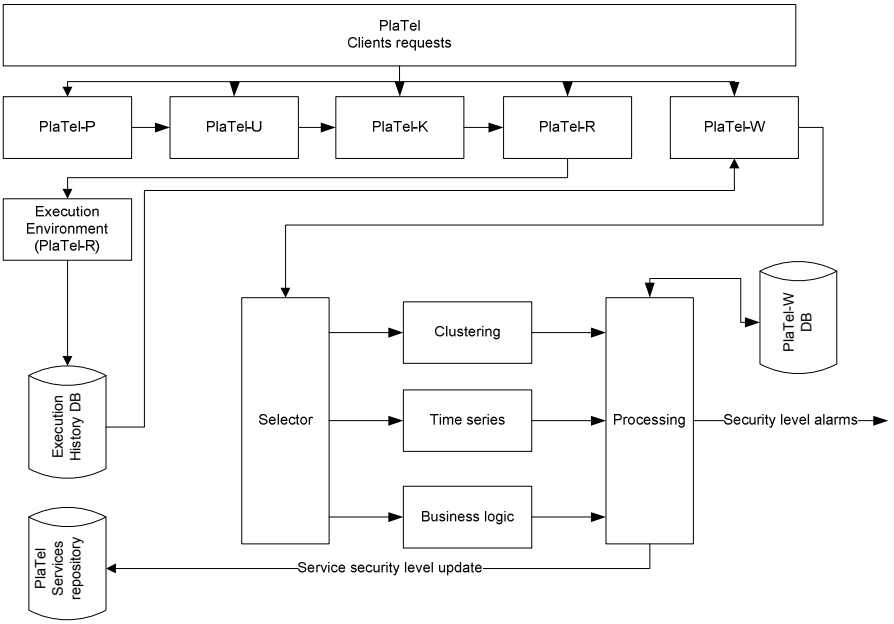

Fig. 2. Architecture of PlaTel-W

2.2 Functionality

The main components of PlaTel-W are responsible for analyzing the data provided by monitoring modules implemented by services execution environment (PlaTel-R). The analysis performed by PlaTel-W focuses on detection of anomalous events in service execution logs. There are three types of analysis performed which uses outlier detection, time series analysis and business logic abuses approach.

Outlier detection

The aim of outlier detection may be defined as the search for an observation which deviates so much from the other observations as to arouse suspicions that it was generated by a different mechanism [10]. This follows the general intuition which can be described by two following statements:

- Normal data object follow a "generating mechanism", e.g. some given statistical process
- Abnormal objects deviate from this generating mechanism

Outlier detection methods can be divided between univariate methods and multivariate methods that usually form most of the current body of research. Another fundamental taxonomy of outlier detection methods is between parametric (statistical) methods and nonparametric methods that are model-free. PlaTel-W implements a class of outlier detection methods which is founded on clustering techniques

(Expectation Maximization based method and Distance-Based Otliers Detection), where a cluster of small sizes or small densities, below the given threshold, can be considered as clustered outliers .

Time series analysis

The other method applied in PlaTel-W uses time series analysis approach to anomaly detection. The anomalous behavior of the systems is determined using the values for the behavioral attributes within a specific context. An observation might be an anomaly in a given context, but an identical data instance (in terms of behavioral attributes) could be considered normal in a different context. Contextual anomalies have been most commonly explored in time-series data [9][10]. One of the earliest works in time-series anomaly detection was proposed by Fox [12]. Some of the time series anomaly detection approaches uses basic regression based models [12]. Another variant is that detects anomalies in multivariate time-series data generated by an Autoregressive Moving Average (ARMA) [12]. Any observation is tested to be anomalous by comparing it with the covariance matrix of the autoregressive process. If the observation falls outside the modeled error for the process, it is declared to be an anomaly. An extension to this technique is made by using Support Vector Regression [13]. Another example of anomaly detection in time-series data has been proposed by Basu and Meckesheimer [12]. For a given instance in a time-series the authors compare the observed value to the median of the neighborhood values.

The implemented in PlaTel-W algorithm of anomaly detection in time series benefits from multidimensional approach presented by M.Burgess [8,9] This method can be applied to detect anomalies in various types of values measured describing the service execution. The only requirement is that the values must constitute time series (e.g. how many times in a given time window a service has been executed). The more details about the implemented method and the obtained results can be found in [7].

