Defence Science Journal, Vol. 68, No. 1, January 2018, pp. 54-63, DOI : 10.14429/dsj.68.11402

A Game Theoretic Software Test-bed for Cyber Security Analysis of Critical Infrastructure

Monica Ravishankar[@, *], D. Vijay Rao[#], and C.R.S. Kumar[@]

[@]DRDO-Defence Institute of Advanced Technology, Pune - 411 025, India
[#]DRDO-Institute for Systems Studies and Analyses, Delhi - 110054, India
[*]E-mail: monica.ravishankar@gmail.com

ABSTRACT

National critical infrastructures are vital to the functioning of modern societies and economies. The dependence on these infrastructures is so succinct that their incapacitation or destruction has a debilitating and cascading effect on national security. Critical infrastructure sectors ranging from financial services to power and transportation to communications and health care, all depend on massive information communication technology networks. Cyberspace is composed of numerous interconnected computers, servers and databases that hold critical data and allow critical infrastructures to function. Securing critical data in a cyberspace that holds against growing and evolving cyber threats is an important focus area for most countries across the world. A novel approach is proposed to assess the vulnerabilities of own networks against adversarial attackers, where the adversary's perception of strengths and vulnerabilities are modelled using game theoretic techniques. The proposed game theoretic framework models the uncertainties of information with the players (attackers and defenders) in terms of their information sets and their behaviour is modelled and assessed using a probability and belief function framework. The attack-defence scenarios are exercised on a virtual cyber warfare test-bed to assess and evaluate vulnerability of cyber systems. Optimal strategies for attack and defence are computed for the players which are validated using simulation experiments on the cyber war-games testbed, the results of which are used for security analyses.

Keywords: Critical infrastructure; Game theory; Belief functions; Negotiations; Cyber war-games testbed.

NOMENCLATURE

Probability framework model

τ_1, τ_2	Decision accuracies of the attacker and defender player
μ	Probability distribution function
v	Value of the game
φ	Probability of successful attack
ω	Probability of unsuccessful attack
δ	Risk assessment parameter
m	Number of interactions in the negotiation game

Belief framework model

$\mathrm{A}_i \times \mathrm{A}_j$	Set of possible actions for the players i and j (attacker and defender)
$\pi_t^i \times \pi_t^j$	Payoff function for the players.
$b_x^{(K)}, c_x^{(K)}$	Belief function and confidence function of player x at level K thinking
$N(t)$, φ	Number of observation equivalents and attenuation coefficient
$\lambda^{(K)}$	Player specific learning speed
$\mu_{a_x^*}^t$	Expected value of player x, for selecting action.
$\theta^{(K)}$	Parameter that controls the sensitivity of probability of player x, for selecting action.

Received: 09 May 2017, Revised: 25 September 2017
Accepted: 06 October 2017, Online published: 18 December 2017

1. INTRODUCTION

National critical infrastructure refers to the complex underlying delivery and support systems for all large scale services considered absolutely essential to a nation[1]. With the widespread implementation of such services on computer systems and network infrastructures, protecting its critical information has become an important focus for many countries across the world. The critical facets of national infrastructure sectors range from people, networks to processes, which depend on massive information communication technologies (ICT), that are considered vital to the normal functioning of modern societies and economy. Such systems are vulnerable to damage as a result of natural disaster, physical incidents or cyber-attacks impacting on critical infrastructure organisations managing complex industrial control systems and data acquisition systems[1-4]. Security researchers and administrators also sometimes fail to propose appropriate security measures toward off attacks. As a consequence, these critical systems remain highly vulnerable to unanticipated attacks[2-4]. Research in this emerging area of security in critical infrastructures requires a solution methodology, carefully devised by the security experts using predetermined processes[5,6]. One such approach is to assess the security of one's own networks from the perspective of an attacker (adversarial modelling) to detect the network threats and test the existing security measures. To predict other's perception of one's strengths and vulnerabilities, applying advanced analytical skills and predicted techniques using game theory, machine learning and artificial intelligence at tactical level needs to be modelled to understand and capture the adversarial nature of the security problem to support decision making[7-9]. To model the cyber-attack-defence scenarios, many game models have been proposed in the literature. They assume that the players have perfect information about the game environment, i.e., the defender being always able to detect an attack and the attacker always being aware of the employed defence mechanism[10-15]. However, it has been observed that the above assumption about perfect information does not hold true in real-world scenarios.

In this paper, we propose game theoretic-based cyber warfare test-bed to assess the network security vulnerabilities of national critical infrastructure (Figs. 1 and 2). A cyber warfare interaction scenario is formulated as a game where the players (cyber attackers and network defenders) are assumed to possess imperfect information about their opponents. With the uncertainty about the current status of the environment, the players have to strategically plan their actions to gain a positive payoff[16-19]. These attack-defence scenarios are modelled and exercised on a virtual cyber test-bed using modelling and simulation techniques to assess and evaluate the vulnerabilities in cyber systems, suggest various course of actions and support decisions of appropriate actions to be taken by the players. The players' decision making capability is modelled and analysed first using a probabilistic framework and then using belief functions[20]. The solution for the games is deduced by computing optimal strategies and suggestions on various attack-defence strategies for the players. We model the behaviour of players and the uncertainties held by them about their opponents using a probability framework and belief framework. We further explore the interactions of the players using negotiation experiments to show that the belief framework provides a better representation of uncertainties and generates realistically better outcomes than the probabilistic framework. These results suggest possible course of actions for the players, that they can exercise and make decisions under an uncertain environment in various cyber war game scenarios. The proposed methodology is validated using simulation experiments on the cyber warfare test-bed.

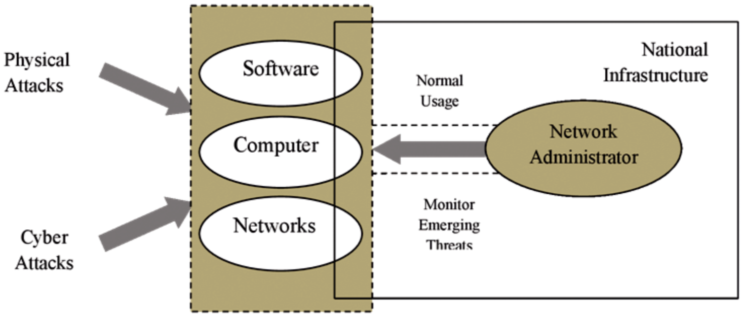

Figure 1. Cyber and physical attacks on national critical infrastructure.

2. DESIGN OF A CYBER WARGAMES TEST-BED

Cyber war games are designed to examine how organisations and critical response teams respond to realistic/ simulated cyber crises and highly skilled adversaries. The war game test process is comprised of phases of identification, defence, response, and recovery to an attack in depth[21-23]. This is achieved by setting up a cyber test-bed to exercise cyber-attack scenarios on a network environment as depicted in Fig. 2.

