Uncertainty Analysis of Attacker - Defender Interactions in MANET Based on Game GSPN with Intuitionistic Fuzzy Parameters

Guțuleac Emilian, Gîrleanu Ion, Iavorschi Inga, Furtuna Andrei

Technical University of Moldova
168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova
Tel: +37322509915, e-mail: emgutul@yahoo.com

ABSTRACT

This paper presents a comprehensive approach to model an expected attacker- defender interaction in a mobile Ad-hoc wireless network (MANET), which combines utilization of theoretical games methods, intuitionistic fuzzy logic and generalized stochastic Petri nets (GSPN), under which it is carried out the security modeling and QoS analysis of MANET with uncertain parameters due to uncontrollable factors. The validity of the proposed model is illustrated by an example with triangular fuzzy intuitionistic numbers using (α, β)- cuts analysis to show how it can be applied to the proposed approach, which better represents both dimensions of uncertainty, stochastic variability and inaccuracy in the shaping of this type systems. To demonstrate the usability of the method in different threat environments, an illustrative example with triangular intuitionistic fuzzy numbers is provided.

Keywords: game, theoretic, approach, intuitionistic, fuzzy, parameter, probability, mobile, ad-hoc, stochastic, Petri, nets, attacker, defender, interaction.

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are becoming very attractive and useful in many kinds of communication and networking applications [10, 17, 19, 23]. This is due to their efficiency, relatively low cost, and flexibility provided by their dynamic infrastructure. MANET is a self-organizing computer networks, formed by the cooperation of mobile computer devices, called nodes, that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the MANET topology may change rapidly and unpredictably over time. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes itself. i.e., routing functionality will be incorporated into mobile nodes [19]. However, because of the special characteristics such as wireless communication medium, lack of any infrastructure and mobility of the network nodes, the MANETs are prone to various passive and active security attacks which may be launched by the insider or outsider attackers [4, 17].

An appropriate model of attacker – defender behavior interactions is a key requirement for quantitative security evaluation of MANET nodes. In this context, there is a necessity of describing node's behavior and evaluate the dependability behaviors which is the capacity of a MANET node to complete its mission, in a defined time frame, in the presence of failures and security attacks.

The security community can benefit from the mature dependability modeling techniques, which can provide the operational measures that are so desirable today. On the other hand, by adding hostile actions to the set of possible fault sources, the dependability community will be able to make more realistic models than the ones that are currently in use [4, 7, 11, 14, 16].

Traditional methods for modeling and evaluating the MANET's QoS, nodes parameters and safety behavior are failures tree, attack tree and theoretical game [3, 9, 12, 15, 21, 24]. However, such methods focus upon evaluation of static behaviors of the net while ignoring the dependencies of events or time aspects of failures and attacks. Thus these methods cannot be used to predict in details the behavior of MANET nodes and particularly for real intentional attacks scenarios. Model-based vulnerability analysis of MANET nodes, checks the security properties via state-space exploration is more suitable for accurately describing the states during the operation of protocol and quantitatively analyzing the vulnerability. Automated computational analyses are commonly used in model-based vulnerability analysis of protocol, because this behavior can be translated into the identifiable type model using formal language. Due to the advantage of quick construction and numerical analysis, analytical modeling techniques, such as continuous time Markov chains (CTMC) and generalized stochastic Petri nets (GSPN) [3, 16, 22, 23, 25], have been used for performance analysis of communication, computer and industrial systems [7, 11, 16]. In addition, analytical modeling is a less costly and more efficient method. It generally provides the best insight into the effects of various parameters and their interactions. Hence, analytical modeling is the method of choice for a fast and cost effective evaluation of MANET.

As a combination, the stochastic game-based methods with GSPN contain the advantages of both stochastic model and game theory [12, 13]. Based on the GSPN model, game theory can be introduced to correctly model intentional attacks upon a system and the attacker strategies are regarded as part of the set of transition probabilities between the states [9, 21, 27]. There are increasing numbers of researches involving vulnerability analysis based on stochastic game [21, 27].

These traditional methods, like probabilistic models CTMC and GSPN [7, 11, 14, 23], for quantitative QoS analyze uses data from component parameters (component's failures and repairing rates, security attack rates and defense rates, etc.) which are known with a certain precision and validated via real experiments. However, unfortunately only experiments are not enough for validating with high precision failures parameters, vulnerabilities, and attacks. In addition, because the structure changes dynamically our knowledge about a potential successful attack is minimized. Thus, in order to elaborate adequate security mechanisms, it is necessary to elaborate new approaches in order to understand and describe wireless nodes behavior, to be capable of analyzing their vulnerabilities and estimate quantitatively their QoS parameters.

The classical QoS evaluation methods assume that accurate data is available to determine the best alternatives among the available options. However, in practice, due to the inherent uncertainty and impression of the available data, it is often impossible to obtain accurate information. Therefore, quantitative QoS evaluation under fuzzy environment problem is an interesting research topic, which had received more and more attention from researchers during the last several years.

