Enhancing the Network Security Using Lexicographic Game

T.P. Anithaashri[1] and R. Baskaran[2]

[1] Anna University, Chennai / VEC – Chennai
thiruani@yahoo.com
[2] Anna University, Chennai
basski@annauniv.edu

Abstract. This paper presents a new modeling method to enhance the network security using game theory. Reconnaissance is applied as a game strategy to obtain more information about the enemy's strategic intentions.Indefinite Event Nets method is used to model the framework and analyze to defend the network attacks. The game issues are solved with the help of Indefinite Key Nets. The course of action for a player in multi-player game environment is also determined. Finally, the Nash equilibrium is computed and best-response strategies for the players (administrator and attacker) are found. It proves how the strategies are realistic and how the administrators can use these results to enhance the security of their network.

Keywords: Repeated game, Reconnaissance, Indefinite Event Nets, Indefinite Key Nets, Game Theory, Lexicographic game, Nash Equilibrium, Network Security.

1 Introduction

Now a days, schools, retailers, banks, Government agencies and a growing number of goods and service providers use the Internet as their integral way of conducting daily business. As an access to the Internet, the individuals either good or bad, can easily connect to the Internet. Due to the ubiquity of the Internet, computer security has now become more important than ever to organizations such as governments, banks, and businesses. Security specialists have long been interested in knowing what an intruder can do to a computer network, and what can be done to prevent or counteract attacks. In this paper, how the game theory can be used to find strategies for both an attacker and the administrator. Let us consider an example of a local network connected to the Internet and consider the interactions between an attacker and the administrator and treating it as a general-sum stochastic game.

The proposed system can find the strategy between the attacker and the administrator with the help of a finite repeated game or infinite repeated game. It also help us to know more information about the attacker's strategic intensions through the concepts of reconnaissance, which is the best strategy among all other game strategies. It can be coded with NLP-1 in MATLAB, that is mathematical computation software package by The Math Works, Inc. and thus the Nash equilibrium solution can be obtained.

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 211–224, 2012.

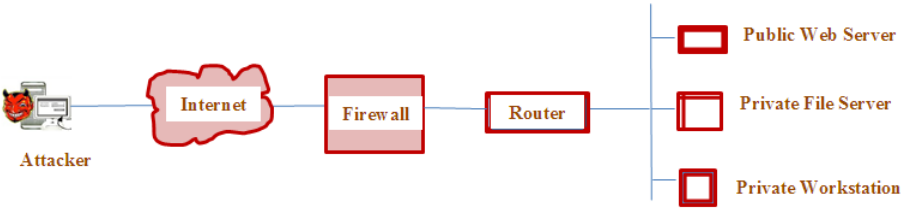

Fig. 1. Network Example (Attacker & Administrator)

2 Related Work

The concept of game technique has been invited to the field of network security and computer security. The literature [1] addresses the problems of false report injection and DoS attacks in wireless networks. This scheme can drop false reports much earlier even with a smaller size of memory. In literature [2], the new framework to detect malicious nodes using zero-sum-game approach and selective node acknowledgements in the forward data path. It proposes a new protocol for preventing malicious bandwidth consumption and demonstrates how game techniques can be successfully used to verify availability-related security properties of network protocols. The network is scanned and mapped for all access points and WLAN nodes in paper [3]. It was focused on many countermeasures and less in feasibility. The literature[4] analyzed the risk assessment of network security and design the new framework by using network prototype. The Stackelberggame technique was used to analyse the payoff functions and Nash equilibrium strategies with payoffs for the malicious users has been adopted in the paper [6]. To analyze the intrusion detection in Mobile Adhoc-Networks , the two-player non-cooperative game technique has been used in the literature [7]. Performance of intrusion detection has been examined for Unix based host machines with Solaris operating system using Markov chain model in the paper [8]. The continuous markov chain model for a homogenous finite state has been utilized to evaluate the system security in the literature [9]. In literature [11], the method of game technique to analyze the security of computer networks was presented. The interactions between an attacker and the administrator are modeled as a two player game for which best-response strategies were computed.

