International Journal of
Mathematical Modelling & Computations
Vol. 08, No. 02, Spring 2018, 115- 124

Application of Stochastic Optimal Control, Game Theory and Information Fusion for Cyber Defense Modelling

M. Mohaghegh Tabar[a,]* and A. Mahmoodi[b]

[a] *Department of Sciences, Fouman and Shaft Branch, Islamic Azad University, Fouman, Iran,*
[b] *Department of Computer Engineering, Ozyegin University, Istanbul, Turkey.*

Abstract. The present paper addresses an effective cyber defense model by applying information fusion based game theoretical approaches. In the present paper, we are trying to improve previous models by applying stochastic optimal control and robust optimization techniques. Jump processes are applied to model different and complex situations in cyber games. Applying jump processes we propose some models for cyber battle spaces. The resulted stochastic models are solved by applying stochastic optimal control methods. A robust optimization technique is proposed to obtain robust estimations in the case of lack of complete data. We address reinforcement learning throughout the by stochastic optimal control formulation. Previous models are improved by applying optimal control approaches to overcome the issue of time steps in game theory based approaches in which times steps cause limitations by considering the cases that may take longer times. Two adaptation methods are proposed in incomplete information cases.

Received: 05 April 2018, Revised: 05 August 2018, Accepted: 23 February 2019.

Keywords: Stochastic optimal control; Information fusion; Game theory; Cyber defense; Robust optimization.

1. Introduction

Drastic events in cyber security domain proving that cyber-attacks can impose huge amounts of loss to wide range of areas including general public, scientific committee, governments, private enterprises, and financial sectors in terms of money, data confidentiality, and reputation and etc. [1, 2, 3].

Furthermore global cyber domain continues to experience increasing network size, interconnectivity, accessibility and consequent increasing in its vulnerability which obviously is a potential treat, even for humanity as a whole. Recent news about the unmeasurable effects some attacks e.g. "WannaCry" [3] around the world can be an example of unrecoverable cyber threats ahead of us. Good news is that research

*Corresponding author. Email: m.mohagheghtabar@fshiau.ac.ir

http://ijm2c.iauctb.ac.ir

communities have been paid attention to the network security problem in recent years, among many researches we referring to [4-7]. Data fusion and information fusion have been gathered the attention of an enormous amount of researches in cyber security [8].

Game theory concepts are also is applied in cyber defense domain [9, 10], most of which are based on static matrix and simple extensive games, which are usually solved by game trees [11-14]. Game-theoretic based approaches are often in the form of static game models [15] and from an assessed information point of view some of them considered with perfect information [16] and some with complete information [17]. However, in real cyber battle spaces we often face with the dynamic game with incomplete and imperfect information from both sides view. For a complete survey about the issue, we refer the reader to [18]. Other forms of defense (active defense) is also developed based on game theory recently [9, 11].

The present paper is based on the framework of the approach proposed by Chen et al. [10] for cyber situational awareness and impact assessment is shown in Figure 1. The approach two fully coupled major parts; (i) Data fusion module (to refine primitive awareness and assessment; to identify new cyber attacks) and (ii) Adaptive feature recognition module (to generate primitive estimations; to learn new identified new or unknown cyber attacks).

In the present paper, we deal with the uncertainty and incompleteness of the available information (from both sides). The uncertainty of actions of attackers is modeled by jumping processes with an initial setting that can be improved during the process and in different steps according to observed data. This makes the model to match with the real environment. Jump process allows us to consider multi-stage attacks properly by considering impact assessments and other features in cyber battle space. Some different models are proposed to cover many complex situations. We improved adaptation processes proposed in [13, 10] applying stochastic optimal control approaches and robust optimization methods. Two case of adaptation features i.e. one-side and two-side adaptation approaches are considered and we derived robust estimation for each side based on available information entered into the system. One of the drawbacks of current methods is that they consider each step relative to time lengths while it is obvious that in real cyber security problems time length of each step is unknown. Considering time steps cause difficulties and limitations authors propose applying H^∞-optimal control methods. The technique is improved by conducting H^∞ stochastic optimal control approaches to obtain optimal strategy at every step. In this paper, we will focus on the Markov game theoretic Level 3 data fusion solution in the overall architecture is introduced in [10].

