Evaluating of Data encryption metric in UML Sequence Diagram Using Fuzzy Petri Net

Mahnaz Hamzehniya, Mazandaran University of Science and Technology
Babol, Iran, mahnaz.hamzehnia@yahoo.com

Nasibeh Moosavi, Mazandaran University of Science and Technology
Babol, Iran, nasibeh.moosavi@ustmb.ac.ir

Maryam Musavi, Mazandaran University of Science and Technology
Babol, Iran, Maryam.musavi@ustmb.ac.ir

Homayoun Motameni, Islamic Azad University, Sari, Iran,
motameni@iausari.ac.ir

Name of the Presenter: Mahnaz Hamzehniya

Abstract

Although today UML is known as one of the most popular modeling languages, but this standard modeling language has some shortcomings such as being semi-formal and but lack of dynamism in modeling. In order to overcome this short coming, many efforts have been made to transform this language into formal methods including Petri nets. Fuzzy Petri net with strong mathematical support were suggested to increase the power of modeling and to show the uncertain data. In this paper, we transform the UML sequence diagram to fuzzy Petri net with an algorithm and then evaluate the security metric of data encryption in software systems. With evaluating these properties, developers can take step for indentifying shortcomings and improving them, so costs and potential losses reduced.

Key words: Data encryption, Fuzzy Petri net, Sequence diagram, Unified modeling language

1. Introduction

With the increasing complexity of software systems, the design issues become more apparent. So in the system design and total structure explanation, software architecture can be a solution to overcome these complexities [4][6]. Unified modeling language with different diagrams is one the major modeling and software development languages [5]. Sequence diagram is used to show these interactions and it models the order of system behavior. Emphasis in this diagram is the time and the order of message sending. However, lack of dynamism and semiformal feature of this standard language is a fundamental weakness in validation and non-functional parameters evaluation [3][14]. Therefore, formal languages such as Petri net with strong mathematical support introduced, can show the synchronous and concurrent
activities. Most of the real-world problems are occurred in an uncertain way then Fuzzy Petri nets were introduced to overcome this challenge which offers a tool for displaying unreliable data about the state of the system. Actually this is a way to increase the power of Petri nets modeling [14], [16].

Security is the ability of a software system to resist unwanted stuffs and to protect information and data against unauthorized efforts [6][16]. Security in ISO/IEC 9126 has metric such as system data encryption. We want to explore the security metric using Fuzzy Petri nets.

2. Background

1 Sequence Diagram

In object oriented systems the operational tasks are done through interaction of objects to exchange messages. Sequence diagram is used to show these interactions and Emphasis in this diagram is the time and the order of message sending. It makes the sequence of events for a particular operation. Parameters and control information can be put on each message [12].

2 Fuzzy Petri Net

Petri nets provide a powerful formal modeling method based on a solid mathematical structure while having graphical representation of system models as net diagrams. Petri nets are not capable of solving these uncertain and ambiguous problems. So a new tool called Fuzzy Petri net can be a very useful tool. Fuzzy Petri net is a combination of, Fuzzy set theory, with Petri net. And with the increasing needs to the industry to the Fuzzy Petri net, various types of this net has come to existence, such as Basic Fuzzy Petri net or Fuzzy Petri net [14], Fuzzy colored Petri net [9] and Adaptive Fuzzy Petri net [11].

A formal definition of fuzzy Petri net is made with 15-tuple (P, Ps, Pe, T, TF, TRTF, A, I, O, TT, TTF, AEF, PR, PPM, TV) [7], [8], [10], [14].

3. Related Work

If today many researchers try to convert this informal language to formal methods such as Petri nets. In [17] used the Theory of Markov to evaluate the non-functional parameters of a software system and then evaluated the performance characteristics of software such as security and reliability with generalized stochastic Petri net. In [19] an algorithm for sequence diagram mapping to Fuzzy Petri net suggested that we can perform the verification and validation of qualitative parameters of the system more accurately. In this study using the proposed approach, the qualitative reliability parameters were evaluated. In [1] made an algorithm to map the fuzzy UML sequence diagram to fuzzy Petri net, this formalization adds automatic processing ability to semiformal UML. In [2] the sequence diagram is converted to high level Fuzzy Petri net, but the parameters are not evaluated. In [16] the activity diagram is converted to fuzzy Petri net but the parameters are not evaluated. In [14] relation diagram is converted to fuzzy Petri net, but the parameters are not evaluated. In [20] activity diagram is converted to Fuzzy Petri net and it is used to evaluate reliability. UML state diagram shows the conditions or situation that may occur for an object and in [15] used an algorithm to convert state diagram to fuzzy Petri net. In [13] to model the dynamic behavior of the system, mapped UML collaboration diagram to fuzzy Petri net using an algorithm, but the parameters are not evaluated. In [18] to evaluate the Throughput of the system then an algorithm was proposed to map sequence diagram to Fuzzy Petri net.
4. Data Encryption
Security is the ability of a software system to resist unwanted stuffs and to protect information and data against unauthorized efforts. [6][21]. According to ISO/IEC 9126 model, data encryption means that implementation of data encryption is the extent for a software system can be completed.