3 Networks as an Indefinite Event

In this section we introduce formal model of anindefinite event . A two-player model is described by a 5-tuple vector as $I=(Z,A^k,H,F^k,\delta)$ where $Z=\{\alpha_1,\alpha_2,\ldots,\alpha_N\}$ is a finite set of states, $P^k=\{a_1^k,a_2^k,\ldots,a_M^k\}$, k=1,2, $I^k=|P^k|$ is the action set of player k. The action set for player k at state s is a subset of P^k. i.e., $P_s^k$is contained in or equal to $P^k$and$\upsilon_{i=1},\ldots,_N P\alpha_i^k=P^k$. $Q:Z \times P^1 \times P^2 \times Z \rightarrow [0,1]$ is the state transition function. $F^k: Z \times P^1 \times P^2 \rightarrow F$, k=1,2 is reward function of player k. $0\leq\delta\leq1$ is a discount factor for discounting future rewards. At the current state the reward worth its full value, but the reward for the transition from the next state is worth δ times its value at the current state.

The event is played as follows : at a discrete time instant t, the event is in state z_t € Z. Player 1 chooses an action p_t^1 from P^1 and player 2 chooses an action p_t^2 from P^2. Player 1 then receive a reward $f_t^1 = F^1(z_t, p_t^1, p_t^2)$, and Player 2 gets a reward $f_t^2 = F^2(z_t, p_t^1, p_t^2)$. The game then moves to a new state z_{t+1} with conditional probability $G(z_{t+1}|z_t, a_t^1, a_t^2)$ according to $H(z_t, p_t^1, p_t^2, z_{t+1})$.

We are interested in determining a course of action for a player in multi-players environment. Specifically we want to learn a stationary though possibly stochastic strategy that maps states to a probability distribution over its actions. The goal is to find such a strategy that maximizes the player's discounted future reward. For this reconnaissance is used as a game of strategy.

3.1 Reconnaissance

The reconnaissance is used to obtain information about the enemy's strategic targets. The advisability of reconnaissance before attack can be investigated by considering the problem as a game of strategy. Let us consider that the attacker and defender has two strategies. Assuming that the attacker, wishes to seize a defended enemy position. For simplicity, let us assume that he has two courses of action, namely

1. Attack with his entire force;
2. Attack with part of his force, leaving the remainder as reserves and a rear guard in case the enemy "outflanks" him.

The defender, is assumed to have two possible courses of action, namely :

i. Defend with his entire force the objective of the attacker;
ii. Defend with part of his force, and send the remainder to "outflank" the enemy and attack the enemy from the rear.

There are four possible outcomes of the above courses of action. They can be summarized by the following 2x2 matrix :

$$A = \begin{array}{c} \\ 1. \\ 2. \end{array} \begin{array}{c} \begin{array}{cc} \text{i.} & \text{ii.} \end{array} \\ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \end{array}$$

a_{21}represents the value to attacker if he attacks with part of his force and defender defends with his entire force. Suppose the outcomes are such that if defender uses strategy (i), then attacker would prefer to use strategy (1), and i.e, $a_{11} > a_{21}$ and if defender uses strategy (ii), then attacker would prefer to use strategy (2). Clearly the attacker could benefit from a knowledge of the defender's intentions. Thus the attacker might find it profitable to send out a detachment of men to reconnoiter in an attempt to discover the plans of the defender. In order to defend himself against such possible action the defender may take countermeasures. Now if the attacker decides to reconnoiter he must sacrifice some of his attacking forces. If the defender decides to take countermeasures he must sacrifice some of his defensive forces. A strategy for the attacker will be a set of instructions which tell him how to act taking into

account the information he may receive. Thus by using reconnaissance the information relevant to the enemy's strategic objective can be obtained.

A strategy is also called a mixed or randomized strategy, which means that the player chooses an action in random manner. The set of mixed strategies includes the pure strategies, when the player chooses the actions in a deterministic way. A pure strategy is a special case of mixed strategy such that probability one is assigned to one action and zero to all other actions. A stationary strategy π^k is a strategy that is independent of time and history. A mixed or randomized stationary strategy is one where $\pi^k(s,a)>0$, $s \epsilon S$ and $a \epsilon A^k$ and a pure strategy is one where $\pi^k(s,a_i) = 1$ for some $a_i \epsilon A^k$. Indefinite games can be classified according to the structure of their payoff functions. Two common classes of games are purely collaborative and purely competitive games. Purely collaborative games are ones where all the players have the same reward function. Purely competitive, or zero-sum, games are two-player games where one player's reward is always the negative of the other's. Like matrix games, zero-sum stochastic games [5] have a unique Nash-equilibrium, although finding this equilibrium is not so easy.

