Game-Theoretic Models for Assessing Security of a SOA Based Intelligence Information System

Slavko Angelevski
Military Academy "General Mihailo Apostolski" Skopje, R.Macedonia
slavko.angelevski@ugd.edu.mk

Jugoslav Achkoski
Military Academy "General Mihailo Apostolski" Skopje, R.Macedonia
jugoslav.ackovski@ugd.edu.mk

Dimitar Bogatinov
Military Academy "General Mihailo Apostolski" Skopje, R.Macedonia
dimitar.bogatinov@ugd.edu.mk

Nevena Serafimova
Military Academy "General Mihailo Apostolski" Skopje, R.Macedonia
nevena.serafimova@ugd.edu.mk

***Abstract*— Modern information technology offers significant support to the Intelligence Cycles (planning, collecting, analyzing of data and their dissemination), by promoting the appropriate and flexible use of information, its searchability and exploitation. Although Intelligence Information Systems can significantly improve current and generate new intelligence working protocols, they are confronted with a serious challenge – the security of the system and the circulated information. Optimization techniques in the context of game and control theory are some of the tools that offer mathematical support for the formalization of the decision-making processes related to networked systems security. Game theory has been recently recognized as a way around the problem of lacking a quantitive decision framework for the security issues, as well as a model that can address more efficiently the problem of computational complexity in simulations.**

Keywords*— *intelligence; information system; security; game theory; strategy; stochastic; defence;

I. INTRODUCTION

Security analysis of IT systems becomes increasingly involved and demanding task, as the level of complexities rises with the ongoing innovations and applications. This has resulted in a large number of defense mechanisms against networked systems' attacks, each of them employing a number of variables. In combining defense mechanisms, decisions often hinge on the tradeoff between the costs and the benefits of the mechanism to the system. On the other side, the attacker has to organize the resources around, for example, exploiting fast but easy detectable or slow but difficult to detect attacks.

Networked systems are difficult to observe and control. Countless number of automated processes are running at each and every moment, hidden somewhere in the background, making connections and communicating with other computers in the network. With hardware and software highly complex nature being one of the reasons for security concerns, the ubiquitous presence of unintentional flaws in the software products are the accompanying cause. Additionally, the distributed architecture of modern networks prevent the administrator from implementing complete defense solutions and achieving full control over the system's behavior in a network.

The rising complexity of defense mechanisms has introduced various theoretical models for their construction and analysis. Such are the fields of probabilistic graph theory, machine learning, pattern recognition, cryptography, application of classification and clustering techniques. More recently, game theory has been used as a competing tool for dealing with the burden of high computational demands.

Two global groups of actors are concerned with security issues of an information system: attackers (malicious users) and defenders (system administrators). Security games, being an attackers/defenders interaction model, have the ability of quantifying possible outcomes, determine availability of strategies as well as predicting possible future behavior. Their presentation can vary from simple, deterministic to complex, stochastic ones where the play proceeds through changing states, according to estimated transition probabilities.

This article discusses game theoretical models for the treatment of Intelligence Information System (IIS) security issues. In Section II, a short description of a SOA-based IIS is given. Section III looks briefly into security issues of this model, Section IV gives a short introduction to security games and presents two different model concepts. In the last section we give some concluding remarks and discuss implementation challenges.

II. INTELLIGENCE INFORMATION SYSTEM BASED ON SERVICE-ORIENTED ARCHITECTURE

The Model of SOA-based Intelligence Information System (IIS) (Figure 1) is created to provide a comprehensive support to the intelligence process, its role and assignments. It encompasses three types of users: service providers, service consumers and Intelligence. Agencies, departments, institutions and other stakeholders can push and pull data on a standardized and flexible manner through communication interfaces using XML schema and web services.

All services are getting information from appropriate service providers through Information Systems of the government institutions or the agencies which are included in

the Intelligence Cycle. In addition, it is possible for other Information Systems to act as service providers for inter-institutional governance. Service providers which support the workflow processes, define which web services can be exploited and define appropriate service registers' security level.