Business logic abuses

Apart from the typical security problems related to service oriented environments, one which is crucial for further evolution of service oriented systems is business logic abuse detection. Business logic abuse is the abuse of the legitimate business logic of a website or other function that allows interaction. Business logic abuse is usually aimed to exploit in some way the system that supports certain business logic e.g. by an illicit use of a legitimate website function.

Detection of business logic abuse is difficult because the offenders are using the same functionality as the legitimate users and therefore, their actions are likely intermixed with real actions. The other problem to overcome in the context of securing business logic is that the intruder is using a legitimate flow on a website or other application, so disabling that flow would influence also the interactions of legitimate users. This is why the new and versatile methods are required to support the service oriented systems with an appropriate services that could secure them from this type of risk.

3 Security Level Evaluation

Service-Oriented Architecture (SOA) defines that services are independent, self-contained modules, which do not store state from one request to another. As services should not depend on the context or state of other services, any state-dependencies are defined using business processes, and data models. Finally, service oriented systems implements some business logic using their ability to compose applications, processes, or more composite services from other less composite services. This activity, sometimes called service composition, allows developers to compose applications and processes using services from heterogeneous environments without regard to the details and differences of those environments. In this context, business logic abuses could be detected by finding some suspicious traces in a system's or/and services' behavior.

This section presents a statistical approach to represent observations of composite services execution. The spatial relationships which are often used as a synonymous with geographical distance between objects, in this case have been redefined as the logical distance between services composing services providing selected business logic functionality. This means that the distance between services is measured in the number of executed intermediate services on the way of providing user required business logic functionality. In normal (secure) situation, a composite service execution requires the constant number of atomic services to be executed to accomplish user request. When some problems with system security appear (e.g. malicious user password guessing, hacker's search for service vulnerabilities, denial of service attacks, etc.) the change in this characteristic is expected. This assumption has been used to model, estimate and describe spatial correlations among services and to detect business logic abuses.

3.1 Experiment Description

The aim of the experiment was to prove the possibility to detect the attack aimed at business process execution in service oriented systems. The business process abuse has been illustrated by abrupt change of data flow among services constituting composite service.

The composition plan defines the relations and expected directions of dataflow among services. The composite service presented in figure 3 assumes that the composite service execution starts by running service V1 and then the results of V1 execution are taken as input by services V2 and V3, the output of V2 is taken by services V4 and V5, etc. The composite service is completed when the service V8 returns the value. All services are executed in PlaTel-R environment and their execution is monitored by corresponding module. In this example, it has been assumed that the monitoring system collects the information about the byte counts of each service output. Because there is no good reference data from the real service oriented system the experiment uses some artificially generated datasets.

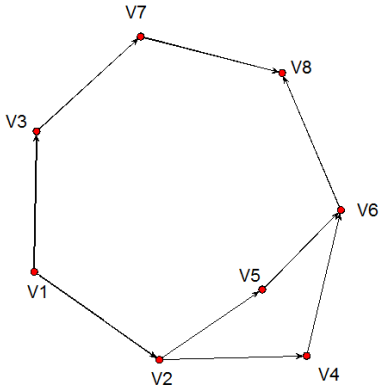

Fig. 3. Composite service execution plan

The four scenarios of composite service execution have been proposed and analyzed. The first scenario presents the situation where there is a strong correlation between the number of bytes at service input and output. It means that the number of bytes at service input determines the number of bytes at service output. The second scenario introduces some variability in relation between data quantity at input and output of services. It means that some randomly generated value reduces correlation between input and output. The third scenario presents how the results of the composite service execution analysis when there is no deterministic relation between data at input and output (it is rather unrealistic case). The last scenario shows the business logic abuse and how it influences the observable relations between services. The business logic abuse has been simulated in the fourth scenario by disrupting the correlation between input and output of the service V4. This scenario may illustrate the situation when intruder tries to execute some services out of planed order defined by the scheduled execution plan or tries to execute a service V4 using multiple and various input streams verify the service firmness.

3.2 The Spatial Analysis for Security Level Evaluation

The anomaly detection in composite service execution has been performed using some basic spatial analysis methods. The brief description of the performed steps is given below.

