Journal of Advances in Computer Research
Quarterly pISSN: 2345-606x eISSN: 2345-6078
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 6, No. 3, August 2015), Pages: 39-49
www.jacr.iausari.ac.ir

Evaluating Adaptability of SET Protocols Using Colored Petri Nets

Nesa Mohsenian * [1], **Homayun Motameni** [2], **Sajjad Jeddi Saravi** [3]

1) Sama technical and vocational training college, Islamic Azad University, Sari Branch, Sari, Iran
2) Department of Computer Engineering, Sari branch, Islamic Azad University, Sari, Iran
3) Sama technical and vocational training college, Islamic Azad University, Sari Branch, Sari, Iran

Mohsenian_n@yahoo.com; Motameni@iausari.ac.ir,Sajjad_Jeddisaravi@yahoo.com

Received: 2013/05/09; Accepted: 2014/09/16

Abstract

Secure Electronic Transaction (SET) protocol is an open protocol, which has the potential to emerge as a powerful tool in securing of electronic transactions. The quality of a design of an Ecommerce protocols has a great influence on achieving non-functional requirements (NFRs) to the system. An increasingly important non-functional attribute of complex software systems is adaptability. Software for adaptive software systems should be flexible enough to allow components to change their behaviors depending upon the environmental and stakeholders' changes and goals of the system. Evaluating adaptability at software to identify the weaknesses of the software and further to improve adaptability of their, are very important tasks. This paper presents a method based on the use of Colored Petri Nets for evaluating Adaptability in SET protocol. We try to see how we can apply the way formalize CPN in terms of quality attributes to evaluate some of them, on the SET protocol

Keywords: SET, Colored Petri Nets, CPN tools, non-functional parameters, Adaptability, Modeling, and Evaluating.

1. Introduction

With the development of Internet, Ecommerce is becoming a more and more important business form. SET (Secure electronic transaction) [1-3] protocol is proposed as a security protocol in Ecommerce that First proposed by Visa and MasterCard. Most security protocols are extremely simple if only their length is considered. Thus, security protocols are excellent candidates for rigorous formal analysis. They are critical components of distributed security, are very easy to express and very difficult to evaluate by hand [4]. SET protocol is currently the focus of attention into, people tried to study all aspects of SET protocol, in order to change its safety, adaptability, speed, complexity, and so there's enough [5].

While there are several NFRs, adaptability is a key requirement for evaluating systems. One definition of adaptability is adapting a software system to change in its environment. An adaptable software system can match changes in its environment. Adaptation is the change in a system to accommodate changes in its environment while adaptability is the ability of a system to make adaptation. [6]

One approach is to use protocol, design methodologies that lend them to formal method analysis. These models are described in [7-10].

Many security protocols in use or proposed for widespread use, such as Secure Electronic Transaction (SET), Internet Key Exchange (IKE), Secure Sockets Layer (SSL), and TLS, offer optional sub-protocols that are agreed upon by protocol participants during protocol execution. Wagner and Schneier [11] discovered a weakness of this type in the Secure Socket Layer (SSL) protocol. In order to fully analyze these protocols, interactions between the sub-protocols must be considered. Unfortunately, this makes the analysis difficult and costly.

Petri Nets are presented by Carl Adam Petri during his Ph.D. thesis that it's a graphical and formal tool to analyze systems and protocols. Colored Petri Nets (CP-Nets) [12] are suitable as a modeling technique to analyze and evaluate systems [13-15]. CP-Nets have already proven also suitable as a modeling technique for analysis of Ecommerce protocols [18-19]. Also in recent years, the methods which are suitable for the security electronic commerce protocols researched [20-22]. Yang and Xiaoyao in [16,17] modeling the ISI and RPC protocols by Colored Petri net (CPN). in [23,24] proposed a model for SET protocol by PN and CPN. Also the methods to evaluate non-functional parameters by CPN are proposed [25-28] and several measures for adaptability have been proposed [29-32]. But these methods of modeling protocols are not calculating the non-functional parameters in Ecommerce protocols.