The paper is organized as follows: In section 2 an overview of application of game theory in cyber domain is presented and basic definitions are stated, in section 3 an adaptive design for linear quadratic games with jump discontinuities is presented, in this section different models for covering complex situations are proposed, section 4 proposes jump linear quadratic model generalized for multi-stage cases, adaptation strategies are presented in section 5 and finally we draw conclusion in section 6.

2. An overview of game theory

In the cyber domain, Game theory describes multi-person decision scenarios in cyber defense spaces as games in which actions are chosen by each player to result in the best possible rewards while anticipating the rational actions from other players. *Players* are considered as a basic entity of a game making decisions and then perform actions. *Strategic* interaction in the domain is described by the *game* that includes some rules to be fulfilled, payoffs to be achieved, actions to be taken as a prediction of logical behavior of both sides. *Payoff* is the positive or negative reward to a player for a given action within the game and an *action* constitutes a move in the given game. Steady state condition of the game is described by *Nash equilibrium* which is a solution concept for the game theory problems. In the following, concepts of stochastic optimal control are applied to obtain the solution of the complex system raised in cyber security. In cyber security domain, game theory has been applied to capture the nature of cyber war or conflict in the sense that attacker's and defenders decision strategies are closely related to each other. Therefore Cyber-security is modeled by at least two and three (considering users too) regular agents interacting in an attempt to maximize their intended objectives. A key concept of the game theory is the ability to examine the huge number of possible threat scenarios in the cyber system while the size of involved problem does not unacceptably high [19]. Combining Game theory and stochastic optimal control techniques we can also provide several probable actions to predicted outcomes of the future threats (projection). It was shown that [10] game theory has the following advantages; (i) it is decentralized. decisions are mostly based on local information; (ii) Uncertainties in the cyber environment can be modelled via Markov decision process (MDP) effectively; (iii) it is a game model with two (or three) players: red force (network attackers) and blue force (cyber defense resources); and (iv) fictitious player learning concept can also be integrated.

A dynamic learning procedure is placed alongside the fusion system. Players are starting with some initial beliefs and choose the best response according to those beliefs as the optimal strategy at each period. Then, after observing their opponent's actions, the players improve their beliefs in the dynamic learning environment. This process is then repeated. It is known that if it converges, the point of convergence is a Nash equilibrium of the game. The game-theory we are working with has at least two players. A player's success in making choices obviously depends on the choices of each other, while sequentially trying to maximize their gain in an attempt to achieve their ultimate goal [20]. In the present paper, we consider a stochastic game in order to model the cyber game properly. We are facing the following concepts in cyber security model:

State Space: All the possible states of involved network nodes consist of the state space. For example, the web-server (IP = 26.134.3.125) is controlled by attackers. State vector for the *i*'th network node at times t is denoted by $x_i(t) = (f_i(t), p_i(t), a_i(t), s_i(t))^T$. where f is the working status of the *i*'th network node, p is the protection status, a is the status of being attacked, and T is the transpose operator and $s_i\left(t\right)$ is unfolded attack sequences (attack tracks) at times t . Analogous to [10] working status f_i can get values "undestroyed", "damaged", or "destroyed" (representing the status of the corresponding node *i* in battle space), p_i for node *i* denotes the defense action such as firewall, IDS, and filter, (each one with probability) unprotected node is denoted by $p_i = NULL$ means that no resource is devoted to this node. The system states are determined by two factors; previous states and current actions (Markovian property).

Action Space: Players at every step, choose targets with associated actions based on its observed network information. There are some actions are defined for players of both teams; attackers and defenders while defenders can apply e.g. firewall, IDS, and filter, cyber network attackers consider network-based attacks e.g. Denial-of-Service (DoS), Buffer overflow, Semantic URL attack, E-mail Bombing and etc. In the model, we also considered multi-stage attacks in which some attacks are accompanied by a different form of scenarios maybe as a misleading or detecting vulnerability.