2.1 Network Simulation Test-bed Design

Designing a cyber test-bed involves the creation of virtual network environment to represent the real world systems and platforms such as Microsoft Windows, Linux, Mac OS, Novell Netware and BSD. The network test-bed is setup using Windows Virtual Machine and Linux Virtual Machine Back Track version 5 for the results reported in this work. Based on the attacker's objective, a number of attack techniques are experimented on the cyber warfare test-bed with the aid of sniffers and traffic generators. The attacker site (red player) is represented by the use of Metasploit, which is an exploit database filled with exploits and payloads installed on the back track machine to launch the attacks on the Windows host. Metasploit was basically designed to help security practitioners' to find vulnerabilities on their networks and fix them, however, this framework is also used by the attackers to exploit the vulnerabilities on a network.

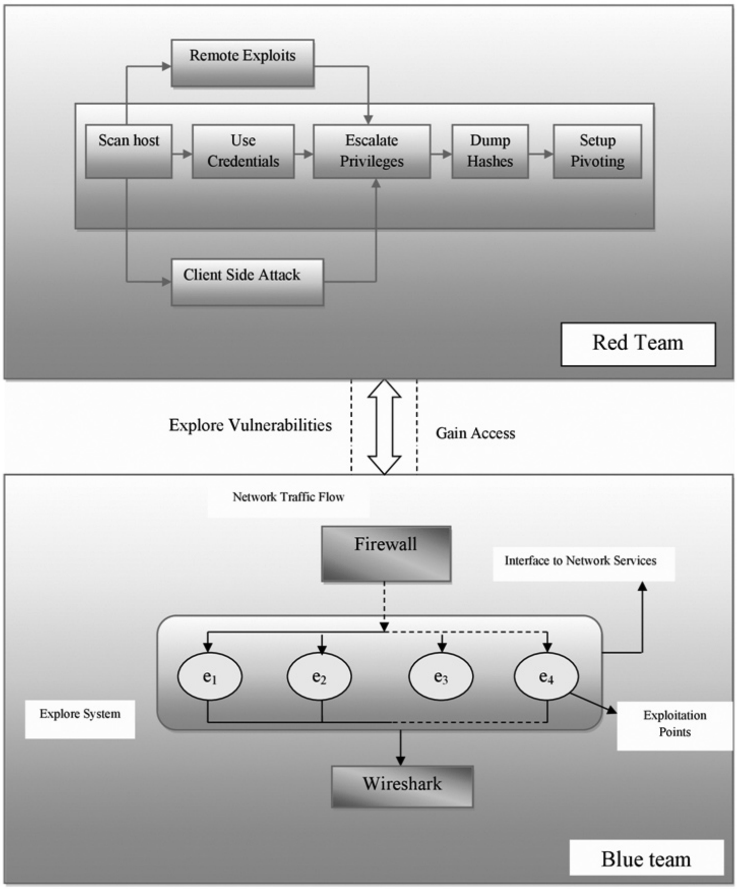

Figure 2. Virtual cyber warfare test-bed design.

These exploits are used to break in to the system and payload is implemented to produce attack actions on the victim machine. Metasploit uses scriptable toolsets like Armitage for adversary simulations and red team operations. These toolsets facilitate Metasploit around the hacking process for discovery of current targets and launch appropriate exploits, post-exploitation and manoeuvre[24]. The victim machine / defender's system (blue player), on the other hand, represent windows virtual machine with Wireshark[25] installed to monitor the network attacks. The goal of the virtual cyber test-bed is to model realistic cyber environments to execute and record the attacks and provide accurate assessment and evaluation of the vulnerabilities that exist in the cyber systems in the real world. This quantifies the impact of a cyber intrusion on the operation of underlying physical system.

3. A GAME THEORETIC APPROACH FOR CYBER SECURITY DECISION ANALYSIS

Although systems are designed against the attacks of the highly skilled adversaries, they are still vulnerable to cyber threats. Defending against sophisticated antagonists is a challenging task which requires not only high technical skills, but also a keen understanding of intentions and incentives behind their attacks and the different strategies used by them. Security decisions are analysed analytically using game theory models. Game theory is an effective method to capture the nature of adversaries, characterise the impacts of cyber-attacks and suggest appropriate security reinforcement mechanism. The cyber warfare scenario is formulated as a game, where the players (cyber attackers and network defenders) are assumed to possess imperfect information about their opponents. Players are modelled within the framework of conflict of interest since decisions made under imperfect information conditions about the opponent could gain a penalty with incorrect beliefs and assumptions. Faced with this situation of reasoning under uncertainty, some additional assumptions are required for a clear superior choice to emerge. To illustrate the process, we first model the behaviour of players under probabilistic framework and then describe how the players' behaviour, and learning can be modelled using belief functions, as an improved framework to represent such uncertainties.

4. MODELLING THE DECISIONS OF PLAYERS UNDER UNCERTAINTY USING A PROBABILITY FRAMEWORK

The term uncertainty in the context of cyber warfare is characterised by the ignorance about the game environment, scarce, unreliable and conflicting information held by the players about their opponents and the inability of the decision makers to resolve the set of all possible outcomes.

We model the state of uncertainty of players using a probability framework. The decision accuracy of the attacker is represented by τ_1 and that defender player is τ_2.The attacker chooses an appropriate action with decision accuracy τ_1 to maximise his attacks while that of the administrator is to minimise the attacks by choosing an appropriate action with decision accuracy τ_2. The solution of this game can be obtained by solving the problem as discussed as follows:

Lemma 1: Let x and τ_2 be optimal, where the attacker uses mixed strategy x and the administrator uses a pure strategy τ_2, then $K(x,\tau_2)=\nu$, where ν is the value of the game.

Proof: Since x is optimal, $K(x,\tau_2)=\nu$, $\forall\ \tau_2$ in the interval $[0,1]$. But if $K(x,\tau_2)$ had been greater than ν, then this inequality would hold for an interval about τ_2. Since $K(x,\tau_2)=\nu$ is assumed to be continuous w.r.t both the variables. Integrating $K(x,\tau_2)=\nu$, w.r.t. $\partial(\tau_2)$, we obtain the value greater than ν. Thus the solution of the game has a probability function where $\forall\ \tau_2 \quad K(x,\tau_2)>\nu$. This contradicts the assumption that τ_2 is optimal. Consider a strategy x° to be an equaliser strategy[26] for the attacker such that $K(x^{\circ},\tau_2)$ yields some constant $\forall\ \tau_2$, then we obtain the following corollaries for this lemma.

