A Stochastic Game Theoretic Approach to Attack Prediction and Optimal Active Defense Strategy Decision

Wei Jiang, Zhi-hong Tian, Hong-li Zhang, and Xin-fang Song

***Abstract*—This paper presents a stochastic game theoretic approach to analyzing attack prediction and the active defense of computer networks. A Markov chain for privilege (MCP) model to predict attacker's behavior and strategies is proposed. We regard the interactions between an attacker and the defender as a two-player, non-cooperative, zero-sum, finite stochastic game and formulate an attack-defense stochastic game (ADSG) model for the game. An attack strategies prediction and optimal active defense strategy decision algorithm is developed using the ADSG and cost-sensitive model. Optimal defense strategies with minimizing costs are used to defend the attack and harden the network in advance. Finally, a simple example of an attack against a network is modeled and analyzed.**

I. INTRODUCTION

TRADIRADITIONAL static protective measures are not sufficient to secure a complex networked system. Existing cyber security technologies can only passively prevent, detect, and react to cyber attacks. Intrusion detection (ID) architecture is a passive information processing paradigm. In many cases intrusion response is "too late" after very serious damage is caused. Attack prediction is very critical for cyber homeland security. It is a big challenge that making correct optimal proactive real-time defense decisions during an earlier stage of the attack. In such a way we can transform passive to proactive cyber defense, and much less harm will be caused without consuming a lot of resources.

Probabilistic methods have been recently proposed by several studies for a theoretical analysis of quantifying the operational security of networked computer systems [1]-[5]. Those research efforts have focused on using state transition to model attacks and system restoration. Ortalo et.al [1] describes a methodology for modeling known UNIX security vulnerabilities as a privilege graph. They describe a technique for transforming a privilege graph into a Markov chain. The states of the resulting Markov chain denote the enhanced privileges gained by an attacker as a result of series of atomic attacks on a system. The arcs on the other hand, represent the effort e spent by an attacker to cause state transitions in this Markov chain. This model allows the evaluation of the proposed measure of operational security mean effort to security failure, analogous to mean time to failure. Swiler et.al [2] use attack graph to model the security vulnerabilities of a system and their exploitation by an attacker. Madan et.al.[3] uses traditional stochastic modeling techniques to capture attacker behavior and the system's response to attacks and intrusions. A quantitative security analysis is carried out for the steady state behavior of the system.

Game theoretical analysis is useful for analyzing, modeling, decision, and control processes for network security. Game theory has been recently proposed by several studies for a theoretical analysis of network security [4]-[9]. Sallhammar et al. [4, 5] presents a stochastic model for integrated security and dependability assessment. By using stochastic game theory they can compute the expected attacker behavior for different types of attackers. Lye and Wing [6] use a game theoretic method to analyze the security of computer networks. They regard interactions between an attacker and the administrator as a two-player stochastic game. And give a concrete example in detail where the attacker is attacking a simple enterprise network that provides some Internet services such as web and FTP. A set of specific states regarding this example are identified, state-transition probabilities are assumed, and the Nash equilibrium or best-response strategies for the players are computed. Peng Liu et al. [7] present a preliminary framework for modeling attacker intent, objectives and strategies (AIOS) using game theoretic approach. Alpcan[8] et al. investigated the basic decision and analysis processes involved in information security and intrusion detection, as well as possible usage of game theory for developing a formal decision and control framework. Xu and Lee [9] use game-theoretical framework to analyze the performance of their proposed DDoS defense system and to guide its design and performance tuning accordingly.

Our work is different from the above game theoretic works in several aspects. First, these works are complex and can not proactive defense in real time, while our work focuses on active defense using the ADSG model. Second, we present Markov chain for privilege model to predict attacker's behavior and strategies. Third, we present a new privilege-escalating attack taxonomy, with respect to the attacker's privileges elevation from lower level to higher level. Finally, our work systematically identifies cost factors of cost-sensitive model and introduces the attack strategies prediction and optimal active defense strategy decision algorithm.