Transition Rule: By transition rule it is possible to calculate the probability of transition of state in different steps, that is to compute $Trans\Big(x(t+1)\,|\,x(t), u^1(t), u^2(t)\Big)$ where $u^d(t)$ and $u^a(t)$ are the overall decisions of network defense system and cyber attackers, respectively, at time step t. Overall actions for each team are specified in Strategies. *Payoff Functions:* In the Markov game model presented in [10], there are two levels of payoff functions for each player. In an analogous way, we introduce lower-level (cooperative within each team based on the available local information) and higher-level (non-cooperative between teams) payoff functions. Lower payoff function at time t for $\Psi_i^d\left(\tilde{x}_i^a(t),u_i^2(t),W^a(t);t\right)$ i'th attackers is defined as where $\tilde{x}_i^a$ is state based on local information collected by i'th member, this information is obviously a subset of complete information gathered from overall nodes. $W^a(t)$ is the weight for all possible action-targets couples of attackers. $W^a(t)$ is computed according to the top-level payoff function team-optimal perspective. The lower level function for attackers is defined as [10]:

$$\Psi_i^a\left(\tilde{x}_i^a(t),u_i^2(t),W^a(t);t\right)=U(\tilde{x}_i^a(t))-w\left(W^a(t),u_i^2(t)\right)c(u_i^2(t))$$

where $U(\tilde{x}_i^a(t))$ is payoff of current local network state, $c(u_i^2(t))$ is cost of action to be taken by the attackers. $w(.)$ is the weight for any specified action of i'th member of the attacker's team based on the received $W^a(t)$ which represents the preference of team defence strategy. Lower level payoff function is defined for defenders similarly

$$\Psi_i^d\left(\tilde{x}_i^d(t),u_i^1(t),W^d(t);t\right)=U(\tilde{x}_i^d(t))-w\left(W^a(t),u_i^1(t)\right)c(u_i^1(t))$$

The top-level payoff functions at time t which are used to evaluate the overall performance of players is defined for attackers and defenders as

$$\Phi^a\left(\tilde{x}_i^a(t),u_i^2(t);t\right)=\sum_{i=1}^{N^a}\Psi_i^a\left(\tilde{x}_i^d(t),u_i^1(t),W^d(t);t\right),$$

$$\Phi^d\left(\tilde{x}_i^d(t),u_i^1(t);t\right)=\sum_{i=1}^{N^d}\Psi_i^d\left(\tilde{x}_i^d(t),u_i^1(t),W^d(t);t\right).$$

Payoff functions computed distributively and sent back to the network administrator. In the present paper, the objective functions are represented as follows

$$J^d(u^1(t))=\int_0^\infty \Phi^d\left(\tilde{x}^d(t),u^1(t);t\right)dt,$$

$$J^a(u^2(t))=\int_0^\infty \Phi^a\left(\tilde{x}^d(t),u^2(t);t\right)dt.$$

3. An adaptive design for linear quadratic games

In order to model the complex situation in the cyber battle field, in the present section, we considered jump processes to model activity or inactivity of different forms of attacks. The activity of certain form of attack, for example, DoS will be denoted by a binary (jump process) coefficient. The linear quadratic game is proposed with the following state

$$\frac{dx}{dt}=A(r(t))x(t)+B^1(r(t))u^1(t)+B^2(r(t))u^2(t), \tag{1}$$

where $A\left(r(t)\right) = A_i$, $B^1(r(t))=B_i^1$ and $B^2(r(t))=B_i^2$ when $r(t) = i$ and $i\in□$. A_i, B_i^1 and B_i^2 are real matrices with proper dimensions. We also assume that the process $r:□^+\to\{1,2,\dots,N\}$ is Markovian with transition probabilities

$$\text{Prob}\{r(t+\Delta)=j \mid r(t)=j\}=\begin{cases}\rho_{ij}\Delta & \text{if } i\neq j\\ 1+\rho_{ij}\Delta & \text{else}\end{cases}$$

where $\rho_{ij}\geq 0$ for $i\neq j$ and $\rho_{ii}=\sum_{i\neq j}\rho_{ij}$. The cyber defense problem is modeled as jump linear quadratic (JLQ) problem in which we are looking for minimization of quadratic cost functions for defenders and attackers

$$J^d(u^1)=E\left\{\int_0^\infty \left(x^T Q^1(r(t))x+(u^1)^T R^{11}(r(t))u^1+(u^2)^T R^{12}(r(t))u^2 dt \mid x(0),r(0)\right\}\right. \quad (2)$$

$$J^a(u^2)=E\left\{\int_0^\infty \left(x^T Q^2(r(t))x+(u^1)^T R^{21}(r(t))u^1+(u^2)^T R^{22}(r(t))u^2 dt \mid x(0),r(0)\right\}\right. \quad (3)$$

where the state x, and u^i for $i=1,2$ are real vectors satisfying (1). The cost matrices $Q^i(r(t))$ and $R^{ij}(r(t))$ for $i,j = 1,2$ are defined by

$$Q^i(r(t))=Q_l^i,\quad R^{ij}(r(t))=R_l^{ij},\quad \text{where} \quad r(t)=l,$$

where $Q^i\succ 0$ and $R^{ij}\succ 0$ for $i,j = 1,2$ where "$\succ$" stands for the positive-definitive property. Systems are stabilizable, (A,C^i) is detectable (where $(C^i)^T C^i=Q^i$ and $|(B^i)^T B^i|>0$ for $i=1,\ 2$. We assume that both players have perfect information structures, with which both players know the exact dynamical system (1).