Corollary 1. If x is a mixed optimal strategy for the attacker player, then every optimal strategy for the defender player is an equaliser strategy.

Corollary 2. If every τ_1, within the interval $[0,1]$ is necessary for the attacker player, then every optimal strategy for the defender player is an equaliser strategy.

The pair of strategies τ_1 and τ_2 is said to constitute a solution for the game if $K(\tau_1,y)\geq K(\tau_1,\tau_2)\geq K(x,\tau_2), \quad \forall\ \tau_1,\tau_2$ within the unit interval $[0,1]$.

The attacker's payoff is formulated as:

$$K(\tau_1,\tau_2)=$$
$$\begin{cases} \tau_1+(1-\tau_1)\tau_2(-1)=-\tau_2+(1+\tau_2)\tau_1, \\ \qquad\qquad\qquad\qquad \mathit{If}\ \ \tau_1<\tau_2 \\ \tau_1(1-\tau_1)+\tau_1(1-\tau_1)(-1)=0, \\ \qquad\qquad\qquad\qquad \mathit{If}\ \ \tau_1=\tau_2 \\ \tau_2(-1)+(1-\tau_2)\tau_1=-\tau_2+(1-\tau_2)\tau_1, \\ \qquad\qquad\qquad\qquad \mathit{If}\ \ \tau_1>\tau_2 \end{cases} \tag{1}$$

Since the players have insufficient knowledge about their opponents, it is assumed that the optimality of each player is composed of a parameter μ chosen at level μ°, to be the probability distribution function over the interval $(\mu,1)$. The value ν, of this game is obtained on the interval $(\mu,1)$ which is considered as the necessary condition for optimality, according to lemma 1. This is possible if the attacker uses a mixed strategy x and the administrator uses a pure strategy τ_2. The expected payoff for the attacker is

$$\begin{aligned} E(x,\tau_2) &= \int_0^1 K(\tau_1,\tau_2)\partial x(\tau_1) \\ &= \int_{\tau_2=0}^{\tau_1=\tau_2-0} K(\tau_1,\tau_2)\partial x(\tau_1)+\int_{\tau_2+0}^{1} K(\tau_1,\tau_2)\partial x(\tau_1) \\ &= \int_0^{\tau_2-0}\left[-\tau_2+(1+\tau_2)\tau_1\right]\partial x(\tau_1) \\ &\qquad\qquad +\int_{\tau_2+0}^{1}\left[-\tau_2+(1-\tau_2)\tau_1\right]\partial x(\tau_1) \\ &= \tau_2[x(\tau_2)-x(\tau_2-0)]-\tau_2+(1+\tau_2) \\ &\qquad\qquad \int_0^{\tau_2-0}\tau_1\partial x(\tau_1)+(1-\tau_2)\int_{\tau_2+0}^{1}\tau_1\partial x(\tau_1) \end{aligned} \tag{2}$$

On considering the parameter μ chosen at level μ°, to be the probability distribution function over the interval $(\mu,1)$ of the form

$$\begin{cases} \partial x(\tau_1) = P(\tau_1), & \mathit{If}, \mu \le \tau_1 \le 1 \\ \partial x(\tau_1), & \mathit{If}, \tau_1 < \mu \end{cases} \tag{3}$$

Then,

$$E(x,\tau_2) = \begin{cases} -\tau_2 + (1+\tau_2)\int_{\mu}^{\tau_2} \tau_1 P(\tau_1)\partial\tau_1 + \\ \qquad (1-\tau_1)\int_{\tau_2}^{1} \tau_1 P(\tau_1)\partial(\tau_1), \\ \qquad\qquad \mathit{If}\ \tau_2 \ge \mu \\ -\tau_2 + (1-\tau_2)\int_{\mu}^{1} \tau_1 P(\tau_1)\partial(\tau_1), \\ \qquad\qquad \mathit{If}\ \tau_2 \le \mu \end{cases} \tag{4}$$

The solution of the game has a probability density function, $\forall\ \tau_2$ where $E(x,\tau_2) = \nu = 0$, then we must have

$$\begin{aligned} &-\tau_2 + (1+\tau_2)\int_{\mu}^{\tau_1} \tau_1 P(\tau_1)\partial(\tau_1) + \\ &\qquad (1-\tau_2)\int_{\tau_2}^{1} \tau_1 P(\tau_1)\partial(\tau_1) = 0 \end{aligned} \tag{5}$$

On differentiating the above expression and further solving it we obtain, $(\tau_2) = \frac{C}{\tau_2^3}$. Substituting the value of $P(\tau_2)$ in the Eqn (4), we get

$$-\tau_2 + (1+\tau_2)C\int_{\mu}^{\tau_2} \frac{\partial(\tau_1)}{\tau_1^2} + (1-\tau_2)C\int_{\tau_2}^{1} \frac{\partial(\tau_1)}{\tau_1^2} = 0 \tag{6}$$

Thus, $\forall\ \mu \le \tau_2 \le 1$, the above expression yields $\mu = \frac{1}{3}, C = \frac{1}{4}$, independent of τ_2.

Thus we have verified that the optimal payoff (in terms probability of decision accuracy) for both the players is τ_1 with the probability density function

$$P(\tau_1) = \frac{1}{4}\tau_1^3, \qquad \forall\ \frac{1}{3} \le \tau_1 \le 1 \tag{7}$$

4.1 Learning from Observations: A Negotiation Game

The behaviour of the players under uncertainty modelled using the probabilistic framework is further analysed using a cyber-attack scenario illustrated as a negotiation game. Here, the attacker's goal is to install a sniffer to crack a root password of the system. The defender on the other hand, will detect the attack actions and take preventive measures by installing a sniffer detector. Consider a situation where the defender is working towards defending the system against the attacks of cyber adversary by employing two different types of defence mechanisms (Type A and Type B). The tactical situation of this problem is such that the defender has to choose a right defence mechanism to safeguard the system against the attack, while attacker has to make an appropriate attack (Type A or Type B) on the system by breaking the corresponding defence. If the attacks go undetected, then the probability of attacking the system is φ.But if the defender detects the attack, the attacker runs a risk of δ, and the probability of succeeding in the attack is $(1-\delta)\varphi = \omega$.

