A Network Security Game Model

Vivek Shandilya
Dept of Computer Science
University of Memphis
Memphis, TN-38152
001 9018481763
vmshndly@memphis.edu

Sajjan Shiva
Dept of Computer Science
University of Memphis
Memphis, TN-38152
001 901 678 5465
sshiva@memphis.edu

ABSTRACT

There have been attempts to model the interaction between users, both malicious and benign, and network administrators as games. Building on such works, we here present a game model which is generic enough to capture various modes of such interactions. The model facilitates stochastic games with imperfect information. The imperfect information is due to erroneous sensors leading to incorrect perception of the current state by the players. To model this error in perception distributed over other multiple states, we use Euclidean distances between inputs from the sensors.

Categories and Subject Descriptors

K.6.5 [Security and Protection]: Authentication, Invasive Software, Unauthorized access

Keywords

Game model; Security games; General Sum Games; imperfect-incomplete information; Stochastic game

1. INTRODUCTION

There is a growing attempt in the past decade to apply game theoretic approaches to the field of network security. In a network, when a user's anomalous behavior is observed by the administrator, it may not be possible to immediately decide if the user is an attacker or not. Moreover, even if the user has malicious intentions, such initial observation may not be sufficient to fully understand the motivations of the attacker. In such cases, when there is not enough information to classify a user exhibiting anomalous behavior, game theory offers a framework for interaction. [2] gives a survey of the works to model the interaction between a user and a network administrator and it provides a classification of these works based on the game models used. [1] modeled the interaction between an attacker and the administrator as a stochastic game with 14 states considering 3 types of attacks. Their game assumed perfect information. [3] presented a two state, imperfect information, zero sum, stochastic game with numerical simulation showing the advantage of considering the imperfect information. The main motivation for considering the imperfection in the information was the errors in the player's sensors. The error in the sensor makes the player believe that he may be in the states other than the state he really is. Here we make extensions to this work. Our model has the same structure with one extension. When there are more than two states in the game, this error in sensor could make him mistakenly believe he is in any of the other states than the one he really is in. The error in perceiving the state gets distributed over the other states depending on the sensor reading's error needed to misread the state as the current state. Based on this extension in the game model, a game with five states is designed. The error in the perception of current state gets distributed over the four states other than the real state. Thus, the probability of the player 1 being deluded to be in any of the other states is proportional to the distance between the sensor readings of state defining variables of the other states from that of the current real state.

2. GAME MODEL

The model considers that a player 2 k observes the game's true state using an imperfect sensor/ a set of imperfect sensors. That means, player k can view the present state ξj to be any state in the information set $I^k{}_{\xi j} = \{\xi j_1, \xi j_2 . . . \xi j_p\}$ with ξj being an element of $I^k{}_{\xi j}$. The perceived action set at this state may be expanded, i.e., player may decide to take an action which is allowed at $\xi j_i \neq \xi j$ where ξj_i , belongs to $I^k{}_{\xi j}$. When the true state is ξj, let the player k's extended action set $B^k{}_{\xi j} = \bigcup_{\xi j \in Ik\xi j} A^k{}_{\xi j}$ where $A^k{}_{\xi j}$ denotes the allowed action set of player k at state is ξj .If the player k takes an action $\alpha^k \in B_{\xi j}$, when the true state is ξj but α^k is not in $A^k{}_j$, then in terms of the influence on state transition probabilities, α^k is considered equivalent to player k taking no action at state ξj . However, its influence on player k's payoff α^k may not be equivalent to player k taking no action at state ξj depending upon the cost of the attempted execution of α^k. Formally, the model is represented by a tuple, $(S, E^1, E^2, A^1, A^2, Q, R^1, R^2, \beta)$ whose elements are defined below.

- $S = \{\xi_1, \xi_2 . . . \xi_N \}$ is the set of states.

k=0, 1. . . K for one administrator and users respectively.