This paper is an extension of our previous work [10]. Compared with our previous work, a new Markov chain for privilege model and privilege-escalating attack taxonomy

Manuscript received October 1, 2007. This paper is supported by the National High-Tech Research and Development Plan of China under Grant Nos. 2007AA01Z406, 2007AA01Z442.

Wei Jiang, Zhi-hong Tian and Hong-li Zhang are with Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin, 150001, China (phone: +86 13811532569; fax:+86 451 86413331; e-mail: jiangwei@pact518.hit.edu.cn).

Xin-fang Song is with Beijing Jingbei Vocational Campus, Beijing, China (e-mail: xfsong435@yahoo.com.cn).

method are presented. What's more, we develop an attack strategies prediction and optimal active defense strategy decision algorithm using our ADSG model. The significance of this work and the benefit to the public can be shown as fellow. First, it is important to predict attacker' behavior for active defense. Second, it is important to take defense strategies with minimizing costs for attacks occurring in the future.

The remainder of this paper is structured as follows. In Section 2 we present formalization definition of the MCP model, ADSG model and discuss the cost-sensitive model. Section 3 describes the attack strategies prediction and optimal active defense strategy decision algorithm. Section 4 includes some concluding remarks and points to future work.

II. MODEL FORMALIZATION

A. The Markov Chain for Privilege Model

The stochastic process describing the dynamic system behavior is a continuous time Markov chain with discrete state space. Let

$$X(t) = \{X_1(t), X_2(t), \ldots, X_N(t)\} \qquad (1)$$

Where $X_i(t)$ denotes the system is in state *i* at time *t*. The interaction between the states in (1) can be displayed by a state transition matrix. In order to model and predict attacker's behavior and strategies, we formal a Markov chain for privilege (MCP) model. We assume that, initially, the attacker knows about all vulnerabilities and will successfully exploit all reachable vulnerabilities to their fullest effect; the attacker has fewer privileges of system (system can be any kind, e.g., a network system, a distributed system, a database system) and only through successful attacks that give him more privileges. The attacker's privilege changes as a result of his progress toward the target can be characterized by a state transition model where each state identifies the set of privileges that he has already gained and transitions between states occur when the attacker succeeds in an atomic attack, allowing him to acquire new privileges.

Assume that each attacker' privileges can be modeled by *N* different states, i.e. $S = \{s_1, \ldots, s_N\}$. The state of privileges changes over time. The sequence of states visited by an attacker' privileges are denoted $X = x_1, x_2, \ldots, x_T$, where $x_t \in S$ and $x_1 \le x_2 \le \ldots \le x_T$, which indicates that privileges are elevated when the attacker succeeds in an atomic attack on some vulnerability.

The probability that the attacker will choose attack *i* in state *k*, denoted as $p(a_i^k)$, Hence, for each state *k* in the state transition model, the attacker's expected choice of attack can be represented by a probability vector $(p(a_1^k), \cdots, p(a_{M_k}^k))$ where $\sum_{i=1}^{M_k} p(a_i^k) = 1$. And the complete set of decision probability vectors for the state transition model is a matrix:

$$P = \begin{pmatrix} p(a_1^1) & \cdots & p(a_{M_k}^1) \\ \vdots & & \vdots \\ p(a_1^z) & \cdots & p(a_{M_k}^z) \end{pmatrix} \qquad (2)$$

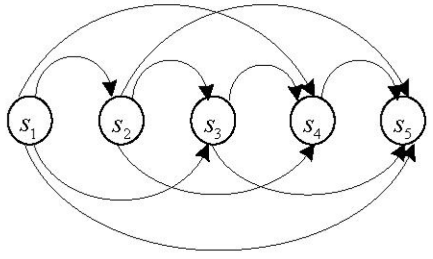
The probability that an attacker may cause a transition of attacker' privileges from state k to state l can therefore be computed as $p(x_{t+1} \mid x_t = k) = p(a_i^k) p_s(a_i^k)$ where $p_s(a_i^k)$ is a success probability of the atomic attack *i*.

The MCP modeled in this paper are assumed to have five possible privilege states $S = \{s_1, s_2, s_3, s_4, s_5\}$, where $s_1 \le s_2 \le s_3 \le s_4 \le s_5$, and they are defined as table I.