In order to describe more accurately the expected behavior of attackers interactions with defense of MANET nodes, in this paper it is presented a new approach for modeling and evaluating the quantitative QoS which combines the utilization of theoretical stochastic games method, intuitionistic fuzzy logic [2] and GSPN that extends the work of [12, 13]. Combining these paradigms a new class of GSPN with stochastic games and intuitionistic fuzzy firing rates of timed transitions is defined, called IFGSPN. The advantage of combining these approaches is that IFGSPN models describe in a more realistic way the expected behavior of attackers, the behavior of the security system and dependability being taken into account. Also, the time aspect and intuitionistic fuzzy parameters are introduced in this paper for characterizing the success probabilities of attacker's actions, which most often are ignored. In addition, these models allow to evaluate some QoS parameters and can help to estimate expected losses, associated with different attack and defense strategies. In this context a numerical example is examined to demonstrate the applicability of the IFGSPN approach proposed in this paper.

To our knowledge, there is no analytical uncertainty analysis of attacker-defender interactions in MANET nodes in terms of the end-to-end delay and throughput on game GSPN with fuzzy intuitionistic parameters.

2. ELEMENTS OF STOCHASTIC GAMES THEORY AND INTUITIONISTIC FUZZY LOGIC

To facilitate the description of this work, here we are to introduce first some relevant basic preliminaries, concepts of stochastic game theory (SGT) and intuitionistic fuzzy sets [2].

Basic concepts of SGT. Game theory is the way to handle the problems where multiple conflicting interests' situation exists. In MANET the interactions between the attacker and the defender is taken as two players. So the SGT provides a range of instruments that can be efficiently used for modeling the interaction between independent nodes and intruders in a MANET [21, 27]. In a theoretical stochastic game, players are independent decision factors; their gain depends on other player's actions. In a MANET, nodes have the same behavioral characteristics. This similarity leads to a tight mapping between components of traditional SGT and elements of this network type.

Based on the IFGSPN model we built before and afterwards we introduce stochastic game using the immediate transitions in order to create a generic and sound framework for computing the expected malicious behaviors of attackers. As a consequence, we decide to take advantage of the SGT

mentioned in [12, 21] as a mathematical tool. We regard each malicious action, which may cause a transition of the current behavior of MANET node, as an action in a game where the attacker's choices of action are based on consideration of the possible consequences. The interactions between the attacker and the security system itself can then be modeled as a current stochastic game associated with the immediate transitions what they are in conflict in IFGSPN model.

This stochastic game, in the context of security analysis, is usually regarded as a two-player, zero-sum, multistage game where, at each stage, the parameters of the game depend on the current state of the IFGSPN mentioned above. Instantly after a MANET node is attacked, the intruder, after analyzing the vulnerability, seldom has the possibility to select between multiple atomic attack actions. An attack action can be considered successful if these actions produce an undesired transformation to the current system state of MANET node. Considering player *A* (the intruder) with a multitude of actions *A*={ $a_1, a_2, ..., a_m$ } and player *D* (the defense) with a multitude of actions *D*={ $d_1, d_2, ..., d_n$ }, the defense system has as its mixed strategy the probabilistic vector $\vec{q}^2 = (q_1^2, q_2^2, ..., q_n^2)$. Considering the reward matrix $\hat{\rho} = (\rho_{i,j})$, *i*=1, 2,…, *m*, *j*=1, 2, …, *n*, where $\rho_{i,j}$ represents the gain of player *A* in case he uses the action a_i, and player *D* uses the action d_j. In this paper, we will use a matrix game where a Nash's equilibrium exists and players use mixed strategies [5].

Intuitionistic fuzzy sets (IFS). The theory of fuzzy sets and fuzzy numbers concepts [2, 6] are used because there is a need to quantitatively show imprecise values, where the range of values that is taken by the membership function is not limited by two values, but is extended to the entire range [0,1]. The grade of membership of an element in a fuzzy set is represented by the real value between 0 and l. It does indicate evidence for this element but does not indicate evidence against it. The fuzzy set was extended to develop the IFS [9, 11] by adding an additional *non-membership* degree and degree of *hesitancy*, which may express more abundant and flexible information as compared with the fuzzy set [2]. This degree of hesitancy is nothing but the uncertainty in taking a decision by a decision maker.

Fuzzy numbers are a special case of fuzzy sets and their importance is for more real applications [1, 2, 6]. As a generalization of fuzzy numbers, an intuitionistic fuzzy numbers (IFN) seems to suitably describe an ill-known quantity [2]. Here we are to introduce first some relevant basic preliminaries, notations and definitions of IFS and IFN.