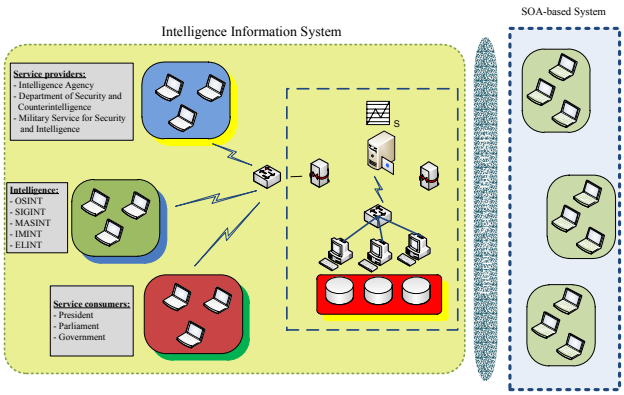

Figure 1: Model of SOA-based Intelligence Information System

Intelligence is based on several disciplines: IMINT, SIGINT, MASINT, OSINT, etc. They fulfill their requirements by completing several tasks: information gathering (assessments, analyses, generating reports), verification and notification (e.g., political and security situation in foreign countries related to security of investments), etc.

Our methodology of developing SOA-based Intelligence Information System consists of several postulates.

The first postulate defines data exchanging methodology within SOA. It should be compatible with publicly described solutions for information systems which support intelligence functions.

The second postulate focuses on the usage of SOA for information systems design, with the intention of finding relevance for developing Intelligence IIS.

The third postulate describes end users' functionalities for the IIS, which can be explored from different aspects. Intelligence, as an end user of IIS, is based upon intelligence disciplines which are further divided to sub-intelligence disciplines.

The fourth postulate refers to the future development of the IIS. Information infrastructure should be adoptable and flexible in order to fully support information sharing process.

The fifth postulate suggests the need for implementation of security standards for achieving adequate security level.

These five postulates promote the SOA system as a most appropriate IT infrastructure for IIS purposes, with minimum requirements for designing services that are needed in the intelligence process and internal functions available for processing from external IIS peer [11].

III. SECURITY ISSUES OF A SOA-BASED IIS SECURITY GAMES)

Networked systems' security is subjected to acts that compromise its confidentiality, integrity and availability or to attempts for obtaining control over a computer or communication network. The types and the scale of security threats can vary according to the specific use of the system. A malicious attacker of an Intelligence System could exhibit activities towards information theft, information alteration, misinformation or system impairment.

The IIS is a distributed computer system, which makes it prone to numerous security threats. Its most vulnerable points lie within the network connectivity, where the communication rules between the hardware, the software and the users are organized around protocols at different layers (such as application, transport, network, link and physical layer). From a security perspective, each of these protocols has weakness that could open a door to a malicious user: privacy concerns resulting from the poor authentication form of the HTTP, spoofed e-mail opportunities with SMTP, a large scale attack possibility due to the distributed architecture of DNS, denial of service (DoS) attack during client-server connection through TCP, poor security as a result of packages' fragmentation in IP, collision and corruption of packages in the Ethernet protocol, ARP cache poisoning etc.

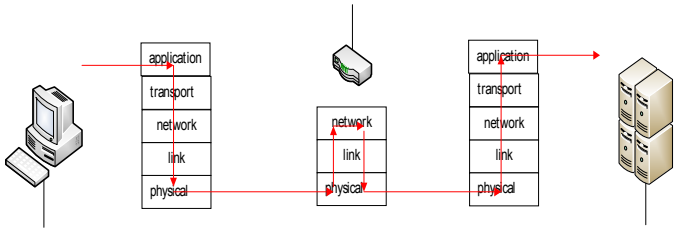

Figure 2. Presentation of layers and data transport

DoS attacks typically evolve in two parts. Firstly, the vulnerabilities of the system are exploited and second, attack tools (command messages) are installed through the network channels. The defense mechanisms that are proposed against DoS attacks can be divided into three groups of actions which are of preventive, detective and reactive nature.