TABLE I
ATTACKER' PRIVILEGES STATES DESCRIPTION

Symbol	Privileges Category	Description
s_1	Internet remote access	Accessing only by some public protocol or service of Internet.
s_2	No shell accounts	The user can find the file, directory, user and device of target system.
s_3	Local common user access	The user not only can read, write, and modify some information on the target system, but also can install some user level program.
s_4	Root user access	The user not only can read, write, and modify any information on the target system, but also can install any program.
s_5	Full access to host	The user can manipulate all characteristics of the system.

Figure 1 shows the Markov model for of attacker' privileges states. The edge from one node to another represents the fact that when an attacker' privileges is in the state indicated by the source node it can transition to the state indicated by the destination node. Note that the graph is not fully connected, which indicates that each atomic attack strictly increases either the intruder's privilege level on the target host or remote login trust between hosts. This means that the attack graph has no cycles.



B. Attack-Defense Stochastic Game Formalization

Definition 1: A two-player zero-sum attack-defense stochastic game is a 5-tuple (N, G, S, Q, U):

- The set, $N = \{attacker, defender\}$, is two players who are attacker and defender.
- G consists of a finite set of positions or states, $G^{(k)}$, k= 1,..., z.
- $S = (S^1, S^2)$ is the strategy spaces of the

players. $\forall i = 1,2,\ \ S^i \neq \varnothing$, $S^i = (s_1^i, s_2^i, \ldots, s_{M^i}^i)$ is strategy set of the player i and $M^i = |S^i|$. The strategy set for player i at state s is a subset of S^i, i.e., $S_s^i \subseteq S^i$ and $\bigcup_{k=1}^{z} S_k^i \subseteq S^i$.

- Q is the state transition function.
- The set, $U = (U_1, U_2)$, of real-valued is payoff functions of the players. And $U_1 = -U_2$.

We denote by $G^{(k)}$ the game in which k is the starting position. Associated with each state, k, is a matrix game, $U^{(k)} = (u_{ij}^{(k)})$. If the attack-defense stochastic game is in state k, the players simultaneously choose a row and column of $A^{(k)}$, say i and j. As a result, attacker wins the amount $u_{ij}^{(k)}$ from defender. And with probabilities that depend on i, j and k, the game either stops, or it moves to another state (possibly the same one). The probability that the game stops is denoted by $s_{ij}^{(k)}$, and the probability that the next state is l is denoted by q_{ij}^{kl}, where

$$s_{ij}^{(k)} + \sum_{l=1}^{z} q_{ij}^{kl} = 1 \qquad (3)$$

for all i, j and k.

The payoffs accumulate throughout the game until it stops. To make sure the game eventually stops, we make the assumption that all the stopping probabilities are positive. Let s denote the smallest of these probabilities.

$$s = \min_{i,j,k} s_{ij}^{(k)} > 0 \qquad (4)$$

So the probability is one that the game ends in a finite number of moves. This assumption also makes the expected accumulated payoff finite no matter how the game is played, since if M denotes the largest of the absolute values of the payoffs, $M = \max_{i,j,k} |a_{ij}^{(k)}|$, then the total expected payoff to either player is bounded by

$$M + (1-s)M + (1-s)^2 M + \cdots\cdots = M/s. \qquad (5)$$

The attacker wishes to maximize the total accumulated payoff and the defender to minimize it.

Each state is specified as the starting position and is represented by a matrix $G^{(k)} = \left(u_{ij}^{k} + \sum_{l=1}^{z} q_{ij}^{kl} G^{(l)}\right)$.

C. Strategies, Reward and Cost for the Two Players

Attacker's strategies were depended on attack taxonomy. An important and sensible goal for attack taxonomy would be to help the defender. We present a new, privilege- escalating attack taxonomy, with respect to the attacker's privileges elevation from lower level to higher level. It is much more useful for a defender than other attack taxonomy in our ADSG model. Such the taxonomy would classify attacks in a way that the attacker has gain by a successful atomic attack. Our attack taxonomy is detailed as table II. For example, probes are actions taken by an attacker to gather information about the system including machines, services and users.