- $E^k = \{E^k{}_{\xi 1}, E^k{}_{\xi 2} . . . E^k{}_{\xi N}\}$, k=1,2 where the jth,

$0 < j < N$, set $E_{\xi j}$ with $E^k{}_{\xi j} = \{p^k{}_{ji} \mid 1 \leq i \leq m_j , \sum^{mj}{}_{i=1} p^k{}_{ji} = 1, p^k{}_{ji} > 0. \}$, represents the error probabilities of k^th player's sensor at the true state ξj over the corresponding information set, $I^k{}_{\xi j}$. $I^k = \{I^k{}_{\xi 1}, I^k{}_{\xi 2} ... I^k{}_{\xi N}\}$, k =1,2 where the $I^k{}_j$ represents the information set of player k when the true state is ξj , i.e., $I^k{}_{\xi j} = \{\xi_{j1}, \xi_{j2} , . . . , \xi_{ji} , . . . , \xi_{jmj}\}$ where $mj = |I^k{}_{\xi j}|$, $\xi ji \in S$, with $m_j \leq N$ being an integer indicating the number of states that have a possibility of being considered the current state at state ξj with the condition that $\xi j \in I_{\xi j}$.

- $A^k = \{A^k{}_{\xi 1}, A^k{}_{\xi 2} . . . A^k{}_{\xi N}\}$, k = 1, 2 is the action set of

CODASPY'15, March 2–4, 2015, San Antonio, Texas, USA.
ACM 978-1-4503-3191-3/15/03.
http://dx.doi.org/10.1145/2699026.2699133

player k, where $A^k_{\xi j} = \{\alpha^k_{j1}, \alpha^k_{j1}. . . \alpha^k_{jMk}\}$ is the action

set of player k at state ξj. Let $B^k = \{B^k_{\xi 1}, B^k_{\xi 2}. . . B^k_{\xi n}\}$, k=1,2, where $B^k_{\xi j}$ represents the action set of player k at $I^k_{\xi j}$.

That means $B^k_{\xi j} = \bigcup_{\xi j \in Ik\xi j} A^k_{\xi j}$. By introducing different action sets at each state we may get distinct $B^k_{\xi j}$ at for each distinct $I^k_{\xi j}$. Let $T^k_{\xi j} = | B^k_{\xi j}|$.

- The state transition probabilities are represented by function Q: S × B1 × B2 × S → [0 1] which maps a pair of states and a pair of actions to a real number between 0 and 1. The model assumes that for any state ξ^k_j if the player k takes an action $\alpha^k_j \in B^k_{\xi j}$, that does not belong to $A^k_{\xi j}$, then $Q(\xi_{j1}, \alpha^k_{i1}, \alpha^l_{i2}, \xi_{j2}) = Q(\xi_{j1}$,Normal operation, $\alpha^l_{i2}, \xi_{j2})$ where l represents the other player.

- The reward of the player k is determined by the function $R^k : S \times B1 \times B2 \to R$ which maps a state and a pair of actions to a real number.

- β, $0 < \beta < 1$ is the discount factor for discounting the future rewards in this infinite horizon game.

3. ERROR DISTRIBUTION

As E^k represents the set of error probabilities of the player *k*, let us consider the set of error probabilities $E^k_{\xi j}$ with the current state being ξ_j. Let the error of the sensor for player *k* at the state ξ_j is $\gamma^k_{j,}$ $0 \le \gamma^k_{j,} < 1$. The error γ^k_j is always less than 1 because the real state ξ_j is always taken as an element of the information set $I_{\xi j}$ at ξ_j. Then at the current state ξ_j, let the probabilities with which administrator perceives the current state to be ξ_1, ξ_2, ξ_3 and ξ_4 be p^k_{j1}, p^k_{j2}, p^k_{j3}, and p^k_{j4} respectively. Then the error at state ξ_j is $\gamma^k_j = (\sum_{i=1}^{N} p^k_{ji})- p^k_{ji} = 1- p^k_{ji.}$. For $1\le i , j \le N$, let ω^k_{ji} be the set of sensor inputs to the player *k* indicating the current state to be ξ_j, while the real current state is ξ_j. In practice the sensor can be a device or a collection of devices which collects values of some parameters of the system. All such parameters can be considered to form an orthogonal basis of the vector space, where some closed volume is taken to be associated with each state. All of those points in that closed region get mapped to one state. All of them have the values of the parameters which lead the player to perceive the current state to be the particular state. Let the current real state be ξ_j, where $1\le j\le N$. At this state the sensor inputs at two different instances be, say ω^k_{ji} and ω^k_{jh}, where $1\le i ,h\le N$ due to erroneous sensors. This leads to the perception of the current state to be ξ_j and ξ_h respectively. Depending on the nature of the system, consider some representative statistical measure of central tendencies of ω^k_{ji} and ω^k_{jh} . Let Ed^k_{jih} to be the Euclidean distance between those measures. In this work, *larger errors are assumed to be less probable than the smaller errors* in sensor operations, that is, $Ed^k j_{j\,I} > Edkj$ implies $p^k_{ji,} > p^k_{jh}$. In the following game with 5-states, the sensor error is distributed over the three states other than the real current state. This means for example, if the sensor error at ξ_1 is 0.3, then the probability with which the administrator perceives the current state to be not ξ_1 is 0.3. This could result in perceiving the current state to be $\xi_{1,}$ ξ_2 and ξ_3 states respectively with probabilities of 0.15, 0.1 and 0.05. From the sensor relation, we have the sensor error at state $\xi_j \mid i \ne j$, $\gamma^k_j = \sum_{i=1}^{N} p^k_{ji}$ related to the probabilities of virtual states. The sensor outputs values of parameters which define states. Particular range of values of particular set of parameters will correspond to a state. In fact the general way to define it, is a set of values, covering the range, for each of the parameters to correspond to a state. And if there are some parameters whose values do not affect in deciding a particular state then then range can accommodate any value.