Nash equilibrium is a steady state of the play of a strategic game in which each player holds the correct expectation about the other player's behavior and act rationally. It does not attempt to examine the process by which a steady state is reached.

Since a set of strategy is used in Nash equilibrium, no player has incentive to unilaterally change her action. In equilibrium state , a change in strategies by any one of them would lead that player to earn less than if she remained with her current strategy. For games in which players randomize (mixed strategies), the expected or average cost must be at least as large as that obtainable by any other strategy.

3.2 Indefinite Key Nets

Indefinite Key Nets are augmented with the set of average transition rates for the exponentially distributed transition firing times. A transition represents a class of possible changes of markings. Such a change, also called transition firing, consists of removing tokens from the input places of the transition and adding tokens to the output places of the transition according to the expressions labeled on the arcs. A transition may be associated with an enabling predicate which can be expressed in terms of the place marking expressions. If the predicate of a transition evaluates to be false, the transition is disabled. In this model, transitions can be categorized into two classes: transitions of Class One are used to represent logical relations or determine if some conditions are satisfied [3].This class of transitions is called immediate transition with zero triggering time.

Transitions of class two are used to represent the operations on the tasks or information processing. This class of transitions is called timed transition with exponential distributed firing time. A marking in this model represents a distribution of tokens in the model. The state space of a model consists of the set of all markings reachable from the initial marking through the occurrence of transition firing. An Indefinite Event net is homomorphism to a continuous time Markov Chain (MC), and there is a one-to-one relationship between markings of the key net and states of the MC [3] and [4].

Indefinite Key Net is a quadruple (S, T, F, λ) where

(1) S is a finite set of states
(2) M is a finite set of moves ($S \cap M \neq \Phi$)
(3) F Contained in or equal to (S x M) U(MxS) is a set of arcs
(4) $\mu = (\mu_1, \mu_2, .., \mu_n)$ is a set of triggering states of transitions.

As an extension of Indefinite Key Nets, Indefinite Incentive Net is a powerful graphical and mathematical tool, which not only is able to model concurrent, asynchronous and nondeterministic events, but also provide transition enabling function and firing probability that can be used to model various algorithms and strategies.

From a structural point of view, both net formalisms are equivalent to Turing machines. But the incentive net provide enabling functions, marking dependent arc cardinalities, a more general approach to the specification of priorities, and the ability to decide in a marking-dependent fashion whether the triggering time of a transition is exponentially distributed or null, often resulting in more compact nets. Perhaps more important, though, are the differences from an indefinite modeling point of view. The incentive net formalism considers the measure specification as an integral part of the model. Underlying this net is an independent semi Markov process with incentive rates associated to the states and incentive impulses associated to the transitions between states [5].

3.3 Indefinite Event Nets

An Indefinite Event Net is the 9-tuple vector $(P,S,M,\pi, A,I, \mu,\delta,I_0)$ where

1. P= 1,2,…,n denotes a finite set of players;
2. S is a ¯ finite set of states;
3. $M= M_1 UM_2 U \ldots U M_n$ is a finite set of moves, where M_k is the set of transitions with respect to player k, for $k \epsilon P$;
4. $\pi: M \rightarrow [0,1]$ is a routing policy representing probability of choosing a particular transition;
5. $A \underline{C} J U O$ is a set of arcs where $J \underline{C} (P \times M)$ and $O \underline{C} (M \times S)$, such that $S \cap M = \Phi$ and $S U M \neq \Phi$;
6. $I: M \rightarrow (I^{(1)}; I^{(2)}, ..., I^{(n)})$ is an incentive function for the player taking each action;
7. $\mu = (\mu_1, \mu_2, \ldots, \mu_k)$ is a set of triggering rates of transitions in transition set, where k is the number of transitions;
8. $\delta(s^k_i)$ is the utility function, when player k in the condition s_i. Accordingly, the player can choose the best transition;
9. $I_0$is the initial marking.

The Indefinite Event Net structure will represent all possible strategies existing within the game.