Let a non-fuzzy universal set X be fixed. An IFS A in X is defined as object of the following form $A = \{(x, \mu_A(x), \nu_A(x)) : x \in X\}$, where $\mu_A(x) : X \to [0, 1]$ and $\nu_A(x) : X \to [0, 1]$ define the degree of *membership* and the degree of *non-membership* of the element $x \in X$ respectively and for every $x \in X$, $0 \le \mu_A(x) + \nu_A(x) \le 1$[??]. The value of $\eta_A(x) = 1 - \mu_A(x) - \nu_A(x)$ is called the degree of *non-determinacy* (or *uncertainty*) of the element $x \in X$ to the intuitionistic fuzzy set A. Obviously, $0 \le \eta_A(x) \le 1$. When $\eta_A(x) = 0$, then an intuitionistic fuzzy set becomes fuzzy set:

$$\{(x, \mu_A(x), 1 - \mu_A(x)) : x \in X\}.$$

An IFN is as an IFS defined over the real axis IR_+. An IFS $A=\{(x,\mu_A(x),\nu_A(x)):x\in IR_+\}$ of a real number is called IFN if: (i) there exists real numbers $x_0\in IR_+$ such that $\mu_A(x_0)=1$ and $\nu_A(x_0)=0$; (ii) membership μ_A of A is fuzzy convex and non-membership ν_A of A is fuzzy concave; (iii) μ_A is upper semi-continuous and ν_A is lower semi-continuous; (iv) support $((A)=\overline{(\{x\in IR_+:\nu_A(x)<1\})})$ is bounded. Therefore, an IFN A is a conjecture of two fuzzy numbers, namely A^+ with a membership function $\mu_{A^+}(x)=\mu_A(x)$ and A^- with a membership function $\mu_{A^-}(x)=\nu_A(x)$.

Two type of IFN are most often encountered in applications: triangular IFN (TIFN) and trapezoidal IFN (TzIFN). In most situations, is recommended to use TIFN for the reason of computational complexity [2]. Thus, a TIFN $\tilde{A}=[a_2;(a_1,a_3);(a_1',a_3')]$ with parameters $a_1'\le a_1\le a_2\le a_3\le a_3'$ is a special IFS on the real number set IR_+, whose membership and non-membership functions are defined as follows:

$$\mu_{\tilde{A}}(x)=\begin{cases}(x-a_1)/(a_2-a_1), & a_1\le x\le a_2\\ (a_3-x)/(a_3-a_2), & a_2\le x\le a_3\\ 0, \quad \text{otherwise}\end{cases},\qquad \nu_{\tilde{A}}(x)=\begin{cases}(a_2-x)/(a_2-a_1'), & a_1'\le x\le a_2\\ (x-a_2)/(a_3'-a_2), & a_2\le x\le a_3'\\ 1, \quad \text{otherwise}\end{cases}.$$

In the application with NFITs of $\tilde{A}$, they are represented as $\tilde{A}=[a_2;(a_1,a_3);(a_1',a_3')]$or by (α,β)-*cut* sets, denoted $\tilde{A}_{\alpha,\beta}=[\tilde{A}^{\alpha};\tilde{A}^{\beta}]$ with $\tilde{A}^{\alpha}\cap\tilde{A}^{\beta}=\varnothing$, that $\tilde{A}_{\alpha,\beta}$ is a crisp subset of IR_+, where $\tilde{A}^{\alpha}=\{x\in X:\mu_{\tilde{A}}(x)\ge\alpha\}$ and $\tilde{A}^{\beta}=\{x\in X:\nu_{\tilde{A}}(x)\le\beta\}$ with $0\le\alpha\le1$, $0\le\beta\le1$, and $0\le\alpha+\beta\le1$.

To represent a NFIT, the following closed intervals are often used:

$$\tilde{A}^{\alpha}=[a_1+\alpha(a_2-a_1),\ a_3-\alpha(a_3-a_2)] \text{ and } \tilde{A}^{\beta}=[a_2-\beta(a_2-a_1'),\ a_2+\beta(a_3'-a_2)].$$

3. IFGSPN MODELING OF ATTACKER - DEFENDER INTERACTION IN MANET NODES

Analogously to dependability analysis, we regard security breach states of MANET nodes as failure states in the security community. In this paper, a malicious attack toward MANET nodes will therefore result from malicious behaviors which have been successful in exploiting existing vulnerabilities.

While investigating QoS systems, known information about values of component's failure parameters, attack rates, risks and vulnerabilities, etc. are, in general, not perfects [1, 6, 11]. The uncertainty of real values of the quantitative parameters can have two origins. First source of uncertainty comes from the randomness character of the information that has a natural stochastic variability. The second source of epistemic uncertainty is related to imprecise and incomplete character of information, because there is no knowledge about real values of system quantitative parameters, which change dynamically their state. Therefore, in order to make our modeling approach more accurate, realistic, and versatile that describe the behavior of the attacker and defense interactions of the MANET nodes, it is necessary to

take into account the probabilistically and fuzzy aspects [12, 22]. This can be implemented by defining a new extension of GSPN, which has quantitative attributes that can have intuitionistic fuzzy values and incorporate the stochastic game, associated with immediate transitions in structural conflict, in way to handle the problems where two conflicting interests situation exist and appears between the attackers and defender. Thus, we use the timed transitions with intuitionistic fuzzy firing rates to determine the intuitionistic fuzzy state probabilities of MANET nod behaviors [1, 6].

