

## Analysis for Ad Hoc Network Attack-Defense Based on Stochastic Game Model

<sup>1</sup> Yuanjie LI, <sup>2</sup> Jie SUN <sup>3</sup> Qiying CAO

<sup>1</sup> College of Information Science and Technology, Donghua University, Shanghai, China

<sup>2</sup> Information Center, Ningbo Women and Children Hospital, Ningbo, China

<sup>3</sup> College of Computer Science and Technology, Donghua University, Shanghai, China

<sup>1</sup> Tel.: +86-021-67705177, fax: +86-021-67705171

E-mail: lyj@lixin.edu.cn, 526521757@qq.com, caoqiying@dhu.edu.cn

*Received: 1 June 2014 /Accepted: 27 June 2014 /Published: 30 June 2014*

---

**Abstract:** The attack actions analysis for Ad Hoc networks can provide a reference for the design security mechanisms. This paper presents an analysis method of security of Ad Hoc networks based on Stochastic Game Nets (SGN). This method can establish a SGN model of Ad Hoc networks and calculate to get the Nash equilibrium strategy. After transforming the SGN model into a continuous-time Markov Chain (CTMC), the security of Ad Hoc networks can be evaluated and analyzed quantitatively by calculating the stationary probability of CTMC. Finally, the Matlab simulation results show that the probability of successful attack is related to the attack intensity and expected payoffs, but not attack rate. *Copyright © 2014 IFSA Publishing, S. L.*

**Keywords:** Ad hoc networks, Stochastic game nets, Continuous-time Markov chain, Action analysis towards attacked ad hoc networks.

---

### 1. Introduction

Ad Hoc networks are a kind of special wireless mobile networks which was initially developed for the military field. With the popularity of mobile devices and wireless networks, Ad Hoc networks will have a wider application prospects. However, because of its characteristics, such as non-central, self-organized, multi-hop, energy and limited computing power of the nodes, it makes the Ad Hoc networks more vulnerable to security threats.

Establishing an effective evaluation and analysis method for Ad Hoc networks security can provide direction to establish the security mechanisms. Hence, there have been many researches in this filed at home and abroad. Kim et al. [1] evaluated the survivability of Ad Hoc military networks by computing the number of single-hop links among

nodes. Jihang et al. [2] proposed a security evaluation method of Ad Hoc networks based on projection pursuit theory, and the method develops a risk assessment and attributes analysis through establishing a RAPCA-PP model. Sathishkumr et al. [3] proposed a network security evaluation model based on fuzzy feedback control method of Ad Hoc networks, and the model can assess the impact from various network attacks. Chen et al. [4] proposed a new multi-agent-based dynamic lifetime intrusion detection and response planning model; the method can quantitatively evaluate different attacks security performance of Ad Hoc networks with different safety standards. Tao Ma et al. [5] proposed an improved method based on attack tree model for attacks to Ad Hoc networks, which can effectively make quantitative analysis to the attribute parameter of nodes. The current situation for research on the

stochastic model method is as follows. Madan etc. [6, 7] built a model of intrusion tolerance system by semi-Markov process model, and obtained the stationary probability by solving and calculating other relevant safety indexes. Singh et al. [8] analyzed and verified the safety performance of intrusion tolerance mechanisms using the random activity network, and built a model of the effects on the system and system intrusion tolerance mechanism to attackers. On the basis of that, it further solved the safety performance indicators. Dacier et al. [9] analyzed network security using the stochastic Petri nets, and turned the atomic attacks in the special weight graph into the random transition of SPN, thus the continuous-time Markov chains can be obtained by solving SPN model. Wang etc. [10] analyzed the security of e-commerce networks using the Stochastic Game Nets (SGN), the method combined stochastic game theory and the stochastic Petri nets, the transitions in Stochastic Petri Nets were assigned by attack and defense action intensity and the equilibrium policy probability, and calculated the stationary probability of isomorphic Markov chain, on this basis the security of e-commerce networks was analyzed finally. Although the method of stochastic model has the capability of model description and advantages of strong scalability, the problem of state space explosion on the model solution exists.