TABLE II
ATTACK TAXONOMY DESCRIPTION

Symbol	Category	Damage cost
s_1^1	Probe	Dcost=2
s_2^1	Illegal common access is obtained	Dcost=20
s_3^1	Run suspicious program	Dcost=50
s_4^1	DDoS attack	Dcost=80
s_5^1	Illegal root access is obtained	Dcost=100
s_6^1	Crash host/service	Dcost=150

In order to quantify costs and rewards, we should first understand the relevant cost factors used to define them. Cost factors are often site-specific because each organization has its own security policies, information assets, and risk factors. Based on the investigation of Lee's and our previous research [10], [11], we build our cost model which includes cost factors as follow: defense operation cost (*DOcost*), residual damage cost (*RDcost*) , damage cost (*Dcost)* and defense negative cost (*DNcost*). *DOcost* is the amount of resources needed to defense an attack (type). We classify defense operation cost into three relative levels, based on their computational costs:

L1: defense operation cost is very small. For example, suspend process, IP blocking.

L2: use some system resources when defense operations were carried out. For example, kill the process.

L3: use much more system resources when defense operations were carried out. For example, create backup.

We can assign relative magnitudes to these features according to their computational costs. For example, Lee assigns a different cost weight level. A level 1 feature may cost 1 to 5, level 2 features may cost 10, and level 3 features may cost 100. In table III, we list a number of known defense strategy and their levels.

TABLE III
DEFENSE STRATEGY DESCRIPTIONS

Defense strategy	Implementation requirements	*DOcost*
Generate Alarm	Kernel	L2
IP Blocking	Kernel	L1
Isolate Host	Kernel or User	L2
Suspend Process	Kernel	L1
Kill Process	Kernel or User	L2
Create Backup	User	L3
⋮	⋮	⋮
No defense	No	No

Some defense strategy cannot defend the attack that may occur in the future result in some attack damage. So we must consider the *RDcost* of a defense strategy, and we can quantify it as fellow: $RD\cos t(d) = \varepsilon \times D\cos t(a)$. Where $\varepsilon \in [0,1]$ is the degree damage cost of attack a when take defense strategy d. *Dcost* generally quantifies the maximum amount of resources or computing power that can be left unusable by the particular attack. *Criticality* measures the importance of the target of an attack. Similar to Northcutt's analysis [12], we assign 5 points for firewalls, routers, or DNS servers, 4 points for mail or Web servers, 2 points for UNIX workstations, 1 point for workstations. *Lethality* measures the degree of damage that could potentially be caused by some attack. Wenke Lee defines a relative lethality scale and uses it as the base damage cost [11]. The *Dcost* of an attack targeted at some resource is $criticality \times lethality$, identified as table II.

DNcost represents an effect of a defense action on a target system, which depends on defense strategies and target system. We can quantify the *DNcost* in the particular environment and defense action. For example, *DNcost* can be defined as follows: $DN\cos t(d,t) = availability \times \mu_a$. $\mu_a \in [0,1]$, and it is denoted the degree of *availability* of the target system *t*.

After the cost factors are defined, the cost values can be given when defense strategies cost analysis and assessment. The total defense cost (*TDcost*) of a defense strategy can be defined as follows:

$$TD\cos t = DO\cos t(d) + RD\cos t(a) + DN\cos t(d) \qquad (6)$$

In the above *d* and *a* is separately a particular defense strategy and attack type.

D. Solve the ADSG's Nash Equilibrium [13]

In stochastic games, the value and optimal strategies for the players exist for every starting position. Moreover, optimal strategies exist that have a very simple form. Strategies that prescribe for a player a probability distribution over his choices that depend only on the game, G^k, being played and not on the stage $n\psi$or past history are called *stationary strategies*. The following theorem states that there exist stationary optimal strategies.