Definition 1. A generalized Petri net (GPN), denoted Γ, is a 10-tuple structure of objects: $\Gamma = < P, T, Pre, Post, Test, Inh, K_p, Pri, G, M_0 >$, where: $P \neq \varnothing$, $|P| = k$, represents the set of places, which describes the local state of net. Places can contain a positive number of tokens. A place is usually represented as a circle graphically; $T \neq \varnothing, |T| = n$ and $P \cap T = \varnothing$, is the set of transitions, which describes the event or the actions and induces the state change. A transition is usually denoted as a rectangle or a line graphically; *Pre*, *Test* and $Inh: P \times T \times IN_+^{|P|} \to IN_+$ are forward incident functions relative to transition: *Pre* is the forward incident function, *Test* (and *Inh*) is the promoter (inhibition) function of transition; $Post: T \times P \times IN_+^{|P|} \to IN_+$ is the backward incident function relative to transition; $K_p: P \times IN_+^{|P|} \to IN$ is the capacity function of places; $Pri: T \times IN^{|P|} \to IN_+$ is the dynamical priority function, for firing transitions enabled by current marking; $G: T \times IN_+^{|P|} \to \{true, false\}$ it the guard function of transitions; IN_+ is the set of non-negative integers; M_0 is the initial marking.

A place from which an arc originates is considered to be an input place of a transition in which the arc terminates. A place in which an arc terminates is considered to be an output place of a transition from which the arc originates. Token is another important sign, it usually denoted as solid dot and contained in places to represent the state of GSPN. The dynamic behavior of auto modified Γ net is managed and controlled by the firing rules described in [7, 8, 14].

Definition 2. A GSPN with IFN firing rates of timed transitions and stochastic games of immediate transitions, named IFGSPN, is a structure of objects, described by a 7-tuple: $\tilde{\Gamma} = < \hat{N}, \hat{\Gamma}, w, \pi, \hat{\rho}, \tilde{\Lambda}, \mu_\lambda, \nu_\lambda U >$, where: $\hat{N} = \{1, 2, ..., \hat{n}\}$ denote the player set; $\hat{\Gamma}$ is a timed stochastic GPN type Γ, where the finite set of transitions T can be divided into two categories, immediate transitions T^0 and timed transitions T^τ, $T = T^0 \cup T^\tau$, $T^0(M) \cap T^\tau(M) = \varnothing$ with $\Pr i(T^0) > \Pr i(T^\tau)$. The transition $t_k \in T^0$ can be fired randomly and the delay is zero, and they are usually represented as thin bars. T^τ is the set of timed transitions and with each of which is associated a random firing delay time that have an exponential-negative distribution. In its turn $T = \bigcup_{l=1}^{\hat{n}} T_l \cup T_r$, $\bigcap_{l=1}^{\hat{n}} T_l \cap T_r = \varnothing$ is partitioned so that subset T_l, l=1,… $\hat{n}$ is associated with player l, and T_r the rest of transitions; $w: T^0 \times IN_+^{|P|} \to IR^+$ is the weight function $0 \le w(t, M) < +\infty$ which determines the firing probability $q(t, M)$ of immediate transition $t \in T^0(M)$ in current marking M, which describes a probabilistic selector; IR^+ is a set of real non-negative numbers; $q^\rho : T_l \to [0, 1]$ is the decision politic, represented by the probability of selecting a particular immediate transition; $\hat{\rho}: T \to (\hat{\rho}_1, ..., \hat{\rho}_l, ..., \hat{\rho}_{\hat{n}})$ is the payoff function,

$\hat{\rho}_l \in (-\infty, +\infty)$; $\tilde{\Lambda} : T^\tau \times IN_+^{|P|} \to IR^+$ is the function that determines the intuitionistic fuzzy firing rate $0 < \tilde{\lambda}(t, M) < +\infty$ of timed transition $t \in T^\tau$, that is enabled by current marking M, the parameters of exponential-negative law. In this case IR^+ is the set with non-negative numbers; $\mu_\lambda : \tilde{\Lambda} \to [0,1]$ and $\nu_\lambda : \tilde{\Lambda} \to [0,1]$ are the membership degree and the non-membership degree, respectively of $\tilde{\lambda}(t, M) \in \tilde{\Lambda}$, which determines the numerical intuitionistic fuzzy values for firing rate of timed transitions; *U* is the payoff function of attackers of MANET and MANET node security system itself.

With each token in place $p_i^l \in (t_k^\bullet \wedge {}^\bullet t_j), t_k \in T_l^0, t_j \in T_l^\tau$ of player *l* is assigned a reward $r_j^l(p_i)$ as its property what it is in p_i^l. Players get the reward $r_j^l(p_i)$ after the firing of the transition $t_j \in T_l^\tau$, and this reward is recorded in the reward vector of the player *l*. For the sake of simplicity and to fit our attacker-defender model, we assume that our stochastic game is a two-player discounted stochastic game.

The attacker's goal is to compromise functionality of a MANET's node. In figure 1 it is presented the GSPN1 model subjacent of IFGSPN1 that describes interaction between attacker and security system in a MANET node for four strategies.