In this paper proposed a technique for measuring adaptability in software systems. This technique is not restrictive and using for Ecommerce protocols. Besides the techniques, here the following properties are presented: In this work, the primary objective is the construction of a CPN-based model for the operation of the SET protocol. For this purpose, the CPN Tools is used to model this protocol and also is shown how to evaluate the adaptability of non-functional parameter in SET protocols. CPN Tools is a popular tool for modeling and analysis of colored Petri nets [33]. Based on the presented model, a formal verification of SET protocol can be proposed. We just model the purchase request in SET, and the whole model can be constructed similarly.

The paper is organized as follows. In Section 2, Ecommerce Security protocol is presented. In section 3 modeling the SET protocol using CP-Nets are performed in CPN tools. In Section 4 a method for model evaluating is proposed and calculates adaptability non-functional parameter by it. Finally in Section 5 we conclude the work and suggest future research.

2. Ecommerce Security Protocol

Electronic commerce is buying and selling of goods and services across the internet. Commercial activities over the internet have been growing in an exponential manner over the last few years. When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an Ecommerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities [34].

2.1 SET Protocol Overview

People today pay for online purchases by sending their credit card details to the merchant. A protocol such as SSL or TLS keeps the card details safe from eavesdroppers, but does nothing to protect merchants from dishonest customers or vice-versa. Secure Electronic Transactions (SET) addresses this situation by requiring cardholders and merchants to register before they may engage in transactions. By SET protocol, business and customers can construct different electronic commerce models on the Internet. Users can construct all electronic commerce transactions of business and customers by SET. Because of features and functions of SET, users can get security and verification on the network transactions [23].

Introduction The intent of SET is to address certain security issues related to three party payment mechanisms conducted over the Internet. In a typical SET transaction, there are two kinds of information. One set of information such as items being ordered is private between the customer and the merchant. The other set of information such as the customer’s credit card number is private between the customer and the bank. The information for the bank is encrypted using the bank’s public key while information for the merchant is encrypted using the merchant’s public key. Both of these sets of information are digitally signed [2]. SET, however, also allows for both of these sets of private information to be included in a single, digitally signed transaction by combining the two signatures [35]. SET relies on cryptography technologies such as public-key encryption and x.509 digital certificates to ensure message privacy, integrity, and authentication.

SET is a family of protocols. The five main ones are cardholder registration, merchant registration, purchase request, payment authorization, and payment capture. The cardholder shares the order information with the merchant but not with the payment gateway. He shares the payment information with the bank but not with the merchant. All parties are protected [3].

2.2 Security Protocol Analysis Using Colored Petri Nets

Introduced by Kurt Jensen, Colored Petri Nets (CPN) has been researched in information technology and computer science. Petri Nets in the graphical forms are like flowcharts and network diagrams, while in mathematical forms, they are like algebra and logic subjects [15]. CPN are suitable as a modeling technique to analyze and verify systems in different areas of science such as artificial intelligence, parallel processing system, control systems, and numerical analysis. CP-Nets have already proven also suitable as a modeling technique for analysis of Ecommerce protocols and security protocols [15]. CPN model is capable of analysis of large and complex systems. The model size problem, which obstructs the wide use of basic PN, can be solved by CPN. In Colored Petri Net, color refers to the type of data associated with tokens and is comparable to data type in programming languages. Each net place in a CPN has an associated color set, which constraints the number and color of tokens that may move along the arc [24]. The computer tool CPN tools is effective to support the analysis and simulation of CPN model. It provides means for verify the correctness of the system and simulate the synchronization. The CPN model can be drawing to evaluate the formal description of SET protocol.

3. Non-Functional Parameters

The quality of an architectural design of an Ecommerce protocols has a great influence on achieving non-functional requirements to the system. Thus, the verifying and evaluate of non-functional parameters could be achieved with more ability. This section shows how can apply the CPN in terms of quality attributes to evaluate some of them and presents a formula for evaluating non-functional parameters. Adaptability and Interoperability on the SET protocol, are the parameters, we will find quality attributes for them.