A certain security attribute of Ad Hoc networks is analyzed to a certain extent with the method of security evaluation in Ad Hoc networks discussed above, but there is short of the ability of dynamic description of the model. To solve this problem, this paper proposes a method of security analysis of the Ad Hoc networks based on stochastic game (Stochastic Game Nets, SGN) [11]. The method combined stochastic game theory and stochastic Petri nets, and built a model of Stochastic Game Nets of Ad Hoc Networks, assigned transitions in Stochastic Petri Nets through the attack intensity and the selection probability, then solved the place-based stability probability in stochastic Petri nets and throughout capacity of transition values for quantitative analysis of network security. Finally, the various performance indicators of Ad Hoc networks security were evaluated and analyzed by simulation experiments.

The main contributions of this paper are summarized as follows:

- 1) The attack and defense model of Ad Hoc Networks based on Stochastic Game Nets is built, by using stochastic game theory and stochastic Petri nets for reference.
- 2) A model of stochastic game nets of Ad Hoc networks is transferred into isomorphic continuous-time Markov chain.
- 3) Study on the equilibrium strategies he stochastic game model and the calculation method of stability probability of continuous-time Markov chain, the security performance of Ad Hoc networks is evaluated and analyzed using Matlab simulation.

## 2. Model of Ad Hoc Networks Based on SGN

### 2.1. Definition of SGN Model of Ad Hoc Networks

The game type of Ad Hoc networks is two-player zero-sum stochastic game. By using the definition of stochastic Petri nets for reference, a definition of SGN model is given with Molloy form as follows.

Definition 1. The SGN model of Ad Hoc Networks is a 9-tuple,  $SGN(Ad\ Hoc) = (N, P, T, F, \pi, \lambda, R, U, M)$ , where,

- 1)  $N = \{N_1, N_2\}$ ,  $N_1$  is the attackers of Ad Hoc networks;  $N_2$  is the Ad Hoc network itself.
- 2)  $P = P_1 \cup P_2 \cup \dots \cup P_n$  is the set of locations, which means the states of system.
- 3)  $T = A \cup D$  is a set of actions,  $A (a_1, a_2, \dots, a_n)$  is an attack actions set of Ad Hoc networks attackers,  $D (d_1, d_2, \dots, d_n)$  is a defense actions set of Ad Hoc networks attackers.
- 4)  $F$  is the selection probability of the arc.
- 5)  $\pi: T \rightarrow [0, 1]$ , is the selection probability of a certain arc (attack or defense action).
- 6)  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ , is the action intensity of attack and defense of Ad Hoc networks.
- 7)  $R: T \rightarrow (r_1, r_2, \dots, r_n)$  is payoff after attack and defense actions of Ad Hoc networks has been selected.
- 8)  $U^k(p_i) (k=1, 2)$  is the payoff function of attackers of Ad Hoc networks and Ad Hoc networks system itself at place  $P_i$ .
- 9)  $M$  is a token set.

### 2.2. Descript the Attack Action and Defense Strategy of Ad Hoc Networks

The typical attack and defense strategies of Ad Hoc Networks are selected to build action set of attack and defense, and attack action of attackers is described as follows:

- 1) Wormhole attack (wormhole): It is a serious attack against routing protocol of Ad Hoc networks by two collusion malicious nodes.
- 2) Sybil attacks: Attackers disguise themselves as multiple nodes to cause node redundant, make route algorithm depending on the node redundancy and other route algorithms can not work properly.
- 3) Selfish attack: Attack nodes only accept data packets and routing packets without forwarding, and thus, it has a great impact on network traffic and network delay.
- 4) RREQ flooding attack: The attacker sends a large number of RREQ packets continuously, so that the whole network is full of RREQ packets which take up a lot of bandwidth of wireless communication, and thus lead to the network congestion, and make the normal communication work and performance of network degrades severely.
- 5) Black hole attack.

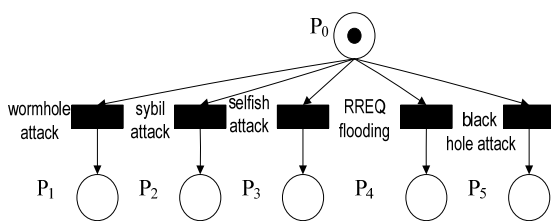
According to the description of attack and defense measures of the Ad Hoc networks, give the one-to-one relationship of the attack actions set A ( $a_1, a_2, a_3, a_4, a_5$ ) and the defense behaviours set D ( $d_1, d_2, d_3, d_4, d_5$ ) in Ad Hoc networks. The details are shown in Table 1.