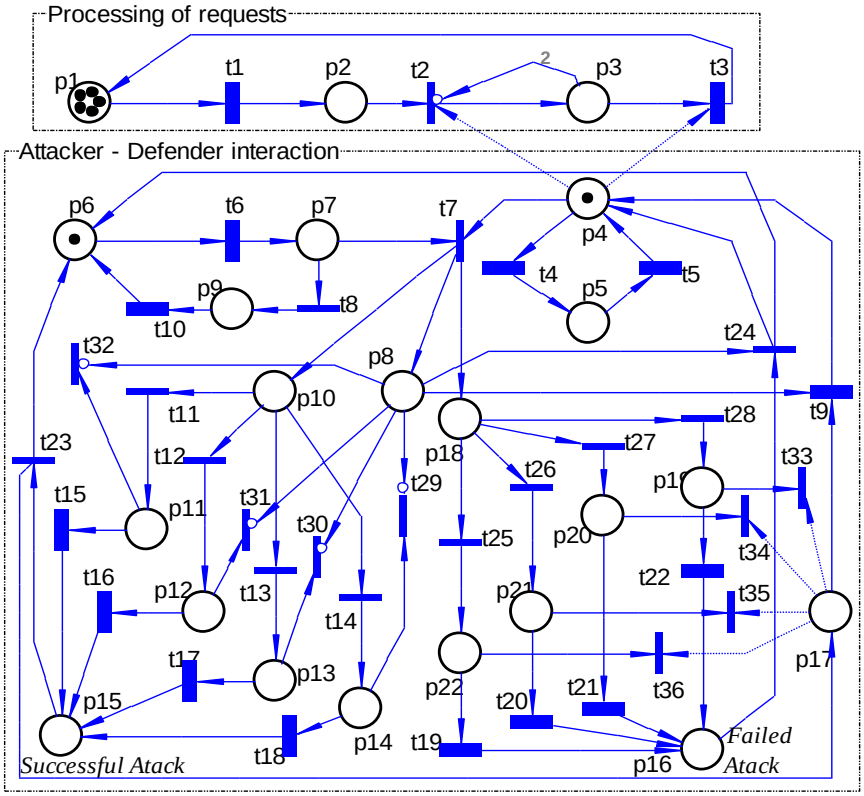

Figure 1. GSPN1 subjacent of IFGSPN1model.

The IFGSPN1 model was built using the methodology described in [7]. In figure 1 the places and transitions are following meaning:

- *places*: p_1 - potential number of users using the node; p_2 - requests in waiting for processing queue; p_3 - request in process; p_4 - operating safety state; p_5 - failures; p_6 - intruder starts the attack; p_7 - intruder has attacked; p_8 - the attack is detected by security system; p_9 - intruder has abandoned the attack; p_{10} - selecting attack strategy; p_{11}, p_{12}, p_{13} and p_{14} - intruder has selected a specific attack strategy a_1, a_2, a_3, a_4; p_{15} - attack has succeeded; p_{16} - attack has failed; p_{17} - security system is damaged (system restore started) ; p_{18} - selecting defense strategy.

- *transitions*: t_1 - users requests arriving; t_2 - allocation of resources for processing one request; t_3 - processing the requests; t_4 - occurrence of a failures; t_5 - reparation; t_6 - analyzing the vulnerabilities and attacking the system; t_7 - attack detection; t_8 - abandoning the attack; t_9 - restoring damaged system after an attack; t_{10} - activities related to abandoning an attack; t_{11}, t_{12}, t_{13} and t_{14} - selecting an respective attack actions: a_1, a_2, a_3 and a_4 (for example: Sybil attack, Selfish attack, RREQ flooding attack and Black hole attack ; t_{15}, t_{16}, t_{17} and t_{18} - attack activities associated with attack action selected by the intruder a_1, a_2, a_3, a_4; t_{19}, t_{20}, t_{21} and t_{22} - respective defense activities d_1, d_2, d_3, d_4 of security system; t_{23} - the start of system restore action; t_{24} - starting the process of processing user requests after attack failed; t_{25}, t_{26}, t_{27} and t_{28} - selecting a respective defense action: d_1, d_2, d_3, d_4; t_{29}, t_{30}, t_{31} and t_{32} - abandoning the attack in case the defense system succeeded; t_{33}, t_{34}, t_{35} and t_{36} - abandoning the defense and start restoring the system in case the attack succeeded.

The firing rates of timed transitions t_i is expressed in form of the TIFN presented as (α, β) - *cuts*, $\alpha \in [0,1]$ and $\beta \in [0,1]$, with respectively trust intervals [2]: $\tilde{\lambda}_i^{\alpha} = (\lambda_i^{\alpha} + \gamma_i'^{\alpha} \cdot \alpha,\ \lambda_i^{\alpha} - \gamma_i''^{\alpha} \cdot \alpha)$, (resp. $\tilde{\lambda}_i^{\beta} = (\lambda_i^{\beta} + \gamma_i'^{\beta} \cdot \beta,\ \lambda_i^{\beta} - \gamma_i''^{\beta} \cdot \beta)$, where $\gamma_i'^{\alpha}$ (resp. $\gamma_i'^{\beta}$) and $\gamma_i''^{\alpha}$, (resp. $\gamma_i''^{\beta}$) are coefficients that determine *certainty* $\tilde{\lambda}_i^{\alpha}$, (resp. *uncertainty* $\tilde{\lambda}_i^{\beta}$) for left and right intervals, respectively. In case that (α, β)-cut is previously determined and is taking $\gamma_i'^{\alpha} = \gamma_i''^{\alpha} = \gamma_i^{\alpha}$, (resp. $\gamma_i'^{\beta} = \gamma_i''^{\beta} = \gamma_i^{\beta}$) the IFTN $\tilde{\lambda}_i$ will be expressed by $\tilde{\lambda}_i = ((\lambda_i^{\alpha}, \gamma_i^{\alpha}); (\lambda_i^{\beta}, \gamma_i^{\beta}))$, which is reduced to calculation.