3.4 Triggering Rule

The Triggering rule of an Indefinite Event Net is given as follows. A marking m represents a distribution of the tokens in indefinite event. Each token s is related with

a reward vector $b(s) = (b_1(s),b_2(s),\ldots,b_n(s))$ as its properties. Each element of M represents a class of possible changes of markings. Such a change of t, also called transition triggering, consists of removing tokens from a subset of places and adding them to other subsets according to the expressions labeling the arcs. A transition t is enabled under a marking I_0whenever, for all $s\epsilon S$ and $(s,m)\epsilon A$, $I(s)\neq\Phi$. Each player gets the reward I(m) through the transition and the reward is recorded in the reward vector b of each token.

Following are the two steps to solve the Indefinite Event Net to find the Nash equilibrium. The Nash equilibrium corresponds to the optimized strategy[3] of each player. We first build the reachability tree according to the Indefinite Event Net, and then find out the Nash equilibrium.

3.5 Procedure to Build a Reachability Tree for Indefinite Event Net

A reachability tree is consists of nodes, which are denoted by all the reachable markings of the Indefinite Net, and the arcs among the nodes. From a Indefinite Net the initial marking I_0, the reachability tree can drawn with the following steps.

(i) Make I_0 the root r of the tree. No dex marked by I is a leaf if and only if there is no transition $m\epsilon M$ which is enabling under I, or there is a node $y \neq x$ along the road from r to x, which has a similar mark I' as I. Define I_1 and I_2 are the null set such that for all $s\epsilon S$.

(ii) If a node x marked by I is not a leaf, trigger a move m, $(s,m)\epsilon A$ to construct a new node in the reachability tree marked as I'.

Following the above steps, we can build the reachability tree from the Indefinite Net. The procedure is similar with that in Indefinite Key Nets.

3.6 Procedure to Find out the Nash Equilibrium

The algorithm is to find the Nash Equilibrium of an action sequence with $\pi^*$for all the players. For every leaf node x_i identified by I_i in the reachability tree and a token s such that there is a state s, $_{Ii}(s) = s_i$, $1 \leq i \leq n$ in the reachability tree.

Generally, there are multiple paths from the initial state to a leaf node. Assume x_i is a leaf node, and there are w_i separate paths from the root to xi. Let $t_1^{(i,w)}$,$t_2^{(i,w)}$,…,$t_K^{(i,w)}$, $K=k^{(i,w)}$ be the w^{th} path from root node to leaf node x_i. We define a leaf probability for the leaf node x_i of the w^{th} path as

$$f^{(w)}(x_i) = \pi(t_1^{(i,w)})\ \pi(t_2^{(i,w)})\ ,.,\pi(t_K^{(i,w)}) \tag{1}$$

Then the final utility vector for the system is

$$(U1,U2,\ldots,Un) = \quad \sum_{(i=1\ldots m)}[\sum_{a=1\ldots wi} a^{(v)}(x_i) * (b^{(v)(}s_i))] \tag{2}$$

Where m is the number of leaves in the reachability tree. Note that $b^{(v)}(s_i)$ of size n x 1 is the reward vector of the token in leaf node x_i on the v^{th} path, and n is the number of players as in the definition of Indefinite Event Net.

According to the state of Nash equilibrium, every player has achieved his best, when others don't change their strategies. Thus, the problem is to find such πthat $(U_1,U_2,\ldots,U_n)$ is a Nash equilibrium for each player, which could be given as:

$$\max \pi\ U = (U_1,U_2,\ldots,U_n) \tag{3}$$

Note that, the above equation is a multi-objective optimization, which can be solved using the mathematical programming methods.

4 Usages in Network Security

In this section, we will apply the Indefinite Event Nets to model the attack and defense actions, and investigate the security properties based on both reconnaissance and Nash equilibrium, and propose the optimum strategy for the computers at each stage to minimise the loss during computer attacks. More information about the enemy's (attacker's) strategic intentions is obtained using reconnaissance [4].By applying the indefinite event net to the basic attack and defend case the structure of sequence can be shown. The following steps are used to apply the Indefinite Event Nets and doing the security analysis.

Step 1: Determine the players in the game N; Present the targets of each player k, and construct each player's action set P^k;

Step 2: Define the incentive function If or each transition and then construct the Indefinite Event Net model;

Step 3: Find the Nash equilibrium with respect to the Indefinite Net model and propose optimum strategy by computing probability;

4.1 Basic Attack-Defend Case

The attack-defend[2] system is the most general form among all the network attacks. In a basic attack-defense cast, there are two players, the defender and the attacker. For easy to illustrate, we choose a simple attack case in this subsection. Here an attacker will try to intrude a computer system, and the computer takes actions to defend. Assume attacker as Player 1 and the defender Player 2. The transition[6] set of the Player 1, the attacker, is given in the following table 1.