**Table 1.** The one-to-one relationship of attack and defense behaviours and its actions set of A and D.

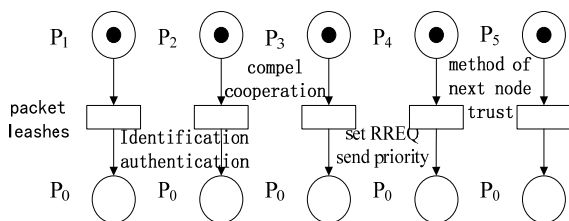
Attack action set A	Meaning of attack action	Defensive action set D	Meaning of defensive action
$a_1$	Wormhole attack	$d_1$	Packet leashes
$a_2$	Sybil attack	$d_2$	Authentication technology
$a_3$	Selfish attack	$d_3$	Forced cooperation
$a_4$	RREQ flooding attack	$d_4$	Set sending priority of RREQ
$a_5$	Black hole attack	$d_5$	Method of the next node trust

**2.3. Role Models of SGN**

According to the attack actions of Ad Hoc networks in the last section, the SGN model can be built from the perspective of the attackers. As shown in Fig. 1, the circle represents the place, rectangle means a transition, the circular with black dots represents the initial state of the place  $P_0$ , and the place  $P_1, P_2, P_3, P_4, P_5$  represents the state of Ad hoc networks system after several attacks. Similarly, you can build a SGN model from the defenders' perspective, as shown in Fig. 2.



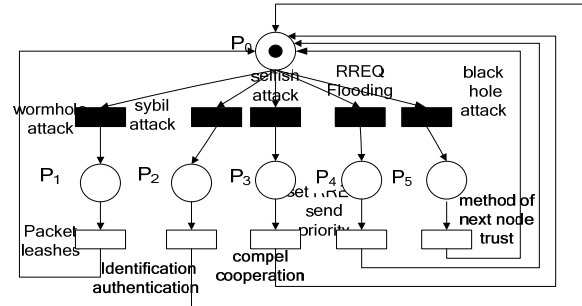
**Fig. 1.** SGN model of attackers' perspective of Ad Hoc networks.



**Fig. 2.** SGN model of defenders' perspective of Ad Hoc networks.

**2.4. The SGN Model of Attack and Defense Combination of Ad Hoc Networks**

According to the role model of SGN constructed in Fig. 1 and Fig. 2, the place of the same meaning can be merged to obtain the SGN model of attack and defense combination in Ad Hoc networks as shown in Fig. 3. The black transitions represent attack action of attacker, and the white transitions represent defense strategy of Ad Hoc networks.



**Fig. 3.** SGN model of attack and defense combination of Ad Hoc Networks.

**3. The Stability Probability of SGN Model of Ad Hoc Networks**

**3.1. Set the Parameter of the Combination Model of SGN and Calculate the Equilibrium Strategy of Attack Actions**

The goal of attackers in Ad Hoc networks is to destroy the networks, so that it cannot run normally. The payoffs of attackers are equal to the loss of Ad Hoc networks system itself. As the attackers do not know what kind of defensive measures the networks itself will take, so the attackers could not select the pure strategy to attack, but a mixture strategy.

According to the previous SGN model of Ad Hoc networks constructed and the computing method of balancing strategy of stochastic game based on hierarchical matrix, the following definition is given.

Definition 2. For the place  $P_0$  of SGN model from the attackers' perspective of Ad Hoc networks, the payoff matrix is described as follows.

$$\mathcal{R}^1(p_0) = \begin{matrix} & \begin{matrix} d_1 & d_2 & d_3 & d_4 & d_5 \end{matrix} \\ \begin{matrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{matrix} & \begin{matrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ r_{31} & r_{32} & r_{33} & r_{34} & r_{35} \\ r_{41} & r_{42} & r_{43} & r_{44} & r_{45} \\ r_{51} & r_{52} & r_{53} & r_{54} & r_{55} \end{matrix} \end{matrix} \quad (1)$$

where, when attackers and defenders adopt a pair of actions ( $a_i, d_j$ ) at place  $P_0$ , the elements  $r_{ij}$  in the payoff matrix represent the payoffs obtained by attackers.