3.1 Adaptability Overview

In literature, adaptability is defined variously. For example, in ISO/IEC 9126-1 [36] the software adaptability has been defined as “the capability of the software product to be adapted for different specified environments without applying actions or means other than those provided for this purpose for the software considered".

As a conclusion, adaptability, related to software engineering, has many facets, including characteristics from both functional and non-functional quality attributes. The latter quality attributes (i.e. operational and development quality attributes) can be seen as architectural in nature. Consequently, adaptability can be considered as a characterization of qualitative property of maintainability of software architecture and it should be taken into account at architectural design phase of the software system. Furthermore, adaptability includes runtime requirements of the software system as well as changes in requirements of stakeholders' objectives [38].

3.2 Adaptability Metrics

Internal adaptability metrics indicate a set of attributes for predicting the impact the software product may have on the effort of the user who is trying to adapt the software product to different specified environments [37]. There are five adaptability dimensions addresses which are listed below with brief explanation:

Table 1. Adaptability metrics

Metric name	Measurement, formula and data element computations
Adaptability of data structures	· X=A/B · A=Number of data structures which are operable and has · no limitation after adaptation, confirmed in review · B=Total number of data structures requiring adaptation capability
Hardware environmental adaptability	· X=A/B · A=Number of implemented functions which are capable of achieving required results in specified multiple H/W environment as specified, confirmed in review · B=Total number of functions with H/W environment

	adaptation capability requirements
Organisational environment adaptability	· X=A/B · A=number of implemented functions which are capable of achieving required results in specified multiple organizational and business environment as specified, confirmed in review · B=Total number of functions with organizational environment adaptation capability requirements
Porting user friendliness	· X=A/B · A=Number of functions supporting ease-of-adaptation by user as specified, confirmed in review · B=Total number of functions with ease-to-adapt capability requirements
System software environmental adaptability	· X=A/B · A=Number of implemented functions which are capable of achieving required results in specified multiple system software environment as specified, confirmed in review · B=Total number of functions with system software environment adaptation capability requirements

3.3 SET Adaptability

SET's architecture has been designed to be adaptable to different business models and operational environments, such as support for cardholders without certificates.

SET certificates - The design of SET uses X.509 version 3 certificates to support public keys for signature and encryption. These certificates include a public key together with the authentication of that key [2].

Use of cardholder certificates - The cardholder's signature certificate provide authentication and integrity of information sent to the merchant and to the Payment Gateway. SET supports environments in which cardholder signature certificates are required, and also environments where cardholder certificates are optional. A payment card brand determines if its application of SET requires signature certificates or not [2].

Certificate required Environments - In environments where certificates are required, all messages that require authentication and integrity from the cardholder shall be signed with a signature authenticated by the cardholder certificate. There are protocol initiation requests that do not include such signatures, since no significant protocol failures would result from their abuse. All other messages are signed, and the recipients of these messages are assured receipt of the corresponding certificates by the protocol [2].

Non-certificate Support - When a cardholder does not have a signature certificate, no digital signature is generated. In place of the digital signature, the cardholder generates the hash of the data and inserts the hash into the digital envelope to ensure the integrity of its contents [2].

4. Modeling of SET Protocol Based On CPN

Ecommerce protocols are almost complexity and will become very difficult to model via complex model. Also the analysis of state space is hard. Therefore, there is need to discover a simple and easy to learn method by CP-Nets.

In this section, based on the analysis methods of security protocols using Colored Petri Nets, we present the modeling of SET protocols by using the CPN tools. In this work, just the CPN model of purchase request in SET protocol according to the figure 1 is derived and the whole model can be constructed similarly.