Moran-I test

It is the most common test for the existence of spatial autocorrelation. Moran coefficient calculates the ratio between the product of the variable of interest and its spatial lag, with the product of the variable of interest, adjusted for the spatial weights used.

$$I = \frac{n \sum_i^n \sum_j^n \omega_{ij}(x_i - \bar{x})(x_j - \bar{x})}{\sum_i^n \sum_j^n \omega_{ij} * \sum_i^n (x_i - \bar{x})^2} \quad (1)$$

Where x is the value of a variable for the ith observation, $\bar{x}$ is the mean of x and the ω_{ij} is the spatial weight of the connection between ith an jth node. Values range from -1 (dispersion) to +1 (correlation). A zero value indicates a random spatial pattern.

Local Moran test
A local Moran's test for the unit i can be constructed as one of the n components which comprise the global test:

$$I_i = \frac{(x_i - \bar{x}) \sum_j^n \omega_{ij}(x_j - \bar{x})}{\frac{\sum_i^n (x_i - \bar{x})^2}{n}} \quad (2)$$

As with global statistics, it is assumed that the global mean $\bar{x}$ is an adequate representation of the variable of interest. As before, local statistics can be tested for divergence from expected values, under assumptions of normality.

Spatial correlogram
Spatial autocorrelation measures the degree to which observations are correlated to itself in space. Spatial correlogram allows to tests and visualize whether the observed value of a variable at one location is independent of values of that variable at neighboring locations. Positive spatial autocorrelation indicates that similar values appear close to each other, or cluster, in space while negative spatial autocorrelation indicates that neighboring values are dissimilar or that similar values are dispersed. Null spatial autocorrelation indicates that the spatial pattern is random. In this research the correlogram of input/output flows of the corresponding network nodes has been investigated.

3.3 Results and Interpretation

This section presents the overview of the main results of the spatial analysis applied to composite services execution in service oriented systems.

Table 1. Moran-I test results

	Scenario			
	1	2	3	4
Moran I statistic	0.14108890	0.15279006	0.5028	-0.0201311
p-value	0.03310	0.02974	-0.14499871	0.2989
Expectation	-0.1428571	-0.14285714	-0.14285714	-0.1428571
Variance	0.02389195	0.02461018	0.09145791	0.05414065

The results presented in Table 1. shows that there is a positive spatial correlation in first and second scenario. It means that the correct execution of composite service shows the spatial correlations. Contrary scenarios 3 and 4 miss this type of correlation. Especially the scenario 4 demonstrates that spatial analysis can be used to detect security breaches in composite services execution and so also business logic abuses should be detected.