Since the attack actions will only be affected by the corresponding defensive actions, the parameters of the payoff matrix can be set as follows.

$$\begin{aligned}
 r_{11}=2, r_{12}=r_{13}=r_{14}=r_{15}=8 \\
 r_{22}=3, r_{21}=r_{23}=r_{24}=r_{25}=5 \\
 r_{33}=1, r_{31}=r_{32}=r_{34}=r_{35}=4, \\
 r_{44}=1, r_{41}=r_{42}=r_{43}=r_{45}=6 \\
 r_{55}=2, r_{51}=r_{52}=r_{53}=r_{54}=7
 \end{aligned} \tag{2}$$

The goal of attackers of Ad Hoc networks is to maximize its payoffs by adopting the certain attack strategy  $\pi^1(a_i)$ , however, the system is to adopt the corresponding defense strategy  $\pi^2(d_j)$ , and make the payoffs of network attack minimized, so the expected payoffs function of attackers can be calculated in the following formula.

$$U^1(p_0) = \max_{\pi_i^1} \min_{\pi_i^2} \sum_{\forall a_i \in A} \sum_{\forall d_j \in D} \pi_i^1(a_i) \pi_i^2(d_j) r_{ij} \tag{3}$$

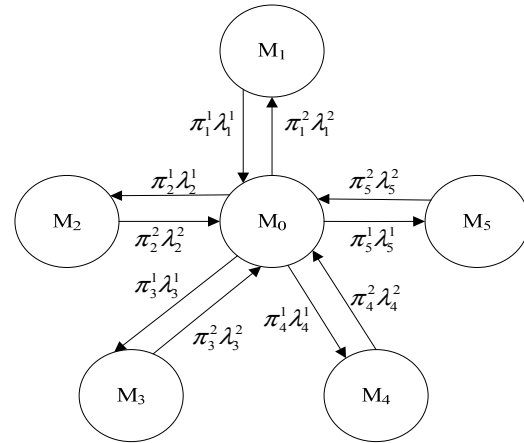
According to the standard calculation method of the equilibrium strategy of stochastic game [12], the equilibrium strategy of attack actions of Ad Hoc networks can be obtained by solving the equation (3). Attack and defense intensity  $\lambda$  and the probability of equilibrium strategy  $\pi$  obtained, as shown in Table 2.

**Table 2.** The parameter setting of combination model of SGN.

	Transition	Action intensity	Equilibrium Strategy
Attack actions	Wormhole attack	10	0.1190
	Sybil attack	12	0.3571
	Selfish attack	6	0.2381
	RREQ flooding attack	8	0.1429
	Black hole attack	10	0.1429
Defense actions	Packet leashes	3	1
	Authentication technology	5	1
	Forced cooperation	7	1
	Set sending priority of RREQ	3	1
	Method of the next node trust	6	1

### 3.2. The Isomorphic Continuous-time Markov Chain

A stochastic Petri net is isomorphic to a continuous-time Markov chain (CTMC) [13], which has been proven. Since SGN is a special stochastic Petri nets, in the same way, according to standard techniques [14], a SGN is isomorphic to a CTMC, as shown in Fig. 4.



**Fig. 4.** The isomorphic CTMC of combination SGN model of Ad Hoc networks.

In Fig. 4, the reachable token set.  $M_i$  ( $i=0, 1, 2, 3, 4, 5$ ), represents the token conditions of set of the places ( $P_0, P_1, P_2, P_3, P_4, P_5$ ). The tag of arc represents the implementation rate of transitions of isomorphic CTMC, the value is  $\pi_i^1 \lambda_i^1, \pi_i^2 \lambda_i^2$  ( $i=1, 2, 3, 4, 5$ ). Where  $\pi_i^1$  and  $\lambda_i^1$  represent the probability of selection and intensity of an attack action respectively,  $\pi_i^2$  and  $\lambda_i^2$  represent the probability of selection and intensity of defense actions respectively, the numerical list is given in detail in Table 2.