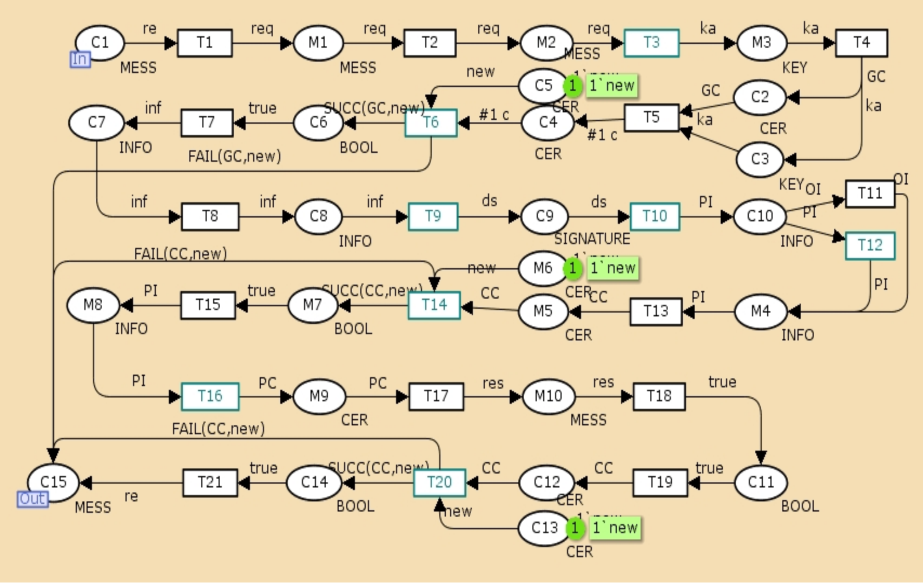


Figure 1. CPN Model of purchase request in SET protocol

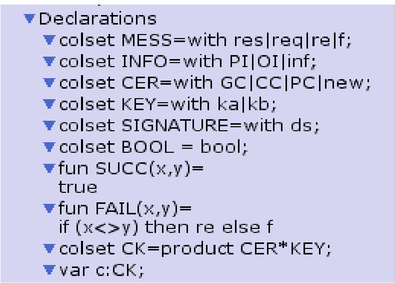
The places and transitions interpretation for Figure 1 is shown in table 1.

Table 2. Places and Transitions interpretation

SYMBOL	DESCRIPTION
T1	Cardholder software sends initiate request to merchant.
T2	Merchant software receives initiate request.
T3	Merchant software generates response and digitally signs it by generating a message digest of the response and encrypting it with the merchant private signature key.
T4	Merchant software sends response along with the merchant and payment gateway certificates to cardholder.
T5	Cardholder software receives initiate response and verifies certificates by traversing the trust chain to the root key.
T6	Cardholder software verifies merchant signature by decrypting it with the merchant public signature key and comparing the result with a newly generated message digest of the response.
T7	Cardholder software creates order information using information from shopping phase.
T8	Cardholder completes payment instructions.

T9	Cardholder software generates a dual signature by hashing a concatenation of the message digests of the OI and the PI and encrypting the resulting dual hash with the cardholder private signature key.
T10	Cardholder software encrypts PI with a randomly generated symmetric key (#1). This key, along with the cardholder's account information, is then encrypted with the payment gateway public key-exchange key.
T11	Cardholder software transmits OI.
T12	Cardholder software encrypted PI to the merchant.
T13	Merchant software verifies cardholder certificate by traversing the trust chain to the root key.
T14	Merchant software verifies cardholder dual signature on OI by decrypting it with the cardholder public signature key and comparing the result with a newly generated message digest of the concatenation of the message digests of the OI and the PI.
T15	Merchant processes request (including forwarding PI to the payment gateway for authorization).
T16	Merchant software creates purchase response including merchant signature certificate and digitally signs it by generating a message digest of the purchase response and encrypting it with the merchant private signature key.
T17	Merchant software transmits purchase response to cardholder.
T18	If transaction was authorized, merchant fulfills order to cardholder, (e.g., by shipping goods).
T19	Cardholder software verifies merchant signature certificate by traversing the trust chain to the root key.
T20	Cardholder software verifies merchant digital signature by decrypting it with the merchant public signature key and comparing the result with a newly generated message digest of the purchase response.
T21	Cardholder software stores purchase response.
M	MERCHANT COMPUTER
C	CARDHOLDER COMPUTER
P	PHASE