Theorem 1 [13]: Each game G(k) has a value, v(k).These values are the unique solution of the set of equation,

$$v(k) = Val\left(u_{ij}^{(k)} + \sum\nolimits_{l=1}^{z} q_{ij}^{kl} v(l)\right) \text{ for k = 1, ... , N.} \qquad (7)$$

Each player has a stationary optimal strategy that in state k uses the optimal mixed strategy for the game with matrix

$$G^{(k)}(v) = \left(u_{ij}^{(k)} + \sum\nolimits_{l=1}^{z} q_{ij}^{kl} v(l)\right) \qquad (8)$$

Where v represents the vector of values, $v = (v(1), \ldots, v(z))$.

For a general ADSG with many states, equations (7) become a rather complex system of simultaneous nonlinear equations. We can use a simple iterative method of approximating the solution to solve such systems in general. This is based on Shapley's proof of Theorem 1.

First we make a guess at the solution, call it $v_0 = (v_0(1), \ldots, v_0(N))$. Any guess will do. We may use as the initial guess, $v_0 = (0, \ldots, 0)$. Then given v_n, we define inductively, v_{n+1}, by the equations,

$$v_{n+1}(k) = Val\left(u_{ij}^{(k)} + \sum\nolimits_{l=1}^{z} q_{ij}^{kl} v(l)\right) \text{ for } k = 1, \ldots, N. \qquad (9)$$

With $v_0 = \mathbf{0}$, the $v_n(k)$ have an easily understood interpretation. $v_n(k)$ is the value of the stochastic game starting in state *k* if there is forced stopping if the game reaches stage *n*. In particular, $v_1(k) = \text{Val}(G^{(k)})$ for all *k*.

The proof of Theorem 1 shows that $v_n(k)$ converges to the true value, $v(k)$, of the stochastic game starting at *k*.

III. Attack Strategies Prediction and Optimal Active Defense Strategy Decision Algorithm

In this section we describe how a stochastic game theoretic model can be used to predict attack strategies and decide optimal active defense strategy algorithm compute the expected attacker behavior, in terms of a set of strategies $S = (s_1, s_2, \ldots, s_{M^i})$. The procedure is as follows:

1) *Identify the game elements:* From the MCP model, pick all privileges states of the attacker. Each of these states can be viewed as a game element $G^{(k)}$ *in* the two-player, zero-sum, stochastic game *G*.
2) *Construct the attacker's strategy set* S^1 *:* S^1 consists of all possible attack strategy. For all transitions out of the game element states which represent intrusions, identify the corresponding attack strategy. All strategy will not necessarily be available in all states; we use $S^1(k) = (s_1^1, s_2^1, \ldots, s_m^1)$ to refer to the set of strategy available in state *k*.
3) *Construct the defender's strategy set* S^2 *:* S^2 consists of all possible defense strategy. We use $S^2(k) = (s_1^2, s_2^2, \ldots, s_n^2)$ to refer to the set of strategy for $S^1(k)$ from known defense strategy set.
4) *Compute the reward of strategies:* For each game element, we assign the reward values to each attack strategy and defense strategy. The reward of attacker and defender is zero-sum, which as computed equation (6).
5) *Calculate transition probabilities of the game states:* The estimation of the appropriate values for the probability vector ($p(a_1^k), \cdots, p(a_{M_k}^k)$) and model parameters *P* can be determined using either training algorithms or expert knowledge, supported by an appropriate methodology.
6) *Solve the ADSG model:* From 1)-5), we have completed the initialization of the ADSG=(N,G,S,Q,U).The last step is to solve the game model. Solving the model means to compute the best strategies for the players who participate in the game.

The set of minmax solution vectors for the game elements G(k), *k* = 1,...,*N*, in the stochastic game model represents a complete attack and defense strategy. For example, the attacker follow minmax solution and he will know that he has maximized his expected payoff of the attack. For the same, optimal defense strategy with minimizing costs can be decided.

IV. Implementation Issues

As our previous work [10], we can use a simple example network, which is similar to Sheyner's [2], in our experiment to test the MCP and ADSG model. The network illustrated in figure 2. The firewall is open and does not place any restrictions on the flow of network traffic. Some important host information is given in table IV.