According to the implementation rate of transitions and standard calculation methods [15], the state transition matrix Q of isomorphic CTMC can be obtained, as shown in Table 3.

Assume that the stability probability of CTMC with n states is an n-dimensional row vector, according to Markov process, the linear equations is as follows.

**Table 3.** The state transition matrix of isomorphism CTMC of SGN model of Ad Hoc Networks.

	M0	M1	M2	M3	M4	M5
M0	-9.3920	1.19003890	4.28522	1.9048	0.8574	1.4290
M1	3	-3	0	0	0	0
M2	5	0	-5	0	0	0
M3	7	0	0	-7	0	0
M4	4	0	0	0	-4	0
M5	6	0	0	0	0	-6

$$\begin{cases} xQ = 0 \\ \sum_{i=1}^n x = 1 \end{cases} \quad (4)$$

When the state transition matrix of Table 3 is put into the equations (4), the reachability token stability probability of isomorphic CTMC of SGN model of Ad Hoc networks can be calculated, the results are as follows:

$$\begin{aligned} P\{M0\} &= 0.3358, & P\{M1\} &= 0.1332 \\ P\{M2\} &= 0.2877, & P\{M3\} &= 0.0914, \\ P\{M4\} &= 0.0720, & P\{M5\} &= 0.0799 \end{aligned} \quad (5)$$

#### 4. The Successful Probability Analysis of Ad Hoc Networks Attack

##### 4.1. The Calculation Method of Successful Probability Analysis of Ad Hoc Networks Attack

Many safety evaluation index of a system can have the quantified analysis based on the reachable marking stability probability from the isomorphism CTMC obtained at hand.

The attackers of Ad Hoc network adopt the attack action  $a_i$  ( $i=1, 2, 3, 4, 5$ ), in place pnormal, the following calculation formula for calculating the successful probability of attack is given in the unit time of the system.

$$p_{attack}(a_i) = P[M(p_r) \neq 0] = 1 - P[M(p_r) = 0] \quad (6)$$

where  $P[M(p_r) \neq 0]$  represents the non-zero probability of token number at the next place where attackers adopt attack action  $a_i$  at place pnormal, and  $P[M(p_r) = 0]$  represents the being zero probability of the token at the next place where attackers adopt attack action  $a_i$  at place pnormal.

According to the formula (6), the calculation formula for the successful probability as the system time goes by can be given at place pnormal where attackers adopt attack action  $a_i$ .

$$p'_{attack}(a_i) = 1 - P^t[M(p_r) = 0] \quad (7)$$

In the formula (7),  $t$  ( $t = 1, 2, 3, \dots$ ) represents the system time,  $p'_{attack}(a_i)$  represents the successful probability of attackers during the system  $t$ .

##### 4.2. The Matlab Simulation Analysis the Probability of Successful Attacks in Ad Hoc Networks

According to the formula (7), the probability of a successful attack is simulated and analyzed in Ad

Hoc networks using Matlab, the results are shown from Figs. 5 to 8.

From Figs. 5 to 8, the curves represent the successful probability of attack as the system time goes by,  $\square$  curve,  $\triangle$  curve,  $\circ$  curve,  $+$  curve and diamond curve represent the wormhole attack, Sybil attack, selfish attack and RREQ flooding attack respectively.

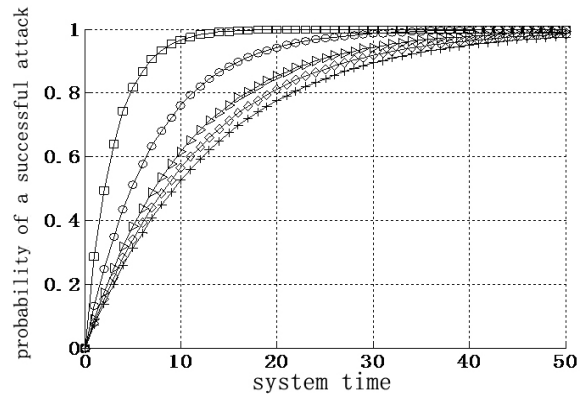


Fig. 5. The probability of successful attack as the system time goes by (attack rate = 1).