\[ X = \frac{A}{B} \]  

(1)

A= Number of implemented instances of encryptable/decryptable data items as specified confirmed in review.
B= Number of data items requiring data encryption/decryption facility as in specifications.
0\leq X \leq 1  
the closer to 1, the more controllable

5. Proposed Algorithm
Because measure the capability of data encryption and converting a sequence diagram to fuzzy Petri net, in table 1 we provide the following mapping:

<table>
<thead>
<tr>
<th>Transfer of Sequence Diagram to Fuzzy Petri Net</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1.</strong> Extraction of the fuzzy rules for the data encryption metric</td>
</tr>
<tr>
<td><strong>Step 2.</strong> Calculation of fuzzy value for each variable</td>
</tr>
<tr>
<td><strong>Step 3.</strong> Calculation of the output value of the fuzzy rules</td>
</tr>
<tr>
<td><strong>Step 4.</strong> Conversion of fuzzy rules to fuzzy Petri net</td>
</tr>
<tr>
<td><strong>Step 5.</strong> Aggregate value of fuzzy rules</td>
</tr>
<tr>
<td><strong>Step 6.</strong> Defuzzification with the method of center of gravity for process</td>
</tr>
<tr>
<td><strong>Step 7.</strong> Calculation of average output of data encryption metric</td>
</tr>
</tbody>
</table>

Table 1. transfer of sequence diagram to fuzzy petri net

Fuzzy rules are as the following:

**M= Data encryption**
\[ X = \frac{A}{B} \]  

(2)

| \( R_1 \) = if \( X \) is \( e_1 \) then \( M \) is \( s_1 \) | \( R_2 \) = if \( X \) is \( e_2 \) then \( M \) is \( s_2 \) | \( R_3 \) = if \( X \) is \( e_3 \) then \( M \) is \( s_3 \) |
|------------------------------------------------|
| \( e_1=(0,0.1,0.2,0.3) \) | \( e_2=(0.2,0.3,0.4,0.5,0.6,0.7,0.8) \) | \( e_3=(0.7,0.8,0.9,1) \) |

Table 2. Fuzzy rules
**Fig 1:** Membership functions for Event of metric

<table>
<thead>
<tr>
<th>$S_1$ = (0, 0.1, 0.2, 0.3)</th>
<th>$S_2$ = (0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8)</th>
<th>$S_3$ = (0.7, 0.8, 0.9, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$ = Low</td>
<td>$S_2$ = Middle</td>
<td>$S_3$ = High</td>
</tr>
</tbody>
</table>

Table 2. Fuzzy rules

**Fig 2:** Membership functions for fuzzy variables

In this step we transform fuzzy rules to fuzzy Petri net.

**Fig 3:** Metric event in fuzzy Petri net

In this step we should apply the transitions to the events.

**Fig 4:** Applying fuzzy rules on the output of event

In this part aggregation should be applied, the output should be integrated to obtain a single output.

**Fig 5:** Output aggregation
The next step is defuzzification with the method of center of gravity and the fuzzy amount should be converted to a determined amount.

In defuzzification with the method of center of gravity, the fuzzy amount should be converted to a determined amount that is calculated with the following formula:

$$\text{COG} = \frac{\int_a^b \mu_A(x)xdx}{\int_a^b \mu_A(x)dx}$$  \hspace{1cm} (3)

The obtained number indicates the size of the metric. Taking the average of the numbers we can evaluate extent of data encryption in software system.

6. Case Study

To represent the application of our proposed Algorithm, in this section we consider an example of an activity diagram for ATM system.

In this study the ATM software has been examined. It has several parts but in this point only the bank user withdrawals will be examined in UML sequence diagram.