For m interactions in the negotiation game, let us assume the probability of choosing each type of strategies by the player, during each interaction to be the following: $\mathrm{A}^x = \mathrm{A}, \mathrm{A}, \ldots, \mathrm{A}, \mathrm{B}, \mathrm{B}, \ldots, \mathrm{B}$, with $x\ \mathrm{A}'s$ followed by $(m-x)\mathrm{B}'s$. This is done in order to observe the confidence with which players make their choices at each interaction. The possibilities by which the attacker may fail in each of his interaction with the defender is computed using the elements $a(x,\mathrm{A})$ and $a(x,\mathrm{B})$ of the $(m+1)\times 2$ payoff matrix, where

$$\begin{aligned} &a(x,A) = 1-(1-\varphi)^x(1-\omega)^x - \omega\varphi(1-\varphi)^{m-1} \\ &a(x,B) = 1-(1-\varphi)^x(1-\omega)^{m-x} - \\ &\omega(\varphi-\omega)^{-1}(1-\varphi)^x\left\{(1-\omega)^{m-x} - (1-\varphi)^{m-x}\right\} \end{aligned} \tag{8}$$

The game considered for this case can be solved, by considering concavity in x, where we perform derivative test for the concavity of the function for a single variable to obtain the saddle point for the game. According to which, let x_0 (first order derivative) be the solution of $\frac{\partial a(x,A)}{\partial x} = 0\,\partial x$

Then,

$$x_0 = m - \frac{\ln \varphi/(1-\varphi) - \ln\ln A}{\ln R}, \qquad R = \frac{1-\omega}{1-\varphi} \tag{9}$$

The probability with which the player decides an action A depends on the value of x_0. Now if $a(x_0,\mathrm{A}) \le a(x_0,\mathrm{B})$, then both attacker and defender would possess a pure optimal strategy, where x_0 would be attacker's strategy and A would be defender's strategy. If $a(x_0,\mathrm{A}) \ge a(x_0,\mathrm{B})$, only then the attacker has a pure optimal strategy x, given by Eqn (10).

$$\frac{x\varphi(\varphi-\omega)}{\omega(1-\varphi)} = \frac{(1-\omega)^{m-x}}{(1-\varphi)^{m-x}} \tag{10}$$

On solving the Eqn (10) we obtain

$$x = \frac{m\omega}{(\varphi+\omega)} \tag{11}$$

The defender has a mixed optimal strategy of A and B. Now, let us adopt these concepts for our discrete 2×2 game matrix, by defining $x_1 = [x_0]$ and we obtain.

$$\begin{bmatrix} a(x_1,A) & a(x_1,B) \\ a(x_1+1,A) & a(x_1+1,B) \end{bmatrix} \tag{12}$$

If $a(x_1,\mathrm{A}) \le a(x_1,\mathrm{B})$, we have pure strategy solutions for both the players otherwise only the attacker has a pure strategy solution while the defender has a mixed strategy solution.

It is observed that modelling the decisions using concepts of probability seems very convenient, however, in many realistic situations, real problems associated with human judgment about uncertainties and beliefs about adversaries cannot be modelled effectively using the probabilistic approach. We propose a belief functions framework as a methodology to model the players' behaviour and decision making.

5. MODELLING THE BEHAVIOUR OF PLAYERS WITH UNCERTAIN INFORMATION USING BELIEF FRAMEWORK

In many practical situations, probability theory is not accepted as a suitable language of uncertainty. Probability estimation requires consistent, significant and non-conflicting data in sufficient quantity and behavioural observations of the individuals. If this internal consistency is not met, equal probability is assigned to alternative states, resulting in random events. In real situations, decisions are modelled to arrive at different sets of alternatives, which is not possible under the probability framework. The expected utility under belief function gives an interval for the expected payoff instead of a single point estimate. Under this approach, the decision maker takes a conservative approach and makes decisions based on the most unfavourable resolution of ambiguity.

In this section, as an evolutionary development of belief framework, behaviour of players is modelled by adding thinking, reasoning and logic planning engine (TR&LP Engine) with experience-weighed attraction (EWA) algorithm[27].

The proposed algorithm based on EWA learning method processes all kinds of state information by logical thinking, then generates processed results to drive behavioural modelling by setting the parameters to adopt to the changing environment. This is done by accumulating new environment experience into the engine, which is what differentiates the belief framework from the traditional pre-programmed ones.

In view of the fact that the game formulation incorporates uncertain information sets of the computational players, they are required to make higher level of strategic thinking to update their beliefs with respect to the previous moves made by their opponents in order to make better moves and achieve higher expected values. This is represented as a tuple

$T = \left\langle \mathrm{P}, \mathrm{A}, \pi_t^i \times \pi_t^j \right\rangle$

where:

P= {Attackers i, Defender j} is the set of players;

$\mathrm{A} = \mathrm{A}_i \times \mathrm{A}_j$, are the set of possible actions of the players;

$\pi_t^i \times \pi_t^j$, Payoff functions for players i and j respectively, are such that $\pi_t^x(a_x)$ denotes the payoff of player x at time t when he chooses action a according to the distribution $a \in \mathrm{A}$.

5.1 Player at Level$_0$-Thinking (L$_0$-T): Pre-Game Thinking

At Level$_0$, each player x knows his own actions a_x, but is uncertain about the decisions of his opponent. As the game progresses, the players swap their turns in making their possible moves, which results in sequences of $\{a_0, a_1, \ldots\}$. After the initial move a_0 has been made, the player who is supposed to make the next move a_t decides whether to accept the move made by his opponent and withdraw from the game or to make a counter-move a_{t+1}. At this level, the player x constructs Level$_0$ beliefs $b_x^{(0)} : \mathrm{A} \rightarrow [0,1]$ about the likelihood $b_x^{(0)}(a)$ that his decision will be accepted by his opponent. With these means, the player can estimate the value of continuing the game by making a move a , where he would randomly select a move $a_t^* \in \mathrm{A}$ that would fetch him higher expected payoff.

$$\begin{aligned} a_t^* &:= \max_{a \in \mathrm{A}} U_x^{(0)}(a, b_x^{(0)}) \\ &= b_x^{(0)}(a_x) \times \pi_t^x(a_x) + (1 - b_x^{(0)}(a)) \times \pi_t^x(a) \end{aligned} \tag{13}$$

After the initial move of the game, the player decides on the action that he believes will fetch him a better outcome, according to the response function given below

$$\begin{aligned} &L_K - T(a_{t-1}) \\ &= \begin{cases} a_t^* & \text{If } U_x^{(0)}(a_t^*, b_x^{(0)}) > \pi_{t-1}^x(a_x) \\ \text{accept} & \text{If } \pi_{t-1}^x(a_x) \geq U_i^{(0)}(a_t^*, b_i^{(0)}) \\ \text{withdraw} & \text{Otherwise} \end{cases} \end{aligned} \tag{14}$$

Equation (14) shows that if the player at $L_0 - T$ believes that the move a_t^* which he believes will fetch him a better expected payoff than either withdrawing from the game or accepting the move $a_{-i}(t-1)$, player i will make a countermove a_t^* to the move $a_{-i}(t-1)$. On the other hand, if the player believes that the move a_t^* does not satisfy these conditions and might incur him a negative payoff, but accepting the move $a_{-i}(t-1)$, will fetch him a better outcome than withdrawing from the game, the player accepts the move $a_{-i}(t-1)$. In all other cases, the $L_0 - T$ player withdraws from the game.