Intruder's goal is to maximize his gain by selecting some attack strategies $q_i^1(a_i)$, and the security system will select a respective defense strategy $q_i^2(d_j)$ in order to minimize its losing caused by intruder. The expected intruder's gain is expressed by the following expression [5, 12]:

$$U^1 = \max_{q_i^1} \min_{q_i^2} \sum_{\forall a_i \in A} \sum_{\forall d_j \in D} q_i^1(a_i) \cdot q_i^2(d_j) \cdot \rho_{i,j} .$$

Some numerical QoS indicators, from a successful attack perspective, in case the intruder and the defense system select the pair of actions (a_i, d_j), associated with post-set immediate transitions of place p_{10} (resp. p_{18}) of model IFGSPN1, can be obtain through stochastic game with provided reward matrix $\hat{\rho} = (\rho_{i,j})_{4\times4}$, which reflects the reward associated with timed transitions t_{14+i} and t_{18+i}, $i = 1, 2, 3, 4$ and intuitionistic fuzzy firing rates for timed transitions.

The IFGSPN1 model was validated using VPNPTool [8, 18], which is a software tool for visual simulation, verification and performance evaluation of QoS indicators for this type models. The IFGSPN1 has bounded, liveness and reversible properties, and therefore underlying embedded CTMC has ergodic property. This model has been analyzed for different intuitionistic fuzzy firing rates values of timed transitions, allow us to determine QoS indicators specified by the user, one of these indicators is the intuitionistic fuzzy probability that MANET node is in safety state, when $\tilde{\pi}_4 = \Pr(M_k(p_4) = 1)$.

To illustrate this approach, we analyzed the part of IFGSPN1 model that describes the attacker-defender interactions with the following value of the payoff matrix elements:

$$\rho_{1,1} = 20,\ \rho_{1,2} = 30,\ \rho_{1,3} = 50,\ \rho_{1,4} = 20,\ \rho_{2,1} = 40,\ \rho_{2,2} = 10,\ \rho_{2,3} = 20,\ \rho_{2,4} = 50,$$
$$\rho_{3,1} = 30,\ \rho_{3,2} = 50,\ \rho_{3,3} = 40,\ \rho_{3,4} = 20,\ \rho_{4,1} = 10,\ \rho_{4,2} = 30,\ \rho_{4,3} = 30,\ \rho_{4,4} = 40.$$

For this payoff matrix we get the following strategies: $\vec{q}^1(A) = (0.061, 0.388, 0.510, 0.041)$ and $\vec{q}^2(D) = (0.082, 0.143, 0.367, 0.408)$ with expected payoff: $U^1 = 32.45$.

The TIFN values of respective timed transitions firing rates $\tilde{\lambda}_i = [\hat{\lambda}_i^{\alpha}; \hat{\lambda}_i^{\beta}]$ with $\hat{\lambda}_i^{\alpha} = (\lambda_i^{\alpha}, \gamma_i^{\alpha})$, $\hat{\lambda}_i^{\beta} = (\lambda_i^{\beta}, \gamma_i^{\beta})$ and $\tilde{\lambda}_i = \hat{\lambda}_i^* \cdot 10^4 \ \mathrm{sec}^{-1}$ are the following:

$$\hat{\lambda}_6^* = [(0.1 + 0.9\alpha), (1.1 - 0.1\alpha); (1 - 0.95\beta), (1 + 0.2\beta)],\ \hat{\lambda}_4^* = 30,\ \hat{\lambda}_9^* = \hat{\lambda}_{10}^* = [(3 + \alpha, 5 - \alpha); (4 - \beta, 4 + \beta)],$$
$$\hat{\lambda}_{15}^* = \hat{\lambda}_{19}^* = [(4 + \alpha, 6 - \alpha); (5 - \beta, 5 + \beta)],\ \hat{\lambda}_{16}^* = \hat{\lambda}_{20}^* = [(3 + \alpha, 5 - \alpha); (4 - \beta, 4 + \beta)],$$
$$\hat{\lambda}_{17}^* = \hat{\lambda}_{21}^* = [(5 + \alpha, 7 - \alpha); (6 - \beta, 6 + \beta)],\ \hat{\lambda}_{14}^* = \hat{\lambda}_{22}^* = [(7 + \alpha, 9 - \alpha); (8 - \beta, 8 + \beta)].$$

The detailed analysis, for these NFIT firing rates of timed transitions, shows that the confidentiality level of MANET node is NFIT $\tilde{\pi}_{Conf.}(\alpha, \beta) = [\tilde{\pi}_4(\alpha); \tilde{\pi}_4(\beta)]$, where:

$$\tilde{\pi}_4(\alpha) = (0.526317 + 0.073083\alpha,\ 0.661832 - 0.062432\alpha),$$
$$\tilde{\pi}_4(\beta) = (0.5994 - 0.184248\beta,\ 0.5994 + 0.091008\beta).$$