Assumption 1. We assume that the dynamical system (1) is mean square stabilizable that is $\lim_{t\to 0} E\left[x^T(t)x(t)\right]=0.$

3.1. Discrete formulation of linear quadratic game

The discrete-time jump linear systems are described by

$$X_{k+1}=A(r_k)X_k+B^1(r_k)u_k^d+B^2(r_k)u_k^d, \quad (4)$$

where $A(r_k) = A_i$, $B(r_k) = B_i$, when $r_k = i$, $i=1,\dots,N$. The random process r_k is a finite-state discrete-time Markov chain with transition probabilities

$$\text{Prob}\{r_{k+1}=j \mid r_k=i\}=\rho_{ij} \quad \text{if } 1\leq i,j\leq N,$$

in the stochastic optimal control of this type of dynamical systems, one obtains a Riccati equation of the form

$$A_i^T S_i A_i - X_i - A_i^T B_i^1 S_i[R_i^{11}+R_i^{12}+B_i^{1T}S_i B_i^1]^{-1}B_i^1 S_i A_i B_i^2 S_i[R_i^{21}+R_i^{22}+B_i^{2T}S_i B_i^2]^{-1}B_i^2 S_i A_i + Q_i^1=0$$

$$S_i=\sum_{j=1}^N \rho_{ij}X_j,\quad X_i\geq 0,\quad i=1,2,\dots,N \quad (5)$$

where $Q_i^m \pm 0$, $R_i^{m,l}\succ 0,\ m,l=1,2$ are the state and defend-attack gain matrices, respectively.

3.2. Linear Systems with Both Jumps and Multiplicative Noise on the State

The corresponding Riccati equations have the form (for further discussions about these type of systems refer to [10, 23])

$$A_i^T X_i + X_i A_i - X_i B_i^1 (R_i^{11} + R_i^{11})^{-1} B_i^1 X_i + \sum_{j=1}^{N} \rho_{ij} X_j + \Delta_i(X_i) + Q_i^1 = 0, \quad i = 1,2,\ldots N \tag{6}$$

where Δ_i for $i = 1,2,\ldots,N$ are some linear matrix functions that are positive, that is, $X \pm 0$ gives $\Delta_i(X) \pm 0$.

3.3. Linear Systems with Both Jumps and Random State Discontinuities

In this type of problems which are discussed in [24], the Riccati equations are obtained as

$$A_i^T X_i + X_i A_i - X_i B_i^1 (R_i^{11} + R_i^{11})^{-1} B_i^1 X_i + \sum_{j=1}^{N} \rho_{ij} (X_j + \Gamma_{ij}(X_j) + Q_i^1 = 0, \quad i = 1,2,\ldots,N \tag{7}$$

where Γ_{ij} for $i, j = 1,2,\ldots,N$ are some linear matrix functions that are positive-definite.

3.4. Infinite horizon optimal control of Jumps Linear systems

Analogous stochastic optimal control problems called H^∞-optimal control have been studied [25] that could be solved applying a set of coupled Riccati equations. For our case, the Ricatti equation of the problem is modeled as

$$A_i^T X_i + X_i A_i X_i \Big[\frac{1}{\gamma^2} (B_{1i}^1 + B_{1i}^2)(B_{1i}^1 + B_{1i}^2)^T - (B_{2i}^1 + B_{2i}^2)(B_{2i}^1 + B_{2i}^2)^T \Big] X_i$$
$$+ \sum_{j=1}^{N} \rho_{ij} (X_j + \Gamma_{ij}(X_j) + (C^1)_i^T C_i^1 = 0, \qquad i = 1,2,\ldots N \tag{8}$$

where prescribed value $\gamma > 0$ is called the level of disturbance attenuation. Let us assume that the system is stable for a suitable value of Γ and the pairs (C_i^l, A_i) for $i = 1,2,\ldots,N$ and $l = 1,2$ are mean-square stabilizable and observable.