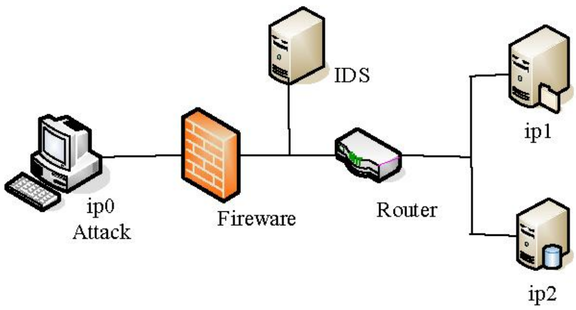


Fig. 2. Example Network

TABLE IV
SUMMARY OF HOST INFORMATION

Hostid	Services	Vulnerability
ip1	ftp, ssh	sshd buffer overflow, ftp .rhost overwrite
ip2	ftp, database	ftp .rhost overwrite, local buffer overflow

There are three possible atomic attacks, identified as follows: (a$_1$) sshd buffer overflow, (a$_2$) ftp .rhosts, and (a$_3$) local buffer overflow. Summary of atomic attack are shown in table V.

TABLE V
SUMMARY OF ATOMIC ATTACK

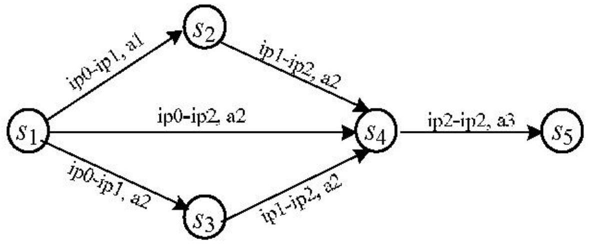
Atomic attack	Type	Vulnerability	Attack complexity	Dcost
a$_1$	Illegal root access is obtained(remote)	sshd buffer overflow	0.7	100
a$_2$	Illegal common access is obtained	ftp .rhost overwrite	0.5	50
a$_3$	Illegal root access is obtained(local)	local buffer overflow	0.3	100

We can construct the strategy set S^2 from table III for S^1 = {a$_1$, a$_2$, a$_3$}, as table VI.

TABLE VI
SUMMARY OF DEFENSE STRATEGY

Defense strategy	*DOcost*	ε
s_1^2 : Generate Alarm	10	$\varepsilon_0 = \varepsilon_1 = \varepsilon_2$ =0.8
s_2^2 : IP Blocking	5	$\varepsilon_0 = \varepsilon_1$ =0, ε_2 =1
s_3^2 : Isolate Host	10	$\varepsilon_0 = \varepsilon_1$ =0, ε_2 =1
s_4^2 : Kill Process	5	$\varepsilon_0 = \varepsilon_1$ =1, ε_2 =0.5
s_5^2 : No defense	0	$\varepsilon_0 = \varepsilon_1 = \varepsilon_2$ =1

Figure 3 shows the Markov privileges state graph that the attacker has on each host, where s_1 is initial privilege on ip0 and s_5 is the target privilege on ip2. It is easy to see that each atomic attack strictly increases either the attacker's privilege level on the target host or remote login trust between hosts. Initially, the attacker has root privileges on his own host ip0 and no privileges on the other hosts. The edge from one node to another represents the fact that the attacker' privileges transit resulting from the success of atomic attack. For instance, "ip0-ip1, a$_1$" represents that the attacker will choose attack a$_1$ from host ip0 to host ip1. The probability of success for atomic attack can be used to estimate the likelihood that an attacker will appear at a given point in the network and the performance of IDS.



s_1 : Root user access on ip0; s_2 : Root user access on ip1;

s_3 : Local common user access on ip1;

s_4 : Local common user access on ip2; s_5 : Root user access on ip2

Fig. 3. Markov privileges state graph

To simplify our analysis, we don't detail the solution of the ADSG model. The set of minmax solution vectors for the game elements *G*(5) in the stochastic game model represents a complete attack and defense strategy. We can find that the rational attacker will choose a$_2$ with higher probability at s_1. For the same, s_2^2 IP Blocking is the optimal defense strategy with minimizing costs. The defender should use optimal defense strategy to harden the network and the attack will be "contained", "isolated", or "defeated" before it causes deadly damage.