Table 1.

m_1	m_2	m_5	m_6	m_7
http attack	ftp attack	web attack	continue attack	web server sniffer

The transition set of the Player 2, the defender, is also given in the following table.

Table 2.

m_3	m_4	m_8	m_9
defend of http attack	Tolerant	defend of web attack	Tolerant attack

By using the above steps the reachability tree can be drawn. Thus the Nash equilibrium can be obtained through equation (3).

5 The Proposed Lexicographic Game for Multi-player Environment

Here we apply Indefinite Event Net to multi player game, which is a typical repeated game in a common defense system. Now a days, more and more systems and agents are trying to cooperate to get a more powerful system. However, each contender in the combined system requires an individual security strategy to satisfy its own target, and these strategies are actually inconsistent at most of times. Therefore, the contender would come to either a finite repeated game or an infinite repeated game for the security strategy.

Let G = {N,(A_i), (~i)} be a strategic game, Let A = $X_i \epsilon NA_i$. An infinitely repeated game of strategy is an extensive game with perfect information and simultaneous moves {N,H,P,$\underset{\sim}{i}$} in which H = $U_{t=0\ldots\infty}A^t$ (where $A^0=\{\phi\}$ is the initial history). P(h) = N for each non terminal history hϵH. ~i is preference relation on the set A^∞ of infinite sequences $(a^t)_{t=0\ldots\infty}$ of action profiles in G that extends the preference relation ~I in the sense that it satisfies the following condition of weak separability : if $(a^t) \epsilon A^\infty$, aϵA, a'ϵA and a ~i a' then $(a^1,\ldots,a^{t-1},a,a^{t+1},\ldots)$~i then $(a^1,\ldots,a^{t-1},a',a^{t+1},\ldots)$ for all values of t. A history is terminal if and only if it is infinite. After any non-terminal history every player iϵN chooses an action in Ai. Thus strategy of player I is a function that assigns an action in Ai to every finite sequence of outcomes in G.

5.1 Discount Factor

There is some number δϵ(0,1) called discount factor such that the sequence v_i^t if and only if

$$\sum_{t=0}^{\infty} \delta_t(v_i^t - w_i^t) \geq 0 \tag{4}$$

According to this criterion a player evaluates a sequence (v_i^t) of payoffs by

$$\sum_{t=0}^{\infty} \delta^t v_i^{t-1} \tag{5}$$

For some discount factor δϵ(0,1). When the players' preferences take this form, we refer to the profile

$$(1-\delta)\lim_{T\to\infty}\sum_{t=1}^{T}\delta^{t-1}v_i^t \tag{6}$$

as the payoff profile in the repeated game associated with the sequence $(v^t)_{t=1}^{\infty}$ of payoff profiles in the constituent game.

5.2 Limit of Means

The limit of means states that the sequence (v_i^t) of real numbers is preferred to the sequence (w_i^t) if and only if

$$\text{Lim inf}\sum_{t=1}^{T}\frac{v_i^t-w_i^t}{\mathrm{T}}>0 \tag{7}$$

That is, if and only if there exists $\epsilon>0$ such that $\sum_{t=1}^{T}\frac{v_i^t-w_i^t}{\mathrm{T}}>\epsilon$ for all but a finite number of periods T.When the players' preferences take this form we refer to the profile for iϵN,

$$\lim_{T\to\infty}\sum_{t=1}^{T}v_i^t\,/T \tag{8}$$

if it exists as the payoff profile in the repeated game associated with the sequence $(v^t)_{t=1}^{\infty}$of payoff profiles in the constituent game.

5.3 Overtaking

By the definition of overtaking, the sequence (v_i^t) is preferred to the sequence (w_i^t) if and only if

$$\text{liminf}\sum_{t=1}^{T}(v_i^t-w_i^t)>0 \tag{9}$$

The following two Lemmas shows that the set of Nash equilibrium payoff profiles of an infinitely repeated game in which the players evaluate streams of payoffs by the limit of means is the set of all feasible enforceable payoff profiles of the constituent game.