The outputs calculate according to fuzzy rules and the above said algorithm.
M= Data encryption
X = A/B

\[ R1 = \text{if } X \text{ is } e1 \text{ then } m4 \text{ is } s1 \]
\[ R2 = \text{if } X \text{ is } e2 \text{ then } m4 \text{ is } s2 \]
\[ R3 = \text{if } X \text{ is } e3 \text{ then } m4 \text{ is } s3 \]

\[ e1 = (0,0.1,0.2,0.3) \]
\[ e2 = (0.2,0.3,0.4,0.5,0.6,0.7,0.8) \]
\[ e3 = (0.7,0.8,0.9,1) \]

\[ S1 = (0,0.1,0.2,0.3) \]
\[ S2 = (0.2,0.3,0.4,0.5,0.6,0.7,0.8) \]
\[ S3 = (0.7,0.8,0.9,1) \]

Table 3. Fuzzy rules

\[ S1=\text{Low} \quad S2=\text{Middle} \quad S3=\text{High} \]
\[ \text{Low}=(0,0.1), \quad \text{Middle}=(0.2,0.3,0.4,0.5,0.6), \]
\[ \text{High}=(0.7,0.8,0.9,1) \]

\[ \mu(x=e1)=0, \mu(x=e2)=0, \mu(x=e3)=1 \]
\[ \mu(m=s1)=0, \mu(m=s2)=0, \mu(m=s3)=1 \]

Data encryption 1=1

\[ \mu(x=e1)=0, \mu(x=e2)=0, \mu(x=e3)=0.98 \]
\[ \mu(m=s1)=0, \mu(m=s2)=0, \mu(m=s3)=0.98 \]

Data encryption 2=0.986

Then Data encryption calculates the same for the rest of the sequence diagram.

\[ \mu(x=e1)=0, \mu(x=e2)=0, \mu(x=e3)=0.99 \]
\[ \mu(m=s1)=0, \mu(m=s2)=0, \mu(m=s3)=0.99 \]

Table 4. Fuzzy rules

\[ \text{Data Encryption} = \frac{1+0.986+0.99+0.975+0.996+0.96+0.986}{7} = 0.985 \]

Data Encryption Metric

<table>
<thead>
<tr>
<th>Withdrawals Steps of ATM</th>
<th>Result</th>
</tr>
</thead>
</table>

Final access controllability is 0.99

Final access controllability was obtained from the average of the results. Table 1 show the result of Access controllability in each section.
### Evaluation of Data Encryption Metrics in ATM

<table>
<thead>
<tr>
<th>Operation</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert Card</td>
<td>1</td>
</tr>
<tr>
<td>Card Check</td>
<td>0.985</td>
</tr>
<tr>
<td>Insert Password</td>
<td>0.99</td>
</tr>
<tr>
<td>Password Check</td>
<td>0.976</td>
</tr>
<tr>
<td>Select Withdrawals Operation</td>
<td>0.996</td>
</tr>
<tr>
<td>Select Amount</td>
<td>0.96</td>
</tr>
<tr>
<td>Cash Check</td>
<td>0.986</td>
</tr>
<tr>
<td><strong>Final Result</strong></td>
<td><strong>0.99</strong></td>
</tr>
</tbody>
</table>

Table 5: Evaluation of data encryption metrics in ATM

#### 7. Discussion on Result

The operations of this software vary for different users, so it was reviewed the sequence diagram of withdrawal by users using the suggested method and it was observed that system data encryption metric in this part is almost 0.99. If it wants to express the percentage, 99 percent of this part of the system in withdrawal by user is secure in terms of data encryption metric. The final result of sequence diagram depends on the result of each section. Because the final result is the average, thus for higher data encryption, the developer of system should create each section of system with higher data encryption. In RUP these kinds of shortcomings will be solved during different iterations.

Figure 9 show Fuzzy Petri net for data encryption metric in ATM system

![Fuzzy Petri net](image)

**Figure 8:** show Fuzzy Petri net for data encryption in ATM system

#### 8. Conclusion

Fuzzy Petri Nets were introduced to offers a tool for displaying unreliable data about the state of the system. Actually this is a way to increase the power of Petri nets modeling. Our goal in
this paper is the mapping of sequence diagrams in UML to fuzzy Petri nets in order to evaluate the data encryption metric so that the developers ensure the safety of them prior to implementation of vital systems. In future study we want to evaluate other UML behavioral diagrams and other qualitative parameters in ISO/IEC 9126 model using different Petri nets.

References


Booch, G et al. (2005). The unified modeling language user guide. Published by Addison Wesley, Second edition, USA.


Medvidovic, N et al. (2002). Modeling software architectures in the Unified Modeling Language. ACM Transactions on Software Engineering and Methodology (TOSEM), vol. 11, pp. 2-57, USA.