4. Generalization of jump linear quadratic model for cyber spaces

For the case that we are facing with multi-stage attacks, the problem becomes more complex which cannot be solved applying previous techniques. In this case, the state dynamical system is modeled as

$$dx(t) = Ax(t)dt + B^1 u^1(t)dt + \sum_{i=1}^{L} \Big(A_i x(t) dp_i(t) + B_i^2 u^2(t) dp_i(t) \Big), \tag{9}$$

where p_i is assumed to be independent Brownian motions with variance, for $i = 1,2,\ldots,L$. Then the objective functions corresponding to the Nash strategy pairs are defined with the following stochastic optimal control problem

$$J^d(u^1) = E\Big\{ \int_0^\infty \Big(x(t)^T Q^1 x(t) + u^1(t) R^{11} u^1(t) + \sum_{i=1}^{L} u^2(t) R_i^{12} u^2(t) \Big) \Big\} \tag{10}$$

$$J^a(u^2) = E\Big\{ \int_0^\infty \Big(x(t)^T Q^2 x(t) + u^1(t) R^{21} u^1(t) + \sum_{i=1}^{L} u^2(t) R_i^{22} u^2(t) \Big) \Big\} \tag{11}$$

where $Q^l \pm 0$ and $R_i^{l,m} \succ 0$ for being the state and defense-attack gain matrices, respectively. The Riccati equation associated with the optimal control problem (10) subject to (9) is derived as

$$A^T S + SA - SB^1 \Big(R^{11} + R^{12} + \sum_{i=1}^{L} \sigma_i^2 B_i^{2T} S B_i \Big)^{-1} B^1 S + \sum_{i=1}^{L} A_i^T S A_i + Q^1 = 0, \tag{12}$$

and analogously for attackers case we face with (11) subject to (9) the Riccati equation is obtained as

$$A^T S + SA - SB^1\Big(\sum_{i=1}^{L}(R_i^{21} + R_i^{22}) + \sum_{i=1}^{L}\sigma_i^2 B_i^{2T} SB_i\Big)^{-1} B^1 S + \sum_{i=1}^{L} A_i^T SA_i + Q^2 = 0, \tag{13}$$

5. An adaptation scheme with incomplete data

The adaptation scheme with Ricatti equations as the solution of optimal control problem (deterministic case) is studied in [10] and as the overall technique is analogous, we leave further discussion about the problem. In the case of complex problems e.g. stochastic optimal control problems (10) and (11) subject to (9) solving Ricatti equations (12) and (13) respectively does not lead to proper solution which is required in the cyber defense problems. Instead, we apply Linear Matrix Inequality (LMI) optimization via a stochastic Lyapunov function approach (see [22] for analogous techniques). In this case, the optimal control law is obtained by as linear system

$$u^1 = U^1 (X^1)^{-1} x, \tag{14}$$

$$u^2 = U^2 (X^2)^{-1} x, \tag{15}$$

In the case of (14), U^1, X^1 are solutions to the LMI optimization problem of the form

Minimize $Tr(Y) + Tr(X^1 Q^1)$ (16)

subject to the following inequality constraints

$$\begin{pmatrix} Y & (R^{12})^{1/2} U^1 \\ (U^1)^T (R^{12})^{1/2} & X^1 \end{pmatrix} \succ 0,$$
$$Ax + B^1 U^1 + X^1 A^T + (U^1)^T (B^1)^T + x(0)x(0)^T + \sum_{i=1}^{L} \sigma_i^2 (A_i X^1 + B_i^2 U^1)(X^1)^{-1}(A_i X^1 + B_i^2 U^1)^T < 0, \tag{17}$$

and in the case of (15), U^2, X^2 are solutions to the LMI optimization problem of the form

Minimize $Tr(Y) + Tr(X^2 Q^2)$ (18)

subject to the following inequality constraints

$$\begin{pmatrix} Y & (\sum_{i=1}^{L} R_i^{22})^{1/2} U^2 \\ (U^2)^T (\sum_{i=1}^{L} R_i^{22})^{1/2} & X^2 \end{pmatrix} \succ 0,$$
$$Ax + B^1 U^2 + X^2 A^T + (U^2)^T (B^1)^T + x(0)x(0)^T + \sum_{i=1}^{L} \sigma_i^2 (A_i X^2 + B_i^2 U^2)(X^2)^{-1}(A_i X^2 + B_i^2 U^2)^T < 0. \tag{19}$$

In such cases, we are facing a complex problem. Let us consider two cases of adaptations here.