5.3.1 Lemma

Every Nash equilibrium payoff profile of the limit of means infinitely repeated game of G = {N, (A_i), (u_i)}is an enforceable payoff profile of G. The same is true for any δϵ(0,1) of every Nash equilibrium payoff profile of the δ-discounted infinitely repeated game of G.

5.3.2 Lemma

Every feasible enforceable payoff profile of G={N,(A_i),(u_i)}is a Nash equilibrium payoff of the limit of means infinitely repeated game of G.

The next lemma shows that the set of Nash equilibrium payoff profiles of an infinitely repeated game in which the players evaluate streams of payoffs by the discount criterion factor.

5.3.3 Lemma

Let w be a strictly enforceable feasible payoff profile of $G=\{N,(A_i),(u_i)\}$. For all $\epsilon>0$ there exists $\delta \in (0,1)$ large enough and a payoff profile w' of G for which $|w'-w|<\epsilon$, such that w' is a Nash equilibrium payoff profile of δ-discounted infinitely repeated game of G.

The following lemma shows that the set of Nash equilibrium payoff profiles of an finitely repeated game in which the players evaluate streams of payoffs by the set of all feasible enforceable payoff profiles of the constituent game.

5.3.4 Lemma

If the payoff profile in every Nash equilibrium of the strategic game G is profile (v_i) of min max payoffs in G then for any value of T the outcome $(a^1,\ldots a^T)$ of every Nash equilibrium of the T-Period repeated game of G has the property that $a^t$is a Nash equilibrium of G for all t=1,…,T.

5.4 Lexicographic Game

Let us assume that the players preferences are lexicographic[18] and restrict the attention to the case in which the repeated component game is Prisoner's Dilemma. Trade of in each player's preferences between the payoffs in the repeated game and the complexity of the network is needed to limit the set of equilibria further.

The set of outcomes that occurs on an equilibrium path is any subset of the given problem. Hence, we obtain the optimal Nash equilibrium for the given network problem.

5.5 Example

If the two individuals repeatedly play the prisoner's dilemma game, then this game has a unique Nash equilibrium, in which each player chooses the action D, which strictly dominates the action C, so that the rationale behind the outcomes (D,D) is very strong. In a repeated game, the desirable outcome in which (C,C) occurs in every period is stable, if each player believes that a defection will terminate the cooperation resulting in a subsequent loss for him that outweighs the short term gain. In this game the focus is to isolate types of strategies which support desirable outcomes in any game. The repeated game has two versions namely finite and infinite. In the finite repeated game, the only Nash equilibrium outcome is that in which the players choose (D,D) in every period and in infinite repeated game, the set of sub game perfect equilibrium payoff profiles is huge.

The objective of this game strategies discernments into the structure of behavior when players interact repeatedly. By defining a machine, which is intended as an abstraction of the process by which a player implements a strategy in a repeated game. A machine for player i, in an infinitely repeated game has the following components namely a set (Q_i) of states, the initial state q_i^0, an output function and transition function. This needs a strategy which specifies an action for all possible histories, including those that are consistent with the player's own strategy. The machine of player P1, shown in figure 3 plays C as long as player P2 plays C; it plays

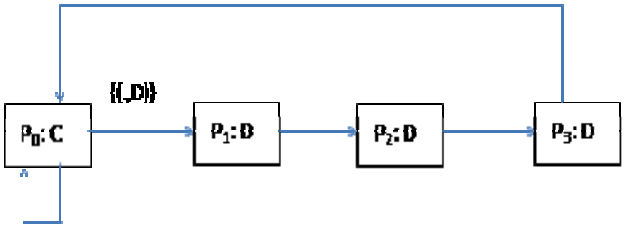

Fig. 2. Strategy of a machine

D for three periods and then reverts back to C, if player p2 plays D when he should play C. Here, we use {(.,X)} is to denote the set of all outcomes in which player 2's action is X.