Other types of malicious attempts can compromise the confidentiality of the system through an unauthorized access to information, which can be stolen, modified or falsified. Malicious software can be used to compromise network nodes. Backdoors implanting, Port Scanning, Remote Password Cracking are some of the attacking tools. The types of attacks as well as possible defense mechanism against them have been widely discussed in the literature and we will, at this point, refrain from further discussion on the issue.

IV. GAME THEORY AND INFORMATION SYSTEMS (SECURITY GAMES)

The theory of games is a formal way of conducting interaction analysis within a group of rational, strategically behaved agents. During a game (or a play), the actions that are undertaken by a participant (i.e. player) influence, to a varying degree, the actions of her opponents. In addition, a specified amount of awareness of the game elements (including other agents' strategies and utilities), as well as of rationality of the

players, is assumed. Together with the action profiles space and the available knowledge structure, these elements make the constituting parts of an initial game description.

By applying security game analysis, we try to detect appropriate protective countermeasures for the information system, obtain suggestions for effective resources allocation and analyze the behavior of the malicious agents that compromise the system's security. A security game consists of four components: players, actions sets for each of the players, the outcome of each player interaction and the information structure of the game. In a two-player non-cooperative security game, we observe an attacker (A) and a defender (D), each with a set of available strategies, further on also referred to with A and D.

The game matrices of A and D represent the estimated gain (or loss) of each player for pure strategy profiles. Having in mind the characteristics of an intelligence system, we consider the gain, for both of the players respectively, to be estimated in relation to a couple of general features*: the availability* (which refers to urgency, timeliness, connectivity etc.) and *the quality* of the information (including its significance for the observed issue, its accuracy and confidentiality).

Two models of security games will be presented. The stochastic game model assumes variable state of game with knowledge about game elements, while the fictitious play (FP) process of game learning takes place in an invariable state of game, but without knowledge of adversaries' profiles and utilities. The FP model still embodies an element of stochasticity, by taking into account the uncertainty of observations and decisions. Both models are discrete and produce probabilities of the expected attacker behavior, which are further used for assessing the security status of the system.

The solution concept we adopt is the Nash Equilibrium (NE), where both players adopt strategies that are the best response to the strategy played by their opponent. Although this imposes strong assumptions about players' rationality, it was shown (*J.Nash 1950*) that NE exists for finite n-player games, albeit not always in pure strategies. The (stochastic) fictitious play process has also good convergence properties for two-player games (see for example [2], [3], [6])

A. Stochastic Game Security Model

The stochastic nature of the game intends to capture the complexities and/or unknown parameters of the security problem at hand. A typical stochastic security game scenario takes place in a networking computer environment, with application servers, database servers, firewalls, cryptographic devices etc. In a SOA-based IIS, services possess individual targeting specifics as well.

The type of hardware, software, bandwidth, user privileges, connectivity etc. describe the state of the system, which changes according to situation developments. A state can be the operational modus of the networked system (functionality of the units, node connectivity, users' privileges, active countermeasures, compromised parts of the system etc.) The more detailed the state presentation is, the more accurate but complex and difficult to analyze the model will be. States can be encoded in the model in various ways. By using for example, a binary representation scheme (1 for active and 0 for inactive components of the system), each of these states could be represented as a binary string of a finite length.

Let $S=\{S_1,S_2,\ldots,S_n\}$ be a finite set of states with a given initial probability distribution $\bar{p}_0=(p_1,\ldots,p_n)$. At a period t, the system will be in one of the states $s(t)\in S$. The transition from one state to another is governed by probability distributions, which depend on the outcome of the immediate game. In reality, some of the transitions will be infeasible, which will be expressed by a zero value of the corresponding transition probability. If we define p_{ij} to be the probability of game's environment transit from state S_i to the state S_j, then we have $\sum_{j=1}^{n} p_{ij}=1$.

For each pair of actions (a,d), $a\in A$, $d\in D$, a state transition probability matrix $\mathbf{M_T}(a,d)$ of order n^2 is given. The probability description of the system's status will change according to

$$\bar{p}(t+1)=\mathbf{M_T}(a,d)\cdot\bar{p}(t). \quad (1)$$

The utility function L of the game reflects the anticipated defender's loss as a result of attacker's actions. Its value can otherwise be interpreted as attacker's gain. Clearly, D wants to minimize the value of L, while at the same time A tries to maximize it. The overall setting is that of a zero-sum game. We will observe the game from the viewpoint of the defender and further on, we will refer to L as the loss function.