For these NFIT values, the degree of membership (certainty) $\mu_{\tilde{\pi}_4}(x)$ at $\tilde{\pi}_{Conf.}(\alpha,\beta)$ is:

$$\mu_{\tilde{\pi}_4}(x) = \begin{cases} (x - 0.526317)/0.073083, & 0.52637 \le x \le 0.599400 \\ (0.661832 - x)/0.062432, & 0.599400 \le x \le 0.661832 \\ 0, & \text{otherwise} \end{cases}.$$

Also, the degree of non-membership (uncertainty) at $\mu_{\tilde{\pi}_4}(x)$ at $\tilde{\pi}_{Conf.}(\alpha,\beta)$ is:

$$\nu_{\tilde{\pi}_4}(x) = \begin{cases} (0.599400 - x)/0.184248, & 0.415152 \le x \le 0.599400 \\ (x - 0.599400)/0.091008, & 0.599400 \le x \le 0.690408 \\ 1, & \text{otherwise} \end{cases}.$$

The degree of hesitation at the respective confidence interval of $\tilde{\pi}_{Conf.}(\alpha,\beta) = [\tilde{\pi}_4(\alpha); \tilde{\pi}_4(\beta)]$ is calculated according to the following expression: $\eta_{\tilde{\pi}_0}(x) = 1 - \mu_{\tilde{\pi}_0}(x) - \nu_{\tilde{\pi}_0}(x)$.

Figure 2 depicted how the impact of the uncertainty on the attack and defense rates contributes in the degrees of certainty, uncertainty and hesitation on confidentiality MANET node.

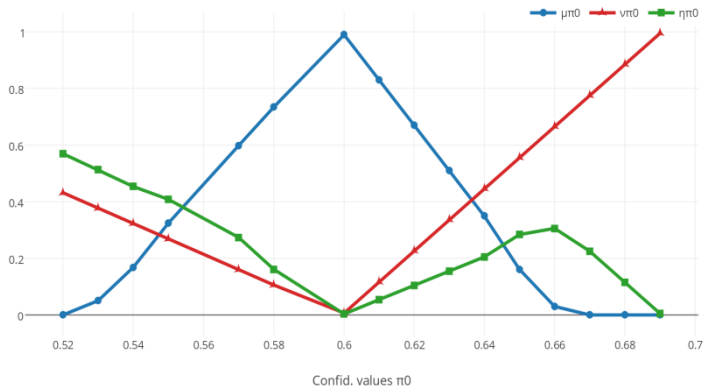

Figure 2**.** The degrees of certainty, uncertainty and hesitation on confidentiality MANET node $\tilde{\pi}_4(\alpha,\beta)$.

If a performance classification without uncertainty is preferred, it is necessary to either change the set of components or improve the values of parameters used in the security system to reduce its non-uncertainty and hesitation.

5. CONCLUSION

In this papers we present an framework for modeling and evaluating of safety behavior of attacker-defender interaction in MANET nodes using the methods, that we combine the theoretical stochastic games, intuitionistic fuzzy logic and generalized stochastic Petri nets (GSPN), based on which we defined a new class of GSPN with intuitionistic fuzzy firing rates of timed transitions and stochastic games, called IFGSPN. This type of models facilitates the describing expected behavior of the malicious intruder and the behavior of MANET's security system.

In this context, we present a concrete IFGSPN1 model that demonstrate how to describes and analyze the interaction between malicious attacks and defense upon a MANET node, specifying intuitionistic fuzzy parameters and the stochastic game. The validity of the proposed model is illustrated by an example with triangular fuzzy intuitionistic numbers using (α, β) - cuts analysis to show how it can be applied to the proposed approach, which better represents both dimensions of uncertainty, stochastic variability and inaccuracy in the shaping of this type nets in different threat environments.

Moreover, the approach is based on the underlying assumption that the attackers have a complete overview of the security system including states, transition rates, and detection rates, and the game is actually a zero-sum stochastic game; these might not always be valid assumptions. Thus, games of incomplete information and non-zero-sum games will therefore be another focus of our research by applying the intuitionistic fuzzy stochastic game.

REFERENCES

1. Augustin T., Miranda E., Vejnarova J. Imprecise probability models and their applications // International Journal of Approximate Reasoning.- 2009. – V.50 - N4 - P.581 - 582.

2. Atanassov K. T. Intuitionistic fuzzy sets // Fuzzy Sets and Systems. - 1986. - V. 20 - P. 87-96.

3. Azni A.H, Ahmad R., Azri Z., Noh M., Basari A. S., Hussin B. Correlated Node Behavior Model based on Semi Markov Process for MANETS // International Journal of Engineering Science and Innovative Technology (IJESIT). - 2013. -V.2 - N4 - P.50 - 59.

4. Azni A.H, Ahmad R. Noha Z. Survivability Modeling and Analysis of Mobile Ad Hoc Network with Correlated Node Behavior // Procedia Engineering. - 2013. - N53 - P.435 - 440.