In the bargain of secure strategy, one player take turns to propose a solution, one at each round. When the two players namely (P1) and (P2) agree on a strategy, the game ends. In the k^{th}moment(k=1,3,5,…,2m+1), where mϵN, (P1) shall propose a security strategy S_k. If (P2)agrees with S_k, then (P1) gets a utility of x. and (P2) gets $(1\text{-}x).\delta_2^{k-1}$, otherwise the game continues. By equation (4), δ1,δ2 ϵ[0,1] are discount factors for (P1) and (P2) respectively, which measures the bargaining cost on time scale, as defined in the game theory. In the k^{th} (k=2,4,6,…,2m) moment, which is P2's turn to propose his security strategy S_k. If (P1) agrees with S_k, then (P2) gets utility of y. $\delta_1^{k-1}$and (P1)gets $(1\text{-}y).\delta_2^{k-1}$by equation (5) and (6) or the game continues. The Indefinite Event Net model of this multi-round game is as follows :

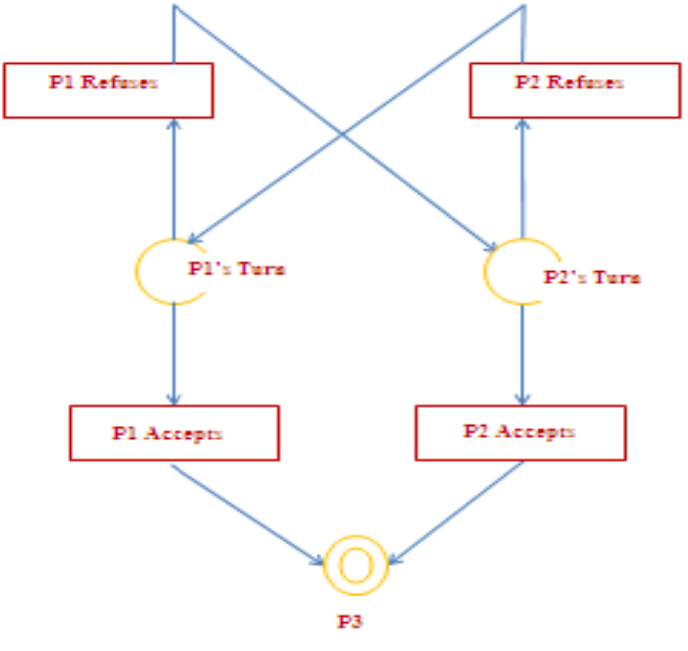

Fig. 3. Indefinite Event Net Model
(Here, D:Accepts, C:Refuses)

In the above Figure-2, each player has two actions, namely accept the strategy and refuse the strategy. The initial marking Io=(1,0,0) and there the reward vector of the initial token is written as $b(s_1) = (0,0)$. Then the reachability tree is given in the Figure-3 below where s1=(1,0,0), s2=(0,0,1), s3=(0,1,0) and T1,T2,T3 are respective actions:

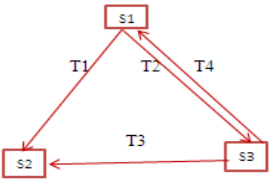

Fig. 4. Reachability Tree

According to a sub-game perfect equilibrium, P1 would always propose x= $(1-\delta_2)/(1-\delta_1\delta_2)$ and P2 would propose y=$(1-\delta_1)/(1-\delta_1\delta_2)$. Now at the k^{th} round of P1's turn, the utility function of the two players is :

$$U^{(k,1)} = \left(\frac{(1-\delta_2)\delta_1^{k-1}}{1-\delta_1\delta_2}, \frac{(1-\delta_1)\delta_2\delta_2^{k-1}}{1-\delta_1\delta_2}\right) \tag{10}$$

Similarly, at the k^{th} round of P2's turn, the utility function of the two players is written as

$$U^{(k,2)} = \left(\frac{(1-\delta_2)\delta_1\delta_1^{k-1}}{1-\delta_1\delta_2}, \frac{(1-\delta_1)\delta_2^{k-1}}{1-\delta_1\delta_2}\right) \tag{11}$$

In the reach ability tree, there is only one leaf node and we have the following constraints :

$$\pi_1+\pi_2=1$$
$$\pi_3+\pi_4=1$$

Thus, we have the following utility function to find the Nash equilibrium

$$\max_\pi U = (U_1, U_2) \tag{12}$$

Hence, we can find out that $\pi_1=1$ is the Nash Equilibrium. In contrast, $\pi_3=1$ would be the Nash Equilibrium while P2 gets the first chance to propose the security strategy.If the problem is a repeated game with finite or infinite state, then the lexicographic game method can be appliedby using either discount factor or limits of means according to the requirements, to obtain the best strategy and thus the optimal Nash equilibrium state can be reached.