Let the game loss matrix for each $S_j\in S$ be given with $G(S_j)=[l_j(d_i,a_i)]_{d_i\in D,\,a_i\in A}$ [1] where the value of $l_j(d_i,a_i)$ is the expected outcome loss for the defender when the action profile (d_i,a_i) is played. If in time period t the game is in a state $s(t)\in S$, then the game matrix will be $G(s(t))\in\{G(S_1),\ldots,G(S_n)\}$. The average loss for D in a finite τ-stage game is estimated by

$$L(t)=\sum_{t=1}^{\tau}\bar{p}_k(t)\cdot O^{(t)}, \quad (2)$$

where $O^{(t)}$ is the NE outcome value of the game at stage s(t), $O^{(t)}=l(\delta^{(t)},\alpha^{(t)})$ with $\delta^{(t)}$, $\alpha^{t)}$ being the optimal strategies (pure or mixed) for D and A at time t. The weighting coefficients $\bar{p}_k(t)$ represent the probability that the system is in state S_k at time t, according to (1).

The solution algorithm for the game can be formulated by a dynamic programming approach. Using recursion, we can inductively obtain the expressions for the optimal value and

[1] Since not all of the actions are applicable in a given state, some of the rows'(columns') elements of this matrix may be zeros i.e. the order of the matrix may be less than |D|×|A|.

the total discounted costs respectively for player D in a state $s \in S$ at stage t,

$$V(s) = \min_{\mu_s} \max_{a \in A} \sum_{d \in D} L_t(s,d,a) \cdot \mu_s(d), \text{ where} \quad (3)$$

$$L_t(s,d,a) = G(s)_{(a,d)} + \beta \cdot \sum_{s' \in S} \mathbf{M}_{\mathbf{T}(s,s')}(a,d) \cdot V(s'), \quad (4)$$

for all t = 1,2,…., μ a mixed strategy for D and $\beta \in [0,1)$ an estimated discount factor. When satisfactory convergence criteria are met, we can obtain from (3) and (4) the optimal defense strategy $\bar{\mu}_S$ and the value $\bar{L}$ (i.e. the loss) that D can expect. The dual (maximin) formulation to this model will provide the optimal attack strategy for A.

We can now formulate the algorithm for solving a stochastic security game.

Value iteration algorithm for a stochastic security game.

1. For all $s \in S$, $d \in D$, $a \in A$ enter values for $L_0(s,d,a)$;
2. Calculate V(s)
3. **repeat**
4. **for** $d \in D$, $a \in A$ do
5. update L(s,d,a) according to (**)
6. update V(s) according to (*)
7. **end for**
8. **until** convergence of V(s)

B. Fictitious Play Security Model

In practice, game engagement is often accompanied by lack of knowledge about the opponents or inaccuracy of the received information, or both. When we lack specific knowledge about our opponents, than we cannot a priori formulate a sustained opinion about their future actions, the personal utilities related to them and consequently, the mixed strategy they will consider the most beneficial. On the other hand, sensor systems that are supposed to report an attack are imperfect and there is always a positive probability for a false positive or negative attack alerts on both sides. Furthermore, the rationality of the players is not error prone as well, and if these factors are summed up then considering an incomplete information game becomes a must.

Once involved in a game, a way out of this situation is to proceed according to observations by trying to determine the best move for our gains. When applying a fictitious play updating of the game knowledge, we assume that our opponents' play unrolls according to a defined, but unknown strategy distribution. Players have no access to the other's player utility function and adjust their strategy choice according to the observations. In such circumstances, the IIS defender will proceed as follows:

(a) Count the appearance of each attacking action a_i and generate an associate frequency value $\nu(a_i)$,

(b) Create the related empirical probabilities for each observed attacking action in period t,

$$p_i(t) = \frac{\nu(a_i)}{\sum_{j=1}^{k} \nu(a_j)} \quad (5)$$

(c) Update the mixed strategy profile of the attacker, $\gamma(t) = (p_1(t), \ldots, p_k(t))$,

(d) Calculate her best response to this profile according to her game matrix D,

$$\beta(t) = \arg\max_{\mu} \left(\mu^T D \gamma(t) + \rho H(\mu) \right), \text{ and} \quad (6)$$

(e) Observe the next attacker's move.