- values corresponding to a set of parameters
- a vector space with these parameters constituting the basis

Thus we can see the state definition as follows.

- $S \to S - O$, where

– $S - O = \{S -O_0,S -O_1,S-O_2, . . . S-O_N\}$,

– $S – O = \{s\text{-}o_{i0}, s\text{-}o_{i1} , s\text{-}o_{i2} , , . . . , s\text{-}o_{iFi}\}$

– $s\text{-}o_{i\,j} = (s\text{-}o_{i\,j}(0), s\text{-}o_{i\,j}(1), s\text{-}o_{i\,j}(2), . . . , s\text{-}o_{i\,j}(g))$ implies j^{th} *g*-dimensional sequence corresponding to i^{th} state, ξ_j .

– $s\text{-}o_{i\,j}(l)$ =a MCT, representative value of the expected range of values for the l^{th} parameter in the j^{th} behavior belonging to ξ_j. *l belongs to set of natural numbers,* $0\le l\le g$

– g = number of parameters observed by sensors

– $0 \le j \le Fi$, where $Fi + 1$ disjoint ranges correspond to state ξ_j

When there is an anomaly detected, in terms of sensor values, which do not exactly fit into any particular state and there is uncertainty about to which state the current values belong to, imperfect information must be considered.

- **C**urrent observed **V**alues of parameters as anomaly

$CV = (cv0, cv1, cv2, . . . , cvg)$ = current values of *g* parameters

- consider the minimum of Euclidean distances with elements in each state$(\Theta_{0f\,0} , \Theta_{1f\,1} , \Theta_{1f\,2} , . . . , \Theta_{1f\,N})$. where *f i implies* the $f\,i^{\,th}$ element, $0 \le f\,i \le Fi$ has the minimum of distances between *CV* and $s\text{-}o_{i\,f\,i}$ element in the $i^{\,th}$ state.
- $\Theta_{1f\,I}$ = square root of ($(\sum_{j=0}^{j=g} cv_j - (s\text{-}o_{ij}))$ / (g))min
- The error in perception of states is given by

$P_{ji} = (\sum_{j=0}^{j=N} \Theta_{if\,i} - \Theta_{if\,i})/(\sum_{j=0}^{j=N} \Theta_{if\,i})$

- Then the error at state ξ_j is given by

$\gamma^k_j = \sum_{i=1}^{N} p^k_{ji} - p^k_{ji} = 1- p^k_{ji}$

- **larger errors are assumed to be less probable than smaller errors**

An simple illustration to show its application can be as below.
Example:

Low_Privilege State

- 8AM-6PM = {Download·2Mbps, Upload·150kbps }

This behavior is high-privilege, when manager works at his computer.

High_Privilege State

- 8AM-6PM = {Download≤2Mbps, Upload≤150kbps }

This behavior is high-privilege, when manager works at his computer.

Sensor Readings At 3:30PM there is 1.7Mbps download and 150 kbps upload.