For the sake of simplicity, we just explain some parts in the model. There are ninety-three nodes in figure 1. These places are associated with the corresponding color set. In this model, several basic color sets are used for most places. The definition of these color sets are given below:



```
▼Declarations
  ▼colset MESS=with res|req|re|f;
  ▼colset INFO=with PI|OI|inf;
  ▼colset CER=with GC|CC|PC|new;
  ▼colset KEY=with ka|kb;
  ▼colset SIGNATURE=with ds;
  ▼colset BOOL = bool;
  ▼fun SUCC(x,y)=
   true
  ▼fun FAIL(x,y)=
   if (x<>y) then re else f
  ▼colset CK=product CER*KEY;
  ▼var c:CK;
```

Figure 2. Declarations of figure 1 model

The color set MESS including four types of message: response, request, message and failure message. The color set INFO explained transformed information and PI and OI. The color set CER including gateway certificates, cardholder certificate, merchant certificate and newly generated message digest. The color set key is private key and public key. The color set SIGNATURE describes the dual signature, and the color set SUCC and FAIL are result the processing.

5. Evaluating Security of SET protocol Based on CPN

This section explains the methodology that will be used in finding non-functional parameters. Here uses attach values to tokens for specify and evaluate various kinds of non-functional quality attributes.

For calculating non-functional parameters of the system we may define a success rate, f, for the transition in CPN. The token in the input of the transition T is assumed that carries the amount which stands for the accumulation of the success rate up to that place [39]. When transition fires the amounts which represent the success rate will be changed to f ´ N, because of transition success rate probabilities are independent of each other. For example the token has got a new probability of firing f ´ N instead of f. figure 4.4 shows the concept. In this figure, N is the data non-functional factor and f is the success rate. The initial value of f is equal to 1 and the final value of f same the security of system.

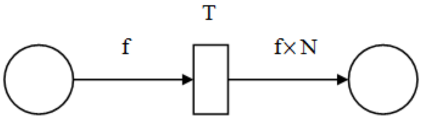


Figure 3: Calculation of Non-functional parameter

The Adaptability is calculated in the formula 1 through transition t. The Adaptability value results from the metrics according to ISP/IEC 9126 [38]. The Adaptability in any stage is the average of these values and Adaptability of the model is the product of all Adaptability in each transition. The values of a, b, c, d and e calculated based on table 1 formulas. The values should be given and normalized by the developer that evaluates the Adaptability.

$$A_i = \frac{1}{5}(a_i + b_i + c_i + d_i + e_i) \quad (1)$$

$$\text{Adaptabili ty} = \prod_{i=1}^{n} A_i$$

a: Adaptability of data structures
b: Hardware environmental adaptability
c: Organisational environment adaptability
d: Porting user friendliness
e: System software environmental adaptability
i: Number of active transitions

Because of SET protocol supported the adaptability metrics, so these parameters are approximately equal with 1. Due to the presence of adaptability functions in SET, this parameter is calculated in MATLAB software. Finally its value in SET protocol was obtained 99.74% that shows the high adaptability in this protocol.

Table 3. Result of adaptability evaluating

Transition	A
T1	1
T2	0.990
T3	1
T4	0.998
T5	0.999
T6	1
T7	0.994
T8	0.997
T9	1
T10	1
T11	1
T12	0.998
T13	0.996
T14	1
T15	0.999
T16	1
T17	0.990
T18	0.991
T19	1
T20	1
T21	0.995
Adaptability=99.74%	

6. Conclusion

Certificate authority, information coding and information integrality are three important parts in the Ecommerce. SET protocol is introduced to solve these problems and used widely as an industrial standard. This work is devoted to the formal specification and modeling of SET protocol by Colored Petri Nets. Based on the previous researches and works cannot evaluate the protocols in terms of non-functional parameters. But through the formalism of the colored Petri net, this operation is done and it was because in this paper used a formal modeling language to model an informal modeling language. Based on the proposed method, the whole formal specification and CPN model of SET protocol can be constructed sequentially. Then the non-functional parameters can be evaluated. Our results, shows the high adaptability parameters in SET protocol.