5.1. One-side adaptation

In the one-side adaptation, we assume that one side of the game e.g. defenders are known the system completely i.e. defenders know matrices $R^{l,m}, Q^l, B^1, B_i^2$ and A, A_i with $l,m = 1,2$, $i = 1,2,\ldots L$ completely while attackers only know matrices $Q^2, R_i^{2,1}$, R_i^{22}, B^1, B_i^2 and A, A_i where $i = 1,2,\ldots L$. The attackers estimating the unknown matrices in order to calculate their optimal strategy. It is essential to take some assumption on this game to make the problem simpler. First, let the defenders apply its state feedback Nash strategies calculated based the information on system dynamics (9)-(١٠). Attackers also in advance know that its opponent will implement state feedback Nash strategies. Attackers will also apply corresponding feedback Nash strategies calculated based the information of system dynamics (9)-(11) but in this case, unknown matrices should be estimated based on available information. In this case because attackers do not access the exact data, we assume that their estimation belongs to an uncertainty set of matrices. Robust optimization technique is applied in order to obtain most reliable results. We assume that $\hat{Q}^1 \in \mathrm{Q}$, $\hat{R}^{12}, \hat{R}^{11} \in \mathrm{R}$ are matrices that estimated by attackers such that spaces Q, R are convex. Then with these matrices, a robust optimization technique is applied to obtain matrices $\hat{X}^1$ and $\hat{U}^1$ from (16) subject to (17). The dynamical system (9) is replaced by

$$d\hat{x}(t) = Ax(t)dt + B^1\hat{U}^1(\hat{X}^1)^{-1}x(t)dt + \sum_{i=1}^{L}\Big(A_i x(t)dp_i(t) + B_i^2 u^2(t)dp_i(t)\Big), \tag{20}$$

Now applying the equations (9) and (20), according to invertibility of $(B^1)^T B^1$ we obtain

$$[(B^1)^T B^1]^{-1}(B^1)^T(d\hat{x}(t) - dx(t)) = (\hat{U}^1(\hat{X}^1)^{-1} - UX^{-1})x(t)dt, \tag{21}$$

which gives us some senses about the estimation error. The adaptation design is illustrated in Figure 1 which shows that in this case at every step we have one robust optimization problem, the estimation result is included in the dynamic system to predict the next state.

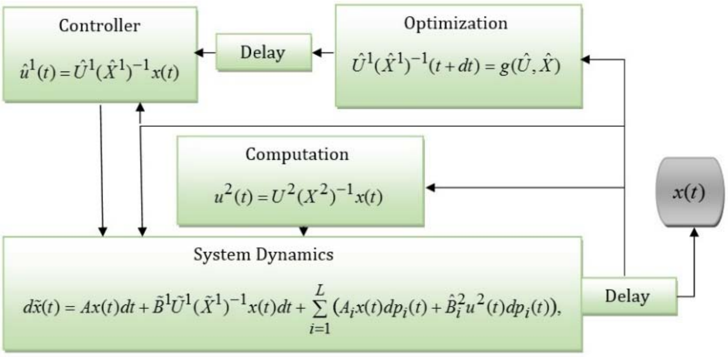
Controller
$\hat{u}^1(t) = \hat{U}^1(\hat{X}^1)^{-1}x(t)$
Delay
Optimization
$\hat{U}^1(\hat{X}^1)^{-1}(t+dt) = g(\hat{U}, \hat{X})$
Computation
$u^2(t) = U^2(X^2)^{-1}x(t)$
$x(t)$
System Dynamics
$d\hat{x}(t) = Ax(t)dt + \hat{B}^1\hat{U}^1(\hat{X}^1)^{-1}x(t)dt + \sum_{i=1}^{L}(A_i x(t)dp_i(t) + \hat{B}_i^2 u^2(t)dp_i(t)),$
Delay

Figure 1. One-side feedback robust control design for adaptation.