5.2 Player at LevelK- Thinking $L_K - T$: Higher Level Thinking

The $L_K - T$ allows player x to judge his moves from the perception of his opponent in order to predict the opponents' future moves. Provided with the uncertain information about his opponent, the player at $L_K - T$ forms beliefs about the decisions of his opponent with the confidence $c^{(K)} \in [0,1]$ and player specific learning speed given by $\lambda^{(K)} \in [0,1]$. The other is experience weight $N(t)$, equivalent to the observation of past experience with respect to present experience, $N(t-1)$ multiplied by attenuation coefficient φ , added to an incremental value 1 , i.e., $N(t) = \varphi. N(t-1) + 1$. The player also constructs Level$_K$ beliefs $b_x^{(K)} : \mathrm{A} \rightarrow [0,1]$ about the likelihood $b_x^{(K)}(a)$ that his decision will be accepted by his opponent with the aid of feedback function $\delta^{(K)}$. Before the attack could progress, the player gets some reward of $b_x^{(K)}(a) \times U_i^{(K)}(a)$, which is the basic reward. After a successful attack (wherein his attacks go unnoticed by the defender), the attacker receives an additional payoff of $\left(1 - b_x^{(K)}(a)\right) \times U_i^{(K)}(a)$. But if the attack is unfortunately a failure, then the player will not receive this additional payoff and will be left out with first part of the reward. If he has not planned any attack action at the given time step, due to which the network traffic is normal, then he receives a payoff $U_i^{(K)}(a) = 0$ .In this way, each additional level of thinking allows the player to consider an additional model of opponent behaviour. Based on $L_K - T$, the player formulates the expected value of making a move $a \in \mathrm{A}$ combined with the expected payoff of other players at $L_{(K-1)} - T$ according to

$$a_t^* := \max_{a\in A} U_x^{(K)}(a) = \left[\frac{\left(1-c^{(K)}\right)\times\left(1-\lambda^{(K)}\right)\times \varphi . N(t-1)\times U_x^{(K-1)}(a)}{N(t)}\right] + \delta^K \sum_{a\in A}\left[\frac{b_x^{(K)}(a)\times U_i^{(K)}(a)}{N(t)}\right] + \left[\frac{\left(1-b_x^{(K)}(a)\right)\times U_i^{(K)}(a)}{N(t)}\right] \tag{15}$$

This yields the following response function

$$L_K - T(a_{t-1}) = \begin{cases} a_t^* & \text{If } U_x^{(K)}(a_t^*, b_x^{(K)}) > \pi_{t-1}^x(a_x) \\ \text{accept} & \text{If } \pi_{t-1}^x(a_x) \geq U_i^{(0)}(a_t^*, b_i^{(K)}) \\ \text{withdraw} & \text{Otherwise} \end{cases} \tag{16}$$

Belief theory builds in suitable principle that actions with higher expected payoff are chosen more often on the basis that, players ‘better respond’ rather than ‘best response’. This is done by relaxing the assumption that players choose the best action by incorporating the property that all actions are chosen with strict positive probability, calculated as follows

$$\mu_{a_x^*}^t = \frac{U_x^{(K)}(a_x^*)^{\theta^t}}{\sum_{K=1}^{A_x} U_x^{(K)}(K)^{\theta^t}} \tag{17}$$

where $\mu_{a_x^*}^t$ is the probability of player x, selecting action a_x^* and the parameter θ^t controls the sensitivity of probability distribution to the expected value for each action.

5.3 Learning from Observations

As $L_K - T$ players updates his beliefs, he also updates his confidence scores in higher level thinking c_K, to reflect the behaviour of his opponent at each level. This is achieved through

$$c^{(K)} := \left(1-\lambda^{(K)}\right) . c^{(K)} + \lambda^{(K)} \times \frac{1+\dfrac{\varphi . N(t-1)\times U_x^{(K-1)}(a)}{N(t)}}{1+\delta^K \sum_{a\in A}\left[\dfrac{b_x^{(K)}(a)\times U_i^{(K)}(a)}{N(t)}\right] + \left[\dfrac{\left(1-b_x^{(K)}(a)\right)\times U_i^{(K)}(a)}{N(t)}\right]} \tag{18}$$

In this way, the player updates his confidence level at each level of thinking that is expected to fetch him a better outcome to the move $a_{(t-1)}$, made by the opponent and evaluated against the decision that the player himself would have made, if he had been a $L_{K-1} - T$ player, in the situation of his opponent.

6. SIMULATION AND ANALYSIS

6.1 Dataset and the experimental environment

Basic datasets DARPA and KDDCUP99 is used for our testing, vulnerability analysis and feature selection. KDDCUP99 dataset is built on the traffic captured by DARPA, which have various intrusions. Each flow is characterised by 41 parameters and labelled as normal or attack of a specific type, which includes denial of service (DoS) attack, user to root attack (U2R), remote to local attack (R2L), and probing attacks[28].

Test-bed Simulation

Once the test-bed scenario of Figs. 1 and 2 is setup, various cyber threat scenarios are created and executed by running the simulations. The time records of normal and abnormal traffic flow along with the indication of attack success and failure for the chosen attack type is depicted in the Table 1. For example time period between 15 to 19 signifies normal traffic, while that between 20 to 22 signifies traffic of attack data which the defender failed to identify, whereas the attack data at time 29 and 31 signifies the traffic that has been identified by the defender. By accumulating the history of network attack scenario, players decision making process under uncertainty has been studied using probability framework and belief function framework.

6.2 Vulnerability Analysis of the Network System based on Probabilistic Framework

For the given test-bed setup, attack and normal flows are generated at each time instant. An important objective is to study the decision accuracy of choosing each action under uncertainty with probabilistic framework as depicted in Fig. 3.

Decision accuracy is considered as correctly guessing which of the given options is better, such that it will yield an optimal solution. Combining a guess into a consensus decision through maximisation rule will result in decision accuracy within the range specified in Eqn (7).

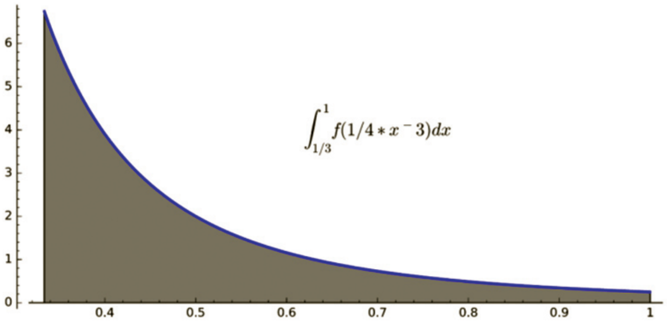

Figure 3. Decision Accuracy for game under uncertainty using probabilistic framework.