In the future, we would like to use this method to evaluate the other non-functional parameters in SET and other protocol and analogy them, also design a tools for evaluate all non-functional parameters.

References

[1] Mastercard & VISA, “SET Secure Electronic Transaction Specification; Book 1 : Business Description. May, 1997

[2] Mastercard & VISA, “SET Secure Electronic Transaction Specification; Book 2 : Formal Protocol Definition. May, 1997

[3] Mastercard & VISA “SET Secure Electronic Transaction Specification; Book 3 : Programmer’s Guide. May, 1997

[4] Pitt, M., “Modeling and verification of security protocols. Advanced seminar paper, “Dresden University of Technology, 2002

[5] Hu, Z., “The Study of E-Commerce Security Protocol, “International Conference on Intelligence Science and Information Engineering, PP. 349—352, 2011

[6] Subramanian N., Chung L., “Architecture-Driven Embedded Systems Adaptation for Supporting Vocabulary Evolution, “Proceedings of International Symposium on Principles of Software Evolution, November, Kanazawa, Japan, PP. 144--153. 3. Fenton NE, Software Metrics – A Rigorous Approach, Chapman & Hall, London, 1991

[7] Yang Xu., Wang, X., Xie, X., “A new electronic payment protocol and its formal analysis, “Computer Applications and Software, vol. 25, no. 9, PP. 93—95, 2008

[8] Heintze, N., Tygar, J., “A model for secure protocols and their compositions “Proceedings of the 1994 IEEE Symposium on Security and Privacy. IEEE Computer Society, Silver Spring, MD, 1994

[9] Yang, X., Xiaoyao, X.., “Extending Rubin logic for electronic commerce protocols, “in Proc. 2nd International Conference on Anti-counterfeiting, Security, and Identification, pp. 448—451, 2008

[10] Yang, X., Xiaoyao, X., “ Analysis of electronic commerce protocols based on extended Rubin logic, “in Proc. 9th International Conference for Young Computer Scientists, pp. 2079—2084, 2008

[11] Wagner, D., “Schneier, B.: Analysis of the SSL 3.0 Protocol In D, “Tygar Ed. USENIX Workshop on Electronic Commerce, PP. 29--40, USENIX Association, 1996

[12] Jensen, K., “Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use., “Volumes 1-3, Basic Concepts. Monographs in Theoretical Computer Science, Springer-Verlag, 1997

[13] Figueiredo, J. de, Kristensen, L., “Using coloured Petri nets to investigate behavioural and performance issues of TCP protocols, “ In Proc. 2nd Workshop on Practical Use of Coloured Petri Nets and Design/CPN, Aarhus, pp. 21—40, 1999

[14] Seifi, Y. Suriadi S., “Analysis of two authorization protocols using Colored Petri Nets “International Journal of Information Security, 2014

[15] Aly, S., Mustafa, K., “Protocol verification and analysis using colored Petri nets, “ Technical Report TR-04-003, DePaul University, 2003

[16] Yang, X., Xiaoyao, X., Huanguo, Z., “Modeling and Analysis of Electronic Commerce Protocols Using Colored Petri Nets, “JOURNAL OF SOFTWARE, VOL. 6, NO. 7, pp. 1181—1187, 2011

[17] Yang, X., Xiaoyao, X., “Modeling and analysis of security protocols using Colored Petri Nets, “Journal of Computers, vol. 6, no. 1, pp. 19—27, 2011

[18] Botao, L., Junzhou, L., “Modeling and analysis of non-repudiation protocols by using Petri Nets, “Journal of Computer Research and Development, vol. 42, no. 9, pp. 1571—1577, 2005

[19] Botao, L., Hong, Gu., “Analysis of fairness in payment protocols based on Hierarchical Timed Coloured Petri Nets, “ Journal of Electronics & Information Technology, vol. 31, no. 6,, pp. 1445—1450,2009