5. Chakeri, A., Sadati, N., Sharifian, S. “Fuzzy Nash equilibrium in fuzzy game using ranking fuzzy numbers”, in: IEEE International Conference on Fuzzy Systems (FUZZ), pp.1-5 (2010).
6. Costa C., Benjamin, G., Bedregal, C., Doria Neto A. D. “Intuitionistic Fuzzy Probability”, in: SBIA 2010, A. C. da Rocha Costa, R. M. Vicari, F. Tonidandel, Editors, Proc. LNAI 6404, Springer-Verlag Heidelberg, pp. 273–282 (2010).

7. Guţuleac E. Descriptive compositional HSPN modeling of computer systems // Annals of the University of Craiova. Series: Atomation, Computers, Electronics and Mechatronics, Ed.: Universitaria, Craiova, România. - 2006. -V.3(30), N.2 , P.82-87.

8. Guţuleac E., Boşneaga C., Reilean A. “VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets“, in: The 6-th International Conference on D&AS2002, Proc., Suceava, România, pp. 243-248 (2002).

9. Ibidunmoye E. O., Alese B. K., Ogundele O.S. A Game-theoretic Scenario for Modeling the Attacker-Defender Interaction // J. Comput. Eng. Inf. Technol. - 2013. -V.2 - N1- P.1-8.

10. Jawandhiya P. M., Ghonge M. M., Ali M., Deshpande J. A survey of mobile Ad hoc network attacks // International Journal of Engineering Science and Technology. - 2010 - N2 - P.4063–4071.

11. Kahraman C., Tüysüz, F. “Manufacturing System Modeling Using Petri Nets”, in: Prod. Engr. & Manage, C. Kahraman, M. Yavuz, Editors, STUD-FUZZ 252, Springer-Verlag, pp. 95–124 (2010).

12. Lin C., Wang Y. Z., Wang Y. “A Stochastic Game Nets Based Approach for Network Security Analysis”, in: The 29th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Proc., pp.21-33 (2008).

13. Lin C., Wang Y Z., Wang Y. “A Stochastic Game Nets Based Approach for Network Security Analysis“, in: The 29 th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Concurrency Methods: Issues and Applications Workshop, Proc., pp.21-33 (2008).

14. Liu F., Heiner M., Yang M. Fuzzy Stochastic Petri Nets for Modeling Biological Systems with Uncertain Kinetic Parameters. // PLoS ONE. – 2016. –V.11 - N2 - P.1-19.

15. Mattoo M. M, Aziz A. A., Lone S. A. Modeling Malicious Multi-Attacker Node Collusion in MANETs Via Game Theory // Middle-East Journal of Scientific Research. – 2017. – V.25 - N3 - P.568-579.

16. Meng T., Wolter K., Wang Q. “Security and Performance Tradeoff Analysis of Mobile Offloading Systems Under Timing Attacks”, in: Computer Performance Engineering 12th European Workshop, M. Beltran et al., Editors, LNCS 9272, pp. 32–46 (2015).
17. Omar M., Challal Y., Bouabdallah A. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy // Journal of Network and Computer Applications, Elsevier. - 2012.- N35 - P.268-286.

18. Petri Nets Tools Database Quick Overview. https://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/quick.html

19. Prabha C., Kumar S., Khanna R. Wireless Multi-hop Ad-hoc Networks: A Review // IOSR Journal of Computer Engineering (IOSR-JCE). - 2014. V.16 - N2 - P. 54-62.

20. Qazi S., Raad, R., Mu Y., Susilo W. Securing DSR against wormhole attacks in multi rate Ad hoc networks // Journal of Network and Computer Applications. - 2013 - N36 - P.582–592.

21. Raj N. Ann M., Bala P. M. An Attack-defense Stochastic Game Approach for Malicious Nodes in MANETs // Imperial Journal of Interdisciplinary Research, IJIR. - 2016. - V.2 - N4 - P.1035-1040.

22. Sallhammar K., Helvik B. E., Knapskog S. J. On stochastic modeling for integrated security and dependability evaluation // The Journal of Networks. - 2006. - V.1 - N5 - P.31 – 42.

23. Singh S., Singh G., Narasimhan L., Shiwani S. Petri Net Modeling and Analysis of Mobile Communication Protocols UMTS, LTE, GPRS and MANET. International Journal of Engineering Science and Innovative Technology (IJESIT). - 2013. - V.2 - N4 - P.255- 258.

24. Tao M., Shan H. An improved method of the attack tree model for mobile Ad Hoc networks Research // Computer Applications and Software. - 2009. - V. 26 - N4 - P.271 – 273.

25. Yi Z., Dohi T. Survivability Analysis for a Wireless Ad Hoc Network Based on Semi-Markov Model // IEICE Transactions on Information and Systems. - 2012. -V.E95.D - N.12 - P.2844-2851.

26. Yadav P., Gaur M. “A Survey on Formal Modeling for Secure Routing in Mobile Ad hoc Networks”, in: International Conference on Distributed Computing and Internet Technology, ICDCIT, pp.18-23 (2015).

27. Zhuo W., Lin C., Chen X. Quantitative analysis method of network attack and defense based on stochastic game model // Journal of Computers. - 2010. - V.9 - P.1748 – 1762.