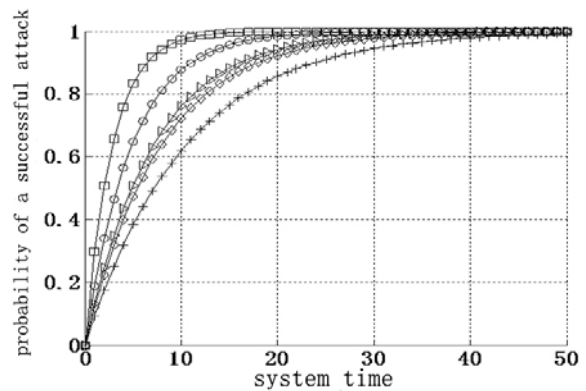


Fig. 6. The probability of successful attack as the system time goes by (attack rate = 5).

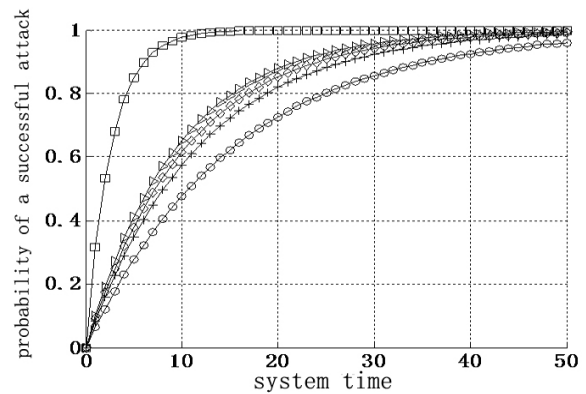
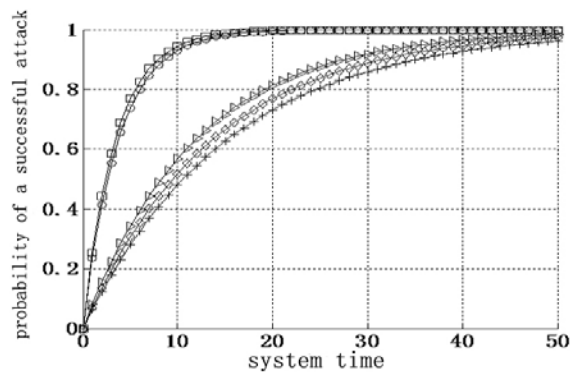


Fig. 7. After improving revenue of wormhole attack the probability of successful attack as the system time goes by (attack rate = 1).



**Fig. 8.** After improving action intensity of wormhole attack the probability of successful attack as the system time goes by (attack rate = 1).

From Figs. 5 to 6, it can be seen that the successful probability of various attack actions increases as the system time goes by. Where, the attack rising speed of Sybil is the fastest, and the wormhole is the second, the RREQ flooding attack is the third, while the selfish attack change is the slowest.

By comparing Fig. 5 with Fig. 6, it can be seen that the size and the trend of successful probability of attack have nothing with attack rate. In Fig. 7, it can be seen that the successful probability of wormhole attack is the lowest. Comparing Fig. 5 with Fig. 7, we can see that improving the payoff of the wormhole attack, and the wormhole attack will reduce the successful probability of attacks and will not change its trend. By comparing Fig. 5 with Fig. 8, we can see that improving the intensity action of wormhole attack can increase the successful probability, and not change the trends of successful probability of wormhole attack.

In summary, we can see that the size of successful probability of attackers of Ad Hoc networks is not related to the rate of attack, but the attack action intensity and its expected payoffs of attackers. And then, increasing the expected payoffs of a successful attack action will reduce the probability of attack action, and the improving intensity of a certain attack action can increase the successful probability of the attack action. Thus, for different Ad Hoc networks, designers of network security mechanism simply reset the initial data of SGN model presented in this paper (including attack action intensity and expected payoffs), to get the desired successful probability of various attack action.