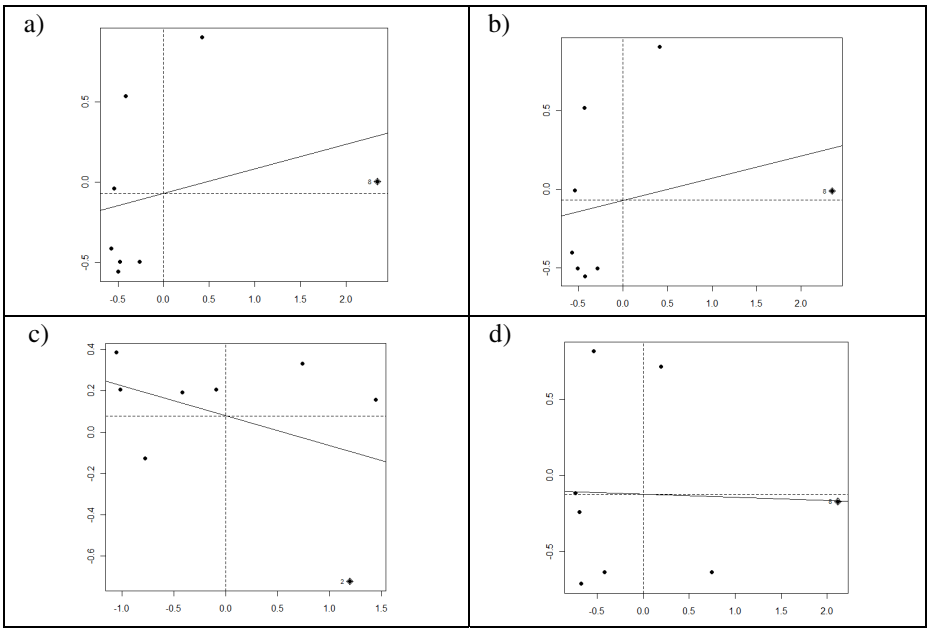

Fig. 4. Spatial correlograms

The results presented in Table 1 can be visualized as a spatial correlograms. Figure 4. presents a plot of spatial data against its spatially lagged values (axis X denotes standardized data flow volume, axis Y spatial lag). Each spatial correlogram is divided into 4 sections: Low Left (LL), Low Right (LR), High Left (HL) and High Right (HR). Points (services) located in LL and HR parts of the plot shows positive spatial correlation while points (services) form RL and HR show negative spatial correlation. The normal composite service execution is illustrated by charts fig 4.a and fig 4.b. The random services execution (no relations among services) is illustrated by chart fig 4.c. The change of the spatial correlation type is visible in chart 4.d. These results demonstrate that such form of visualization can be very helpful in business logic abuses detection.

4 Conclusions and Future Work

The paper presented an original approach to the analysis of composite service execution with the application of statistical spatial analysis methods. The proposed method is an integral element of PlaTel platform which has been designed for ICT users to support the task of service management, execution and monitoring in service oriented systems. The cooperation of all defined within PlaTel modules creates an extensive possibility to provide high quality security monitoring system. As an example application of PlaTel modules cooperation, the anomaly detection tasks has been

examined. The obtained results are very promising, so the further research in this field has been planned.

The further works are intended to apply spatial analysis to real world data and to extend the analysis with some additional methods to enable reliable classification of security events. The next steps will be focused on further integration among PlaTel modules, particularly the interesting task is integration of the security analysis with composition module (PlaTel-U and PlaTel-K). Information about detected abuses should be taken into account while the next compositions of services are performed.

References

1. Magedanz, T., Blum, N., Dutkowski, S.: Evaluation of SOA concepts in telecommunications, Berlin (2007)
2. Harris, T.: SOA in Telecom (2010)
3. Strategies for enabling new serwices, http://www.tmforum.org
4. FP7 Call 1 achievements in software and services (2011)
5. Bond, G., Cheung, E., Fikouras, I., Levenhsteyn, R.: Unified telecom and web services composition: problem definition and future directions. In: IPTCOM 2009 (2009)
6. Chandola, V., Benerjee, A., Kumar, V.: Anomaly Detection, A Survey (2007)
7. Kołaczek, G.: Multiagent Security Evaluation Framework for Service Oriented Architecture Systems. In: Velásquez, J.D., Ríos, S.A., Howlett, R.J., Jain, L.C. (eds.) KES 2009, Part I. LNCS (LNAI), vol. 5711, pp. 30–37. Springer, Heidelberg (2009)
8. Burgess, M.: An Approach to Understanding Policy Based on Autonomy and Voluntary Cooperation. In: Schönwälder, J., Serrat, J. (eds.) DSOM 2005. LNCS, vol. 3775, pp. 97–108. Springer, Heidelberg (2005)
9. Burgess, M.: Two Dimensional Time-Series for Anomaly Detection and Regulation in Adaptive Systems. In: Feridun, M., Kropf, P., Babin, G. (eds.) DSOM 2002. LNCS, vol. 2506, pp. 169–180. Springer, Heidelberg (2002)
10. Gorodetski, V.I., Karsayev, O., Khabalov, A., Kotenko, I., Popyack, L.J., Skormin, V.: Agent-Based Model of Computer Network Security System: A Case Study. In: Gorodetski, V.I., Skormin, V.A., Popyack, L.J. (eds.) MMM-ACNS 2001. LNCS, vol. 2052, pp. 39–50. Springer, Heidelberg (2001)
11. Hwang, K., Liu, H., Chen, Y.: Cooperative Anomaly and Intrusion Detection for Alert Correlation in Networked Computing Systems, Technical Report, USC Internet and Grid Computing Lab, TR 2004-16 (2004)
12. Lakhina, A., Crovella, M., Diot, C.: Characterization of Network-Wide Anomalies in Traffic Flows. Technical Report BUCS-2004-020, Boston University (2004), http://citeseer.ist.psu.edu/715839.html
13. Ammeller, D., Franch, X.: Service level agreement monitor (SALMon). In: 2008 7th International Conference on Composition-Based Software Systems, pp. 224–227 (2008)