5.2. Two-side adaptation

In this case both defenders and attackers do not know other side's matrices, that is defenders only have matrices $Q^1, R^{11}, R^{12}, B^1, B_i^2$ and A, A_i for $i = 1, 2, \ldots, L$ while attackers aware of $Q^2, R_i^{22}, R_i^{21}, B^1, B_i^2$ for $i = 1, 2, \ldots, L$. Both sides estimate the unknown matrices of the other side and in every step, we have two robust optimization problems should be solved for both sides. Equations (20) and error estimation (21) can be constructed for both sides analogously. Adaptation design is represented in Figure 2 shows that at every step two robust optimization is solved in order to obtain an estimation of linear operators which in turn is applied for estimating each sides action. The estimated action then is included in the dynamic system to obtain an estimation of the next state.

6. Conclusions

In the present paper, we presented a model that considers multi-stage cyber-attacks by jump stochastic process. Furthermore H^∞ -optimal control approach is applied to consider the situation in which the game steps may take several (unknown) time to get very realistic and robust estimation of the state. At the final part, the cases of one-side adaptation scheme as well as two side adaptation schemes are presented. The proposed high-level information fusion based approach for cyber defense has more advantages comparing with previous models which can consider more realistic and complex situations. For future researches in this field, the authors propose to apply the method driving lower information fusion levels such as attach tracks and projection. These can be done by including transition matrices of alert tracks tough the systems state and hence improve the overall information fusion method.

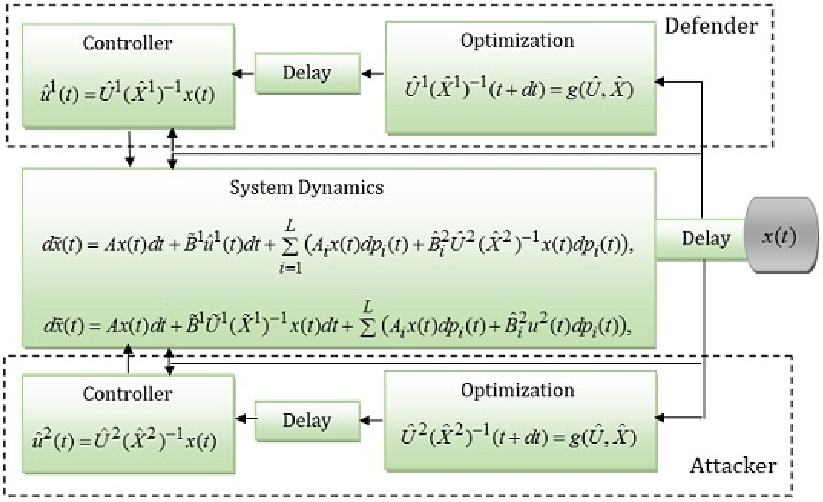
Defender
Controller
$\hat{u}^1(t) = \hat{U}^1(\hat{X}^1)^{-1}x(t)$
Delay
Optimization
$\hat{U}^1(\hat{X}^1)^{-1}(t+dt) = g(\hat{U},\hat{X})$
System Dynamics
$d\bar{x}(t) = Ax(t)dt + \tilde{B}^1\hat{u}^1(t)dt + \sum_{i=1}^{L}(A_i x(t)dp_i(t) + \hat{B}_i^2\hat{U}^2(\hat{X}^2)^{-1}x(t)dp_i(t)),$
$d\bar{x}(t) = Ax(t)dt + \tilde{B}^1\tilde{U}^1(\tilde{X}^1)^{-1}x(t)dt + \sum^{L}(A_i x(t)dp_i(t) + \hat{B}_i^2 u^2(t)dp_i(t)),$
Delay
$x(t)$
Controller
$\hat{u}^2(t) = \hat{U}^2(\hat{X}^2)^{-1}x(t)$
Delay
Optimization
$\hat{U}^2(\hat{X}^2)^{-1}(t+dt) = g(\hat{U},\hat{X})$
Attacker

Figure 2. Two-side feedback robust control design for adaptation scheme.

References

[1] J. Page, M. Kaur and E. Waters, Director's liability survey: Cyber-attacks and data loss--a growing concern, Journal of Data Protection and Privacy, **(۲)** ۱ (2017) 173-182.

[2] A. Cook, A. Nicholson, H. Janicke, L. A. Maglaras and R. Smith, Attribution of Cyber Attacks on Industrial Control Systems, EAI Transactions on Industrial Networks and Intelligent Systems, **3 (7)** (2016) ۱۵-۱.

[3] X. Liu, Z. Li, Z. Shuai and Y. Wen, Cyber-attacks against the economic operation of power systems: a fast solution, IEEE Transactions on Smart Grid, **8 (2)** (2017) 1023-1025.