## 5. Conclusions

The simulation analysis shows the following conclusions: in Ad Hoc networks, trends of the successful probability of attack action are not related with the attack rate, but the attack strength and attackers' expected payoffs. In this paper, the model based on stochastic game nets of Ad Hoc networks is

constructed with an assumption that attackers are independent. We are also interested in the model construction if the attackers are dependent which we will have a further study.

## Acknowledgments

This work was supported by National Natural Science Foundation of China under Grant No. 61272034.

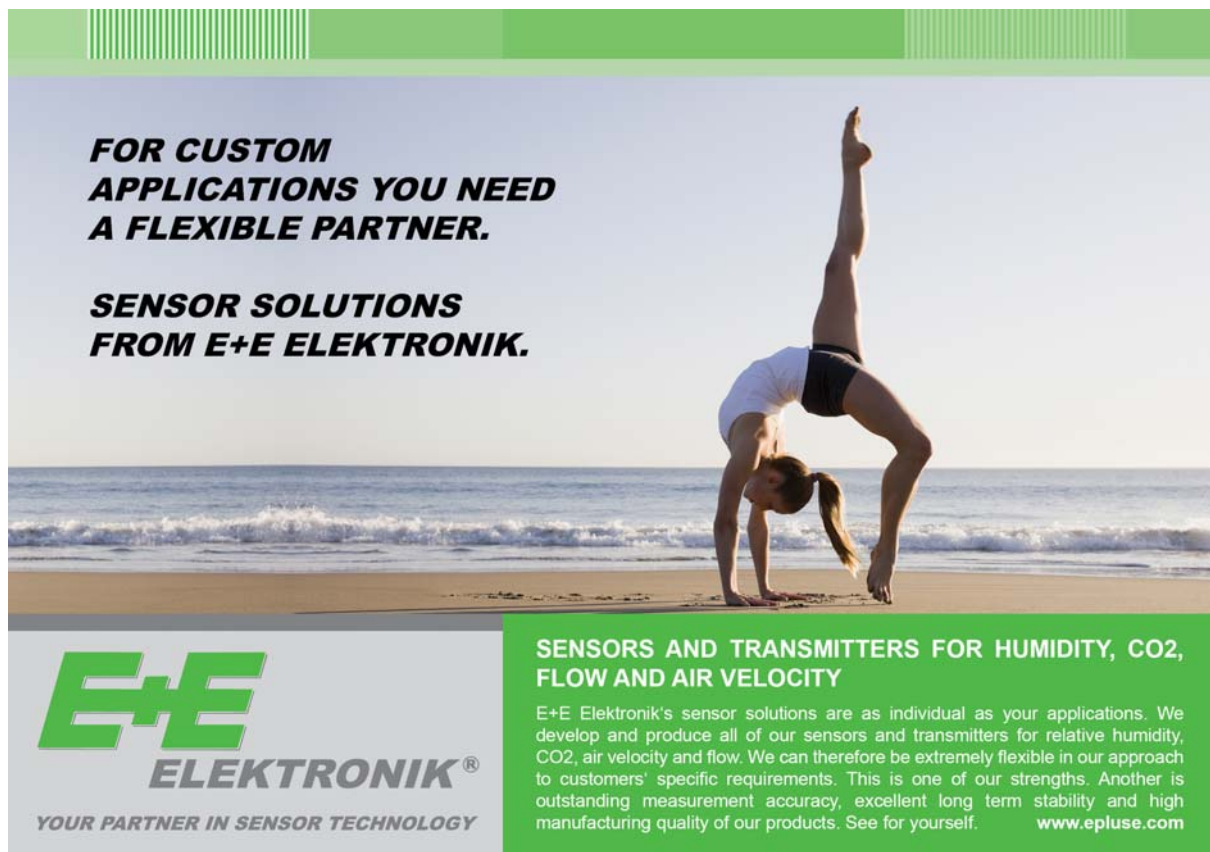
## References

- [1]. Kim K., Roh B. H, Ko Y. B, et al., Survivability measure for multi channel MANET-based tactical networks, in *Proceedings of the International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity*, 2011, pp. 1049-1053.
- [2]. Jihang Ye, Mengyao Liu, Cai Fu., Trusted risk evaluation and attribute analysis in Ad-Hoc Networks Security Mechanism based on Projection Pursuit Principal Component Analysis, *IEEE Computer Society*, Vol. 1, 2010, pp.492 – 497.
- [3]. Sathishkumar Alampalayam, Panup Kumar, An adaptive and predictive security model for mobile ad hoc networks, *Wireless Personal Communications: An International Journal*, Vol. 29, Issue 3-4, 2004, pp. 263 – 281.
- [4]. Chen Hongsong, Ji Zhen Zhou, Hu Mingzeng, et al., Design and performance evaluation of a multi-agent-based dynamic lifetime security for AODV routing protocol, *Journal of Network and Computer Applications*, Vol. 30, Issue 1, 2007, pp. 145 – 166.
- [5]. Tao Ma, Hong Shan, An improved method of the attack tree model for mobile Ad Hoc networks Research, *Computer Applications and Software*, Vol. 26, Issue 4, 2009, pp. 271 – 273.
- [6]. Madan B., Goeva-Popstojanova K., Vaidyanathan K., Trivedi K. S., A method for modelling and quantification of security attributes of software systems, in *Proceedings of International Conference on Dependable Systems and Networks*, Washington, DC, USA, 2002, pp. 505 – 514.
- [7]. Madan B., Goeva-Popstojanova K., Vaidyanathan K., Trivedi K. S., A method for modelling and quantifying the security attributes of intrusion tolerant systems, *Performance Evaluation*, Vol. 56, Issue 1-4 2004, pp. 167 – 186.