6.2.1 Behavioural Analysis

Attackers explore the vulnerabilities of the network system to gradually gain privileges and exploit the system. Modelling a system which generates, analyses and generates recommendation strategies for security measures and interaction with the adverse environment lies in the effectiveness of the finite automaton it is built upon. A non-deterministic finite automaton is defined as $A = (S, \pi, e, C)$, where

S is a finite set of system states

π is a finite set of input sequence

e is the exploit which measures the vulnerabilities and is modelled as transition function: $S \times \pi \rightarrow P(e)$, which is the probability of potential exploits.

C is the acceptance condition for the sequences of input string, S_i , $\forall\, i \geq 0$.

Accordingly, for any exploit measure e_i , the probability $P(e_i)$ uses access complexity (AC) metric[29] which describes the computation of the described vulnerability as follows:

$$P(e_i)\begin{cases} \text{score=0.35,} & \text{value=High(H)} \\ \text{score=0.61,} & \text{value=Medium(M)} \\ \text{score=0.71,} & \text{value=Low(L)} \end{cases}$$

This metric measures the complexity of the attack required to exploit the vulnerability once the attacker has gained access to the target system. The lower the required complexity, the higher the vulnerability score. For the attack scenario setup discussed in section 4.1, a time point between 1 and 2 recorded by the network sniffer indicates the attack type to be 'Neptune' which is a Dos attack. In this case, the affected configuration is highly vulnerable and is very rarely seen in practice, because the attacking team have elevated privileges and spoof additional system in addition to the attacking system. So the exploit measure for this type of attack is 0.35. The time point between 4 and 5 indicates the attack type to be probing in which the affected configuration is non-default and is not commonly configured. In this case since the attacking team is limited to a group of system at some level of authorisation, the vulnerability score is medium with the exploit measure 0.61. The time point between 8 and 9 indicates R2L attack type wherein the affected configuration is default or ubiquitous and comparably less vulnerable with exploit measure 0.71. The time table of the respective attack types is shown in Table 2.

For the negotiation game, let us assume 12 interactions between two sets of players (attacker and defender). Provided with the uncertain game environment, the attacker chooses over the attack types at each interaction. The attack types provided to the attacker during the game are: DDoS attack, probing attack and R2L attack. With the knowledge on the vulnerability levels and exploit measures of each of these attacks, the player selects the attacks with the confidence. On the other hand the defender decides whether to attack or not to attack. Thus for the given number of interactive sessions, the confidence score of the players is analysed for different attack and defence strategies according to Eqn (12). For example, if the attacker chooses the attack type 'Neptune' during the first interaction, then he succeeds in his attacks with the probability, $\varphi = 0.35$, if his attacks go undetected by the defender. But if the attack get detected by the defender, then the attacker runs a risk of $\delta = 0.9$, then probability of succeeding in the attack is $\omega = 0.035$. Similarly the game is proceeded for, $m = 12$ interactions and the confidence with which the players make decision under uncertainty about their opponents is depicted in Fig. 4.

6.3 Vulnerability Analysis of the Network System based on Belief Framework

For the given test bed setup, time periods with normal traffic data and attack traffic date is captured using Wire Shark tool to study the players' decision making process under uncertainty with belief framework. If the attacker's previous moves have succeeded, then $b(t-1)$ is set to 1 , else it is set to 0 . But, since the decisions are made under uncertainty with no preferential biases, the probability of successful and failed actions is initially set to 0.5 along with the feedback function δ and the coefficient λ , which signifies the player's learning speed about his opponent.

With the above settings and test-bed setup, time periods with normal traffic data and attack traffic date is captured using Wires hark tool to study the players' decision making process under uncertainty with belief framework. The expected payoff obtained by choosing an action x , at each time step as depicted in Fig. 5.

The probability of action x selected at each successive time strikes with varying levels of sensitivity increases over each trial as shown in Fig. 6.

6.3.1 Confidence Analysis

A negotiation game was modelled and simulated between two sets of players (attacker and defender) where each player was made to negotiate with either a $L_0 - T$, $L_1 - T$, $L_2 - T$ or a $L_3 - T$ player. The order in which the players encounter these different opponents is counterbalanced across the players. Since the game is a representation of imperfect information, the chance events at the initial stage of the game is programmed 'nature's moves', where the initiator was randomly decided. In consequent games, the players swapped in the role of initiator. The $L_0 - T$, players were initialised by playing randomly

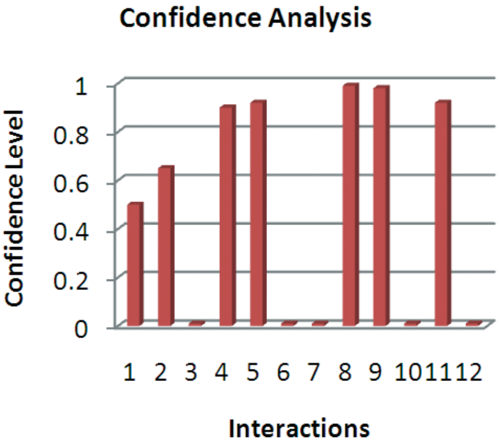

Figure 4. Behaviour analysis of players using probability framework.

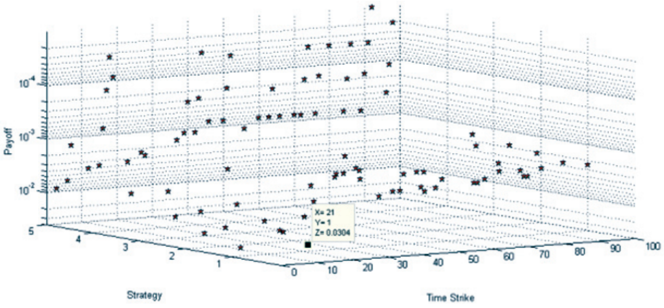

Figure 5. Attacker's expected payoff obtained for each attack action.

Table 1. Time table of attack actions.