[4] S. Parkinson, P. Ward, K. Wilson and J. Miller, Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges, IEEE Transactions on Intelligent Transportation Systems, (2017).

[5] J. M. Ehrenfeld, WannaCry, Cybersecurity and Health Information Technology: A Time to Act, Journal of Medical Systems, **41 (7(** (2017), doi:10.1007/s10916-017-0752-1.

[6] A. Terai, S. Abe, S. Kojima, Y. Takano and I. Koshijima, Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine Based on Communication Profile, IEEE European Symposium in Security and Privacy Workshops (EuroS & PW),)2017) 132-138.

[7] Y. M. Li, H. Voos and M. Darouach, Robust H^∞ fault estimation for control systems under stochastic cyber-attacks", In Proc. of 33rd China Control Conference, Nanjing, China, (2014) 3124-3129.

[8] I. M. Alsmadi, G. Karabatis and A. Aleroud, Information Fusion for Cyber-Security Analytics, Springer International Publishing, (2017).

[9] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, .N Pissinou and S. S. Iyengar, Game Theory for Cyber Security and Privacy, ACM Computing Surveys (CSUR),) **(۲)** ۵۰2017) 30:1--30:37.

[10] D. Shen, G. Chen, J. B. Cruz, E. Blasch and M. Kruger, Game theoretic solutions to cyber-attack and network defense problems, Intelligent automatic INC Brockville MD, (2007).

[11] W. Kun, M. Du, D. Yang, C. Zhu, J. Shen and Y. Zhang, Game-theory-based active defense for intrusion detection in cyber-physical embedded systems, ACM Transactions on Embedded Computing Systems (TECS),**(۱) ۱۶** (2016) 18:1--18:21.

[12] K. Sallhammar, S. J. Knapskog, B. E. Helvik, Using Stochastic Game Theory to compute the expected Behaviour of attackers, In Proc. of Symposium on Applications and the Internet Workshops, (2005).

[13] A. Agah, S. K. Das and K. Basu, A non-cooperative game approach for intrusion detection in sensor networks, Vehicular Technology Conference, VTC2004-Fall, (2004) 2902-2909.

[14] T. Alpcan and T. Basar, A game theoretic application to decision and analysis in Network Intrusion Detection, In Proc. of 42nd IEEE CDC Maui, Hawaii, USA, (2003) 2595-2600.

[15] Y. Liu, C. Comaniciu and H. Man, A bayesian game approach for intrusion detection in wireless ad-hoc

networks, ACM International Conference Proceeding Series,)2006).

[16] T. Alpcan and L. Pavel, Nash equilibrium design and optimization, International Conference on Game Theory for Networks, GameNets, (2009).

[17] K. C. Nguyen, T. Alpcan and T. Basar, Stochastic games for security in networks with interdependent nodes, In Proc. of International Conference on Game Theory for Networks, GameNets, (2009).

[18] R. Sankardas, C. Ellis, S.Shiva, D. Dasgupta .V ,Shandilya and Q. Wu, A survey of game theory as applied to network security, In Proc. of 43rd Hawaii International Conference of System Sciences (HICSS), (2010) 1-10.

[19] S. N. Hamilton, W. L. Miller, A. Ott and O. S. Saydjari, Challenges in applying game theory to the domain of information warfare, In Proc. of the 4th Information survivability workshop (ISW-2001/2002), (2002).

[20] A. Alazzawe, A. Nawaz and M. M. Bayaraktar, Game theory and intrusion detection systems, (2006), http://theory.stanford.edu/˜iliano/courses/06S-GMU-ISA767/project/papers/alazzawe-mehmet nawaz.pdf

[21] M. J. Obsborne and A. A. Rubinstein, A course in game theory, MIT Press, (1994).

[22] L. El Ghaoui, State-feedback control of systems with multiplicative noise via linear matrix inequalities, Systems and Control Letters, **24** (1995) 223-228.

[23] K. Sallhammar, S. J. Knapskog, B. E. Helvik, Using Stochastic Game Theory to compute the expected Behaviour of attackers, In Proc. of Symposium on Applications and the Internet Workshops, (2005).

[24] M. Mariton, Jump linear quadratic control with random state, Disconti-Utomutica, **23**) 1987) 237-240.

[25] C. E. De Souza and M. D. Fragoso, H^∞ control for linear systems with Markovian jumping parameters, Control Theory and Advanced Technology, **9** (1993) 457-466.