There are some implementation issues which must be resolved when the model is tested. For example, the generation of states in the MCP model. If there is a common set of attack strategies that allow an attacker to become root from a normal user account on the same machine, this could be a useful building block.

Another issue is how to estimate the parameters in our experiments. In fact, the parameters for our experiments were estimated manually. This is a time-consuming task with inherent uncertainties. The estimation of the appropriate values for the model parameters *P*, $p_s(a_i^k)$ and for the cost model can be determined using either training algorithms or expert knowledge, supported by an appropriate methodology.

Finally, how to demonstrate the probability and cost parameters in our MCP and ADSG model will affect the expected attacker behaviour and active defense decision.

V. CONCLUSION AND FUTURE WORK

In this paper, we have presented a stochastic game theoretic approach to analyzing attack prediction and the active defense of computer networks. On one hand, a Markov chain for privilege (MCP) model to predict attacker's behavior and strategies have been proposed. On the other hand, we developed a taxonomy of attack and defense for our model. Moreover, we regarded the interactions between an attacker and the defender as a two-player, non-cooperative, zero-sum, finite stochastic game and formulate an attack-defense stochastic game (ADSG) model for the game. Then, an attack strategies prediction and optimal active defense strategy decision algorithm has been developed using the MCP, ADSG and cost-sensitive model. **Finally, a simple example of an attack against a network is modeled and analyzed.**

Nevertheless, our work in attack prediction and optimal active defense decision is still preliminary and several important research issues need to be further explored. In particular, in our future work (a) we would detailedly improve our models **in order to get better** attack prediction and optimal active defense strategy decision; (b) we would investigate cost factors and quantified analysis of defense and attack; (c) we verify and analyses the ADSG model's ability to predict real-life attacks.

ACKNOWLEDGMENT

The authors gratefully acknowledge helpful discussions with some members in our research center. We also thank anonymous reviewers for their constructive suggestions.

REFERENCES

[1] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 25(5): pp.633–650, Sept/Oct 1999.

[2] S. Jha, O. Sheyner, and J. Wing. Two formal analyses of attack graphs. In Proceedings of the 2002 Computer Security Foundations Workshop, 2002.

[3] K. B. B. Madan, K. Vaidyanathan Goseva-Popstojanova, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems", In Performance Evaluation", volume 56, 2004.

[4] K. Sallhammar, S. J. Knapskog, and B. E. Helvik, "Using stochastic game theory to compute the expected behavior of attackers", in Proceedings of the 2005 International Symposium on Applications and the Internet (Saint2005) Workshops, 2005.

[5] Karin Sallhammar, B. E. Helvik and S. J. Knapskog, "Towards a Stochastic Model for Integrated Security and Dependability Evaluation", In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), 2006.

[6] K.-W. Lye and J. Wing, "Game strategies in network security," Foundations of Computer Security Workshop in FLoC'02, Copenhagen, Denmark, July 2002.

[7] P. Liu and W. Zang, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", Proc. of the 10th ACM Computer and Communications Security Conference (CCS'03), Washington, DC, October 2003, pp. 179-189.

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

[9] J.Xu and W. Lee, "Sustaining availability of web services under distributed denial of service attacks", IEEE Trans. Compute. 52, 4, pp.195–208, 2003.

[10] Wei Jiang, Zhi-hong Tian, Hong-li Zhang, and Xin-fang Song, "A game theoretic method for decision and analysis of the optimal active defense strategy", 2007 International Conference on Computational Intelligence and Security (CIS' 2007) , December, Harbin, China, to be published.

[11] W. Lee, W. Fan, M. Millerand, S. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response", Journal of Computer Security, volume 10, 2000, pp. 5–22.

[12] S. Northcutt. Intrusion Detection: An Analyst's Handbook, New Riders, 1999.

[13] L. S. Shapley (1953) Stochastic Games, *Proc. Nat. Acad. Sci.* 39, pp. 1095-1100