Here, μ is strategy profile of D, H is the entropy function given by $H(\mu) = -\mu^T \cdot \log(\mu)$ which covers for the uncertain observations and decisions and ρ is a non-negative parameter expressing D's tendency toward randomization of her actions. It is assumed that on the opposite side, the attacker is applying the same procedure resulting in a subsequent best response action.

For strictly positive values of ρ in (6), the FP model is stochastic. If both players set a zero value for this parameter, it will remove the stochasticity and result in the classical FP model. The most important implication is that in the later case we can expect a set-valued result from the best response maximization, while in the former case the resulting best response strategy is unique.

Fictitious play algorithm.

1. Given a payoff matrix,
2. **for** t = 1, 2, …
3. update the actions' empirical frequency of the opponent,
4. pick an optimal pure strategy from ( ) (randomizing the choice if needed),
5. **end for**

In [15], a time-invariant model of stochastic fictitious play for security games has been considered and asymptotic stability results for the dynamics have been given. This approach is inspired by the realistic expectations that firstly, players would want to take individual time steps for the next move instead of synchronizing their actions and secondly, they would tend toward adjusting the history of the play by weighting observed actions, thus speeding up the strategic convergence towards equilibrium. Whereas in the time-variant model presented above we have an updating equation for the *observed* opponent play given by

$$\gamma(t+1) = \frac{t}{t+1}\gamma(t) + \frac{1}{t+1}s(t), \quad (7)$$

the time-invariant version gives the following *estimation*:

$$\bar{\gamma}(t+1) = (1-\eta) \cdot \bar{\gamma}(t) + \eta \cdot s(t) \quad (8)$$

for some $\eta \in (0,1)$. In the equations above, s(t) is the pure strategy unit vector.

The mean dynamic of the time-invariant FP for each of the players is given by

$$\bar{\gamma}_i(t+1) = (1-\eta)\cdot\bar{\gamma}(t) + \eta\cdot\beta(\bar{\gamma}_{-i}(t)) \quad (9)$$

where *i* stands for either of the defending or attacking player, -*i* for the opposite player and β for the respective player's best response. The mean dynamics of the empirical strategic frequencies will thus be calculated according to

$$\gamma_i(t+1) = \frac{t}{t+1}\gamma_i(t) + \frac{1}{t+1}\beta(\bar{\gamma}_{-i}(t)), \quad i \in \{A, D\}. \quad (10)$$

The mean dynamic of the time-invariant model is shown to be asymptotically stable for estimated values of the parameter η.

V. CONCLUSION

Security of a networked system is a problem that is far from its final solution. Even if a good defense model comes at hand, it is very likely that it will soon be outsmarted by some inspired and not well-minded user, which can be somewhere far on the world wide web and quite beyond the control of those who are supposed to defend the system (the administrators). Braking complex encryption schemes or performing various deceptive actions is not so uncommon nowadays, so pushing and pulling information trough a network becomes a high risk endeavor.

In a SOA-based Intelligence Information System, networked system's security vulnerabilities are emphasized by concerns of even higher level, due to the nature and significance of the circulated information. Its defense strategies should be developed and analyzed very carefully, always with a thought that there is no perfect mechanism i.e. a solution to all security challenges.

In this context, game theory emerges as a useful and cost-effective tool for analysis, prediction and planning of defense activities. It can offer a way around the problem of lacking a quantitive decision framework, such is the case with other network security solutions. This is especially important when having in mind that intelligent, proactive adversaries are often at hand, which could render some of the other mathematical analyzing tools inapplicable or exceptionally consuming. The use of games in analyzing security issues creates opportunities for examining numerous attack scenarios, calculating possible outcomes and suggesting directions for the future course of actions.