Time	Duration	Protocol_ Type	Service	Flag	Src_ Bytes	Dest_ Bytes	Land	Wrong_ Frag	Urgent	Hot	num_failed_ logins	logged_ in	num_ compromised	Root_ shell	Su_ attempted	Attack type
1	0	tcp	private	REJ	0	0	0	0	0	0	0	1	0	0	0	**neptune**
2	0	tcp	private	REJ	0	0	0	0	0	0	0	1	0	0	0	**neptune**
4	0	icmp	eco_i	SF	20	0	0	0	0	0	0	0	0	0	0	**saint**
5	1	tcp	telnet	RSTO	0	15	0	0	0	0	0	0	0	0	0	**mscan**
8	0	tcp	telnet	SF	129	174	0	0	0	0	1	0	0	0	0	**guess_password**
9	0	tcp	ftp	SF	26	157	0	0	0	0	1	0	0	0	0	**guess_password**

Table 2. Time table of attack types.

Time	Duration	Protocol_ Type	Service	Flag	Src_ Bytes	Dest_ Bytes	Land	Wrong_Frag	Urgent	Hot	num_failed_ logins	logged_in	num_ compromised	Root_ shell	Su_attempted	Attack type
15	37	tcp	telnet	SF	773	354200	0	0	0	0	0	1	0	0	0	**normal**
16	0	tcp	http	SF	350	3610	0	0	0	0	0	1	0	0	0	**normal**
17	0	tcp	http	SF	213	639	0	0	0	0	0	1	0	0	0	**normal**
18	0	tcp	http	SF	246	2090	0	0	0	0	0	1	0	0	0	**normal**
19	0	udp	private	SF	43	44	0	0	0	0	0	0	0	0	0	**normal**
20	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0	0	**neptune**
21	0	tcp	idap	REJ	0	0	0	0	0	0	0	0	0	0	0	**neptune**
22	0	tcp	pop_3	SO	0	0	0	0	0	0	0	0	0	0	0	**mscan**
29	0	icmp	ecr_i	SF	520	0	0	0	0	0	0	0	0	0	0	**smurf**
30	0	udp	private	SF	54	51	0	0	0	0	0	0	0	0	0	**normal**
31	805	tcp	http	RSTR	76944	1	0	0	0	0	0	1	0	0	0	**apache2**

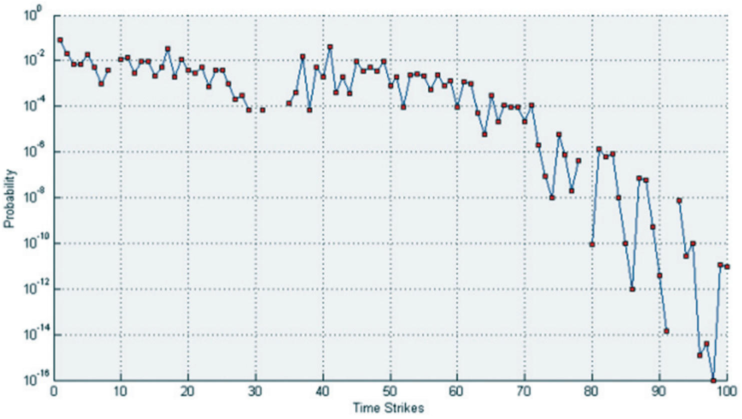

Figure 6. Probability distribution for each action being selected for next strike.

generated games against an $L_0 - T$ attacker player. At the start of each game, the player’s beliefs were reset to its initial state to compute the performance of the defenders

The moves of the players and his confidences c_K in the $L_K - T$ is observed and recorded accordingly. These confidences c_K give insight in whether the behaviour of the players is more symptomatic of $L_0 - T$, $L_1 - T$, $L_2 - T$ or a $L_3 - T$. For each level of thinking, Fig. 7, shows how similar players moves were to the moves of each of the $L_0 - T$, $L_1 - T$, $L_2 - T$ or a $L_3 - T$. purple points shows similarity of players moves to $L_0 - T$, green points indicate similarity of players moves to $L_1 - T$ and red and blue points show similarity to $L_2 - T$ and $L_3 - T$. Figure 7 also shows that players moves are more similar to $L_1 - T$, $L_2 - T$ and $L_3 - T$ than they are to $L_0 - T$.

In this game, both $L_0 - T$ and $L_1 - T$ players make moves that were believed to be accepted by their opponent. In contrast, $L_2 - T$ and $L_3 - T$ players tend to make decisions to alter the beliefs of their opponent. Due to which the early moves of $L_0 - T$ and $L_1 - T$ players were more favourable to their opponent and those made by $L_2 - T$ and $L_3 - T$ players, whose moves were favourable to themselves than their opponents. This signifies that, players make moves that are more consistent with $L_2 - T$ and $L_3 - T$ when their opponent is capable of $L_2 - T$ and $L_3 - T$ as well. Since the game is played under uncertainty, players had an understanding that they would confer with varying number of opponents, but they are unaware of their opponents with different $L_K - T$ abilities. The results obtained from these experimental games confirm that players can benefit from the use of $L_K - T$.

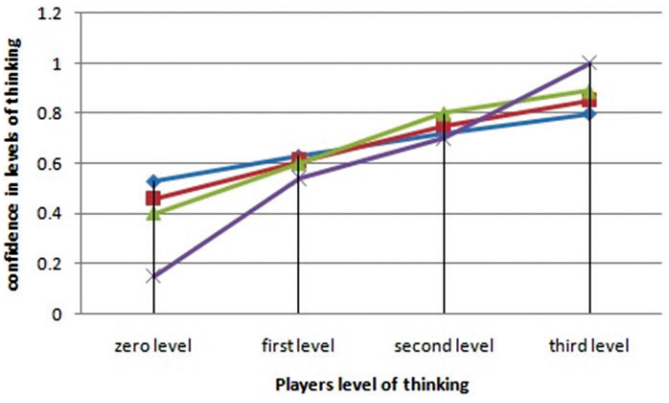

Figure 7. Confidence analysis of players using belief framework.

7. DISCUSSION AND CONCLUSIONS

National critical infrastructure is increasingly becoming a vulnerable asset in cyber-space. Training for risk assessment and mitigation requires the design and development of cyber warfare test-bed that models the attackers and defenders of such assets in cyberspace. In the present work, we model the behaviour of the players with incomplete and uncertain information and their decision making based probabilistic and belief frameworks. It is observed that the belief function model which uses higher level of thinking differs from the probabilistic models in that the behaviour of the player changes based on the observed behaviour of their opponents. We have investigated the interactions between the computational players under belief framework with higher level thinking can help in providing better framework to represent the uncertainties and thus obtaining better payoff instead of a single estimate as in probabilistic framework. In a negotiation experiment, we simulated interactions between the players and found that in contrast to strict probabilistic setting, reasoning using belief functions with higher level thinking helps to stabilise mutually beneficial interaction. In the belief setting, we let the players of different levels of thinking alternate to interact with each other under uncertainty. This represents the players’ the behaviour which helps in optimising one’s own behaviour. These results suggest that the belief framework which uses higher level thinking in computational players play a useful role in training the people in cyber war game setup to negotiate adversaries to expect better outcomes.