- [8]. Singh S., Cukier M., Sanders W. H., Probabilistic validation of an intrusion-tolerant replication system, in *Proceedings of the International Conference on Dependable Systems and Networks*, CA, USA, 2003, pp. 616 – 624.
- [9]. Dacier M., Deswarte Y., Kaaniche M., Quantitative assessment of operational security: Models and tools, *Laboratory for Analysis and Architecture of Systems: Technical Report*, 96493, 1996.
- [10]. Wang Y. Z., Lin C., Meng K., Lu J. J., Analysis of attack actions for E-commerce based on stochastic game nets model, *Journal of Computer*, Vol. 4, Issue 6, 2009, pp. 461 – 467.
- [11]. Wangyuan Zhuo, Chuang Lin, Xueqi Chen, Quantitative analysis method of network attack and defense based on stochastic game model, *Journal of Computers*, Vol. 9, 2010, pp. 1748 – 1762.

- [12]. Shapley L. S., Stochastic Games, in *Proceedings of the of the National Academy of Science USA*, Vol. 39, 1953, pp. 1095 - 1100.
- [13]. Sallhammar K., Helvik B. E., Knapskog S. J., On stochastic modelling for integrated security and dependability evaluation, *The Journal of Networks*, Vol. 1, Issue 5, 2006, pp. 31 – 42.
- [14]. Zuberek W. M., Performance evaluation using unbound timed Petri nets, in *Proceedings of the Third International Workshop on Petri Nets and Performance Models*, 1989, pp. 180 – 186.
- [15]. Molloy M. K., Structurally bounded stochastic Petri nets, in *Proceedings International Workshop on Petri Nets and Performance Models*, 1987, pp. 156 - 163.

---

2014 Copyright ©, International Frequency Sensor Association (IFSA) Publishing, S. L. All rights reserved.  
(<http://www.sensorsportal.com>)



**FOR CUSTOM APPLICATIONS YOU NEED A FLEXIBLE PARTNER.**

**SENSOR SOLUTIONS FROM E+E ELEKTRONIK.**

**E+E ELEKTRONIK®**  
YOUR PARTNER IN SENSOR TECHNOLOGY

**SENSORS AND TRANSMITTERS FOR HUMIDITY, CO<sub>2</sub>, FLOW AND AIR VELOCITY**

E+E Elektronik's sensor solutions are as individual as your applications. We develop and produce all of our sensors and transmitters for relative humidity, CO<sub>2</sub>, air velocity and flow. We can therefore be extremely flexible in our approach to customers' specific requirements. This is one of our strengths. Another is outstanding measurement accuracy, excellent long term stability and high manufacturing quality of our products. See for yourself. [www.epluse.com](http://www.epluse.com)