- ((0.7+0.3)-0.7)/(0.7+0.3)=0.3 Probability in Low_Privilege State. Mean Download: 1Mbps
- ((0.7+0.3)-0.3)/(0.7+0.3) =0.7 Probability in High_Privilege State. Mean Download: 2Mbps

4. UTILITY OF THE GENERIC GAME MODEL IN SECURITY SYSTEMS

The generic game model is used as the first step in designing the architecture of the security system, which acts as an event driven system. When a set of anomalies is detected in the operation of the system the potential attacks are identified, using a taxonomical approach [5], and then using the methodology outlined in [4] another taxonomical approach is used to select the suitable game model as shown in Figure 1.

The generic game model presented here is useful to design the different game models suitable for different types of attacks. In fact even a similar type of attack in different situations need different game models as outlined in [4]. But it is not practical to manually design different game models. To derive it in an automated way the generic game model should be extendable to accommodate the distinct specifications needed for different types of attack. The Figure 2 shows how the generic game model will be actually useful in the finally coming up with the appropriate response to the attacks.

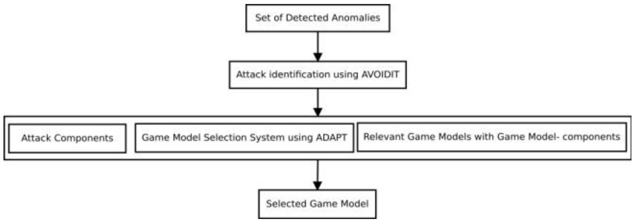
Set of Detected Anomalies
Attack identification using AVOIDIT
Attack Components
Game Model Selection System using ADAPT
Relevant Game Models with Game Model- components
Selected Game Model

Figure 1. Event flow in the Security System.

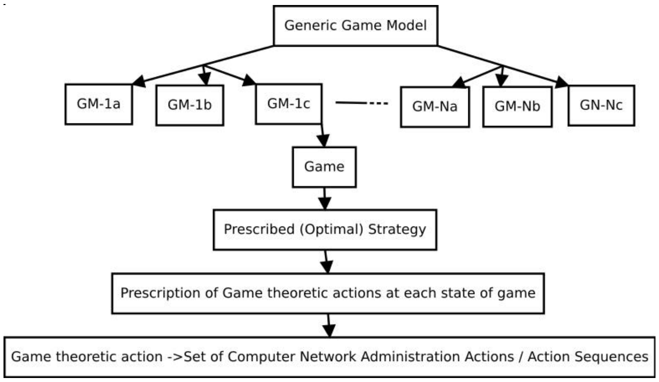
Generic Game Model
GM-1a
GM-1b
GM-1c
GM-Na
GM-Nb
GN-Nc
Game
Prescribed (Optimal) Strategy
Prescription of Game theoretic actions at each state of game
Game theoretic action ->Set of Computer Network Administration Actions / Action Sequences

Figure 2. Generic Game Model’s Utility.

5. CONCLUSION

In this short paper we present the formal game model and how the errors due to imperfect information distributed over many states can be computed. In our ongoing work we are building a generic security game based on this model, and show how to efficiently computing effective equilibria to be able to find out the preferable strategy to ensure optimal outcome.

6. REFERENCES

[1] Lye, K. and Wing, J. 2005. Game Strategies in network security. *International Journal of Information Security, vol. 4, no 1, pp. 71-86.*

[2] Roy, S., Ellis, C. , Shiva, S., Dasgupta, D., Shandilya V. and Wu. Q. . . 2010. A survey of game theory as applied to network security. *The 43rd Hawaii International Conference on system Sciences.*

[3] Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu. Q.. 2010. A stochastic game with imperfect information for cyber security. *The 5th International conference on i-warfare & security (ICIW), Dayton, Ohio.*

[4] Simmons, C., Shiva, S., Bedi, H., and Shandilya. V. 2013. ADAPT: A game inspired attack-defense and performance metric taxonomy. *Security and Privacy protection in Information Processing Systems, pp. 344-364. Springer Berlin Heidelberg.*

[5] Simmons, C., Shiva, S., Phan, V., Shandilya, V. and Simmons, L. 2012. IRS: An issue resolution system for cyber-attack classification and management. SAM, *Los Vegas, July*.