Computer implementation of security game models has already been considered, implemented and discussed in the literature. It provides for an automated decision process which significantly contributes to the security treatment. The models presented in this article have both advantages and disadvantages. A state-dependent model such as the stochastic game, can provide for a more authentic game environment but on the flip side, the state space can be very large. To simplify the calculations, we may be compelled to restrict to a much smaller subset of states and consider suitable presentation patterns for them. In addition, determining the actions of both parties, in particular of the attacker, is another challenge for the model building. Opponent's true strategy set is especially case sensitive in the FP model, since the concept does not account for actions that have not been previously observed, even though they might be very plausible.

The future challenges are related to the implementation of game models to the specifics of the IIS setting and its service-oriented architecture. SOA components are loosely coupled and exposed as independent services on a network. The intelligence disciplines that are related to the services of the IIS involve human, image, signal, open source and other types of intelligence analysis, employing diverse resources which differ both in nature and functionality. In this light, a successful model will develop around a good quantitative estimation of parameters, carefully specified attitude towards inevitable tradeoffs (prioritize security, system performance, utilities, defense costs or other important features), testing of various defense techniques and their combinations through simulation

REFERENCES

[1] L. S. Shapley, "Stochastic Games", Proceedings of the National Academy of Science USA, vol 39, pp. 1095-1100 , (1953)

[2] D.Fudenberg, J.Tirolle, "Game Theory", MIT Press, 1991

[3] G. Schoenmakers, J. Flesch, and F. Thuijsman, "Fictitious Play in Stochastic Games", Maastricht University, Department of Mathematics, 2001

[4] N.Williams, "Stability and Long Run Equilibrium in Stochastic Fictitious Play", Department of Economics, Princeton University, 2002

[5] K. Lye, J.M. Wing, "Game strategies in network security", In Proceedings of the 15th IEEE Computer Security Foundations Workshop, 2002

[6] U.Berger, "Fictitious Play in 2xn Games", Journal of Economic Theory 120.2: 139-154, 2005

[7] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection", Proc. of the 42nd IEEE Conference on Decision and Control, pages 2595–2600, Maui, HI, December 2003

[8] E.A Hansen,. D.S. Bernstein, and S.Zilberstein, "Dynamic programming for partially observable stochastic games", Proceedings of the National Conference on Artificial Intelligence, 2004

[9] K.Sallhammar, S. J.Knapskog, and B. E. Helvik, "Using Stochastic Game Theory to Compute the Expected Behavior of Attackers", Proceedings of the Intl. Symposium on Applications and the Internet (SAINT 2005), Trento, Italy

[10] P.Liu, W.Zang and M.Yu.,"Incetive-based modeling and inference of attacker's intent, objectives and strategires", ACM Transactions on Information and System Security (TISSEC), 2005

[11] T. Alpcan, T. Basar, "An intrusion detection game with limited observations", 12th International Symposium on Dynamic Games and Applications, Sophia Antipolis, France, July 2006

[12] Y.Liu and H.Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks", Workshop on Game Theory for Communications and Networks, 2006

[13] K. C. Nguyen, T. Alpcan, and T. Basar, "Security games with incomplete information", Proc. of IEEE International. Conference on Communications (ICC 2009), Dresden, Germany, June 2009

[14] S.Roy, C.Ellis, S Shiva., D.Dasgupta, V.Shandilya and Q .Wu, "A Survey of Game Theory as Applied to Network Security", Proceedings of the 43rd HICSS, Hawaii, 2010

[15] K. C. Nguyen, T. Alpcan, and T. Basar,." Fictitious play with time-invariant frequency update for network security", Proc. of IEEE International Conference on Control Applications (CCA), 2010

[16] J.Ackoski, V.Trajkovik, and D. Davcev, "Service-Oriented Architecture Concept for Intelligence Information System Development," The Third Intl. Conferences on Advanced Service Computing (IARIA 2011), Rome, Italy, September 25 - 30, 2011