[20] Kleftouris, D.N., Maragos, N., Ziogou, C., Mouchos, Ch., “AN AGENT BASED APPROACH TO MODELING THE SECURE ELECTRONIC TRANSACTION PROTOCOL, “Proceedings of the International Conference on Theory and Applications of Mathematics and Informatics – ICTAMI 2003, pp. 205—218, 2003

[21] Desai, N., Garg, K., Misra, M., Bharadwaj, V., “Modeling Hierarchical Mobile Agent Security Protocol Using CP Nets, “Springer-Verlag Berlin Heidelberg 2007, pp. 637—649, 2007

[22] Ayanam, V. S., “SOFTWARE SECURITY VULNERABILITY VS SOFTWARE COUPLING A STUDY WITH EMPIRICAL EVIDENCE, “A Thesis Presented to The School of Computing and Software Engineering , 2009

[23] Wang, C., Wen, C. P., Hung, L., Chiang, D., “A Technique for Behavior Testing of SET Payment Based on Petri Nets, “Tamkang Journal of Science and Engineering, Vol. 3, No.2, pp. 117--121 , 2000

[24] YAN, Z., GAN, R., “Modeling of SET Protocol Based on UML and Colored Petri Net, “IEEE, pp. 124—129, 2001

[25] Motameni. H., Mozafari, M., Movaghar, A., “Evaluating UML State Diagrams Using Colored Petri Net, “SYNASC'05 , 2006

[26] Motameni. H., Movaghar, A., Kardel, B., “Verifying and Evaluating UML Activity Diagram by Converting to CPN, “Proc. of SYNASC'05 , 2005

[27] Motameni. H., Montazeri, H., Siasifar, M., Movaghar, A., Zandakbari, M., “Mapping State Diagram To Petri Net: An Approach To Use Markov Theory For Analyzing Non-Functional Parameters, “CISSE’06 Proceedings of 2th IEEE International Conferences on Computer, Information, and Systems Sciences, and Engineering, Bridgeport, USA, 2006

[28] Nematzadeh, H., Safaai, B.D., Maleki, H., Nematzadeh, Z., “Evaluating Reliability of System Sequence Diagram Using Fuzzy Petri Net, “International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, pp. 142—147, 2009

[29] Andresen, K, Gronau, N., “Criteria to Assess the Adaptability of Software Engineering Approaches, “IRMA International Conference, 2007

[30] Andresen, K., “Design and Use Patterns of Adaptability in Enterprise Systems, Gito, 2006

[31] Ak¸ Sit, M., Tekinerdo, G. B., Bergmans, L.: Achieving Adaptability through Separation and Composition of Concerns, “in M. Muhlhauser (ed.), Special Issues in Object-Oriented Programming, dpunkt, pp. 12—23, 1996

[32] Fenton, N., “Software Metrics – A Rigorous Approach, “Chapman & Hall, London, 1991

[33] Westergaard, M.: CPN Tools 4: Multi-formalism and Extensibility. Springer-Verlag Berlin Heidelberg, pp. 400–409, 2013

[34] David, J. Olkowski, Jr., “Information Security Issues in E-Commerce, “SANS GIAC Security Essentials , March 26, 2001

[35] Netsavvy Communications., “Enabling Technologies: Secure Electronic Transactions (SET), 1999

[36] ISO/IEC Std. 9126-1. Software engineering - product quality - part 1: Quality model. International Organization for Standardization / International Electrotechnical Commission, Tech. Rep. TR 9126-1:2001(E) , 2001

[37] ISO/IEC JTC1/SC7, Software engineering –Product quality – Part 3: Internal metrics, N2416R, ISO/IEC TR 9126-3, 2002

[38] Tarvainen, P., “Adaptability Evaluation at Software Architecture Level, “The Open Software Engineering Journal, 2, pp. 1—30, 2008

[39] Fukuzawa, K., Saeki, M., “Evaluating Software Architectures by Coloured Petri Nets, “SEKE’ Fourteenth International Conference on Software Engineering and Knowledge engineering, 2002