6 Conclusions and Future Work

This paper presents a lexicographic game to analyse the problems of network security. These applications demonstrate the soundness and efficiency of the game theory. However, the design described is just a beginning. Reconnaissance as game of strategy is used to know more information about the strategies of players. By using

lexicographic game technique, we compute the Nash equilibrium of the game issue. Since this proposes a more flexible formulation for the game issue, there may be more than one Nash equilibrium in the solution. Thus, finite repeated game and infinite repeated game theory concept is applied to obtain the multiple solutions of Nash equilibrium and a try is made to propose a bound for the multiple Nash equilibriums. In future we can use the Markov decision process to decompose the large models and our lexicographic method allows us to perform complete analysis for the set of attack scenario states. Moreover, in terms of the modeling and analyzing approach, some simplification and approximation methods of indefinite key net could be well conduced indefinite event net with the repeated game theory lemmas which we believe would be promising in handling the complex game issues and provide a better solution. Thus, estimation of the performance measure of the system with the best-response strategies are chosen, including availability, survivability, measures related to security in wireless sensor network, cloud computing and so on.

References

1. Yu, Z., Guan, Y.: A dynamic en-route filtering scheme for data reporting in wire-less sensor networks. IEEE/ACM Transactions on Networking 18(1) (February 2010)
2. Reddy, Y.B., Srivathsan, S.: Game Theory Model for selective forward attacks in wireless sensor networks. In: 17th Mediterranean Conference on Control and Automation Makedonia Palace, Thessaloniki, Greece, June 24-26. Grambling State University, Lousiana State University (2009)
3. Min-kyu-Choi, Robles, R.J., Hong, C.-H., Kim, T.-H.: Wireless Network Security: Vulnerabilities, Threats and Counter measures. International Journal of Multimedia and Ubiquitous Engineering 3(3) (July 2008)
4. Chunhe, W.H., Zhang, X.C., Ma, Y.J.: A Network Security Risk Assessment framework based on Game Theory. School of Computer Science and Engg. IEEE, Beihang University (2008), doi:10.11.09/FGCN 2008–IEEE & CSI Jnl.
5. Mahimkar, A., Shmatikov, V.: On the advantage of network coding for improving network through-put. In: Proceedings of 18th IEEE Computer Society Foundations Workshop (2005)
6. Theodorakopoulos, G., Baras, J.S.: Game Theoretic modeling of Malicious users in collaborative Networks. IEEE Jnl. (2004)
7. Patcha, A., Jung-Min-Park: A game theoretic approach to modeling Intrusion detection in Mobile-Ad-hoc- Networks. IEEE (2004)
8. Nong, Y., Zhan, Y., Borror, C.M.: Robustness of the Markov-Chain Model for Cyber-Attack Detection. IEEE Transactions on Reliability 53(1) (March 2004)
9. Nicol, D.M., Sanders, W.H., Trivedi, K.S.: Model-based evaluation: From dependability to security. IEEE Transactions on Dependability and Secure Computing 1(1) (2004)
10. Wang, X., Reiter, M.: Defending against denial-of-service attacks with puzzle auctions. In: Proceedings of IEEE Security and Privacy (2003)
11. Lye, K., Wing, J.M.: Game strategies in network security. In: Proceedings of the 15th IEEE Computer Security Foundations Workshop (2002)
12. Sheyner, O., Jha, S., Wing, J.: Automated generation and analysis of attack graphs. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA (2002)

13. Browne, R.: C41 defensive infrastructure for survivability against multi-mode attacks. In: Proceedings 21st Century Military Communications. Architectures and Technologies for Information Superiority, vol. 1, pp. 417–424 (2000)
14. Shan, Z., Lin, C., Ren, F., Wei, Y.: Modeling and performance analysis of a multi server multi queue system on the grid. In: Proceedings of the 9th International Workshop on Future Trends of Distributed Computing Systems, pp. 337–343 (2000)
15. Howard, R.A.: Dynamic Probabilistic Systems. Semi-Markov and Decision Processes, vol. II. John Wiley and Sons, New York (1971)
16. Liu, P., Zang, W., Yu, M.: Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security 8(1), 1–41
17. Stinson, D.R.: Crypography – Theory and Practice, 2nd edn. Chapman & Hall/CRC (2002) ISN:I-58488-206-9
18. Fudenberg, Tirole, J.: Game Theory. The MIT Press (1991)