REFERENCES

1. Amoroso, Edward G. Cyber attacks: Protecting national infrastructure, BH, Elsevier, 2010.
2. Cyber attacks on critical infrastructure insights from wargaming. https://warontherocks.com/2017/07/cyber-attacks-on-critical infrastructure-insights-from-war-gaming/ (Accessed on 21 September 2017).
3. Cyber attacks against critical infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Accessed on 21 September 2017).
4. The real cyber threat. http://www.thehindu.com/opinion/lead/lead-article-by-mk-narayanan-on-aadhaar-bill-the-cyberthreat-is-very-real/article8371335.ece (Accessed on 21 September 2017).
5. The national security case against Aadhaar. https://thewire.in/118541/national-security-case-aadhaar/[Accessed on 21 September 2017].
6. Gueye, Assane. A game theoretical approach to communication security. University of California, Berkeley, 2011; (PhD Thesis).
7. Lin, F.Y.S.; Yen, H.H. & Chen, P.Y. Maximization of network survivability considering degree of

disconnectivity. *In* Proceedings of 7th International Wireless Communications and Mobile Computing Conference, June 2011.

8. Alpcan, T. & Baser, T. Network security: A decision and game-theoretic approach. 1st ed. Cambridge University Press, November 2010.
9. Alpcan, T. & Baser, T. A game theoretic analysis of intrusion detection in access control systems. *In* Proceedings of the 43rd IEEE Conference on Decision and Control, 2004.
10. Shiva, S.; Roy, S. & Dasgupta, D. Game theory for cyber security. *In* Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. ACM. New York, USA, 2010. doi: 10.1145/1852666.1852704.
11. Roy, S.; Ellis, C.; Shiva, S. ; Dasgupta, D. ; Shandilya, V. & Wu, Q. A survey of game theory as applied to network security. *In* 43rdHawaii International Conference on System Sciences, 2010. doi: 10.1109/HICSS.2010.35.
12. Shiva, S.; Roy, S.; Bedi, H.; Dasgupta, D. & Wu, Q. A stochastic game model with imperfect information in cyber security. *In* 5th International conference on i-warfare and security (2010).
13. Tadelis, S. Game theory: An introduction. Princeton University, 2013. ISBN: 9780691129082.
14. Duncan, R.D. & Raiffa, H. Games and decisions: Introduction and critical survey. Courier Corporation, 1957. ISBN: 9780486659435.
15. Ravishankar, M.; Rao, D.V. & Kumar, C.R.S. A game theoretic approach to modelling jamming attacks in delay tolerant networks. *Def. Sci. J.,* 2017, **67**(3), 282-290. doi : 10.14429/dsj.67.10051
16. Ramirez-Marquez, J.E.; Rocco, C.M. & Levitin, G. Optimal network protection against diverse interdictor strategies. *Reliability Eng. Sys. Safety*. 2011, **96**(3), 237–282.
17. Chen, P.Y.; Shih, I.J. & Lin, F.Y.S. Maximization of multi-round network survivability under considerations of the defender's defensive messaging strategies. *In* International Conference on MOBILe Wireless MiddleWARE, Operating Systems and Applications, 2013.
18. Bier, V.M.; Oliveros, S. & Samuelson, L. Choosing what to protect: Strategic defensive allocation against an unknown attacker. *J. Public Economic Theory*, 2007, **9**(4), 563–587.
19. Dighe, N.S.; Zhuang, J. & Bier, V.M. Secrecy in defensive allocations as a strategy for achieving more cost-effective. *Int. J. Performability Eng.*, 2009*,* **5**(1), 31-43.
20. Shafer, G. & Kaufmann, M. Readings in uncertain reasoning. 1990.
21. Colbert, E. & Kott, A. Cyber-security of SCADA and other industrial control systems. *In* Proceedings of 12th International Conference on Cyber warfare and Security, USA, 2017.
22. Sommestad, T. & Hallberg, J. Cyber security exercises and competitions as a platform for cyber security experiments. *In* Secure IT Systems. Edited by Jøsang A., Carlsson B. NordSec 2012. Lecture Notes in Computer Science. *Springer*, Berlin, Heidelberg, **7617**. doi: 10.1007/978-3-642-34210-3_4
23. Siaterlis, C.; Perez-Garcia, A. & Masera, M. Using an emulation Test-bed for operational cyber security exercises. ICCIP 2011: Critical Infrastructure Protection V pp. 185-199. doi: 10.1007/978-3-642-24864-1_13
24. Kennedy, D.; O'Gorman, J. & Kearns, D. Metasploit: The penetration tester's guide. No Starch Press, 2011. ISBN: 978-1593272883.
25. Chappel, L. Wireshark network analysis: The official Wireshark certified network analyst study guide. Chappel University, 2012.
26. Berger, James O. Statistical decision theory: Foundations, concepts, and methods. Springer Science & Business Media, 2013.
27. Ingre, Y. & Yadhav, A. Performance analysis of NSL-KDD dataset using ANN. *In* Proceedings of 2015 International Conference on Signal Processing and Communication Engineering Systems (SPACES). doi: 10.1109/SPACES.2015.7058223.
28. Colin, C. & Ho, T. Experience-weighed attraction learning in normal form games. *Econometrica*, 1999, **67**(4), 827-874.
29. Vulnerability metrics. https://nvd.nist.gov/vuln-metrics/cvss (Accessed on 21 September 2017).

ACKNOWLEDGMENTS

The authors would like to gratefully acknowledge Dr Srinivasan Vathsal and anonymous reviewers for fruitful discussions, suggestions and reviews.

CONTRIBUTORS

Ms Monica Ravishankar is pursuing her PhD from Defence Institute of Advanced Technology, Pune. Her research interests include: Operations research and game theory.
Contribution in the current study; she designed of mathematical model, simulation and analysis of data and preparation of the manuscript.

Dr D. Vijay Rao obtained his MS (Engg) and PhD from IISc Bengaluru. Currently working as a Scientist with the Institute for Systems Studies and Analyses, Delhi. His areas of specialisation include: Military Systems analysis, design and development of wargames and strategic systems, modelling and simulation of warfare systems and military operations analysis.
Contribution in the current study; he initiated the work, contributed in the design and analysis of data and preparation of the manuscript.

Dr C.R.S. Kumar obtained his MTech from IIT Madras and PhD from University of Melbourne. Currently working as faculty member of Defence Institute of Advanced Technology, Pune. His areas of specialisation include: Jamming/anti-jamming, game theory and cognitive radios networks.
Contribution in the current study; he provided logistic support required for the research