A Game Theory Approach for Intrusion Prevention Systems

Julián Francisco Mojica Sánchez[1], Octavio José Salcedo Parra[1,2](✉), and Lewys Correa Sánchez[2]

[1] Department of Systems and Industrial Engineering, Faculty of Engineering,
Universidad Nacional de Colombia, Bogotá D.C., Colombia
{jfmojicas,ojsalcedop}@unal.edu.co

[2] Faculty of Engineering, Intelligent Internet Research Group,
Universidad Distrital "Francisco José de Caldas", Bogotá D.C., Colombia
osalcedo@udistrital.edu.co,
lcorreas@correo.udistrital.edu.co

Abstract. This document evaluates works related to game theory applied to IPS (Intrusion Prevention System) in networks and proposes a game theory model that allows optimize expenditure of resources in detection of intrusions in networks.

Keywords: Intrusion prevention system · Game theory · Vulnerabilities

1 Introduction

The internet of things every day is being introduced more into our daily lives due to the access that people have both to internet and new technology, with the increase of everyday devices connected to the internet also increases the amount of sensitive information transmitted wirelessly [1].

The increment of devices connected to Internet and the sharing of a big amount of sensitive information and the intrinsic vulnerabilities of wireless communications, made the infrastructure of the Internet of Things networks a point of interest for criminals. For that reason it is necessary to ensure the privacy, available and integrity of this information through security adaptive mechanisms to different types of attacks [2].

The simplicity required in the Internet devices of the thing makes impossible the implementation of internally security systems in these. Because the creation of devices has been increasing to a greater extent than the development in network security with IOT devices, these devices have become a gateway to networks for attackers. Among the different attacks suffered by Wi-Fi networks connected to IOT devices we have: low password exploitation, reverse engineering hardware, remote code execution, man in the middle and hidden monitoring functions. The most common use of remotely controlling IOT devices by cybercriminals is DoS, due it is easy to achieve if the devices have not been configured with basic security measures and allows them to obtain money by preventing access to a server or website [3].

J. C. Figueroa-García et al. (Eds.): WEA 2018, CCIS 915, pp. 218–229, 2018.
https://doi.org/10.1007/978-3-030-00350-0_19

The sensitivity of information and the failures in the security of wireless networks have led the research community to undertake research and development efforts simultaneously in new IOT devices and security mechanisms for wireless networks. An important point is the need for real-time processing and reaction to attacks because IOT devices transmit information constantly [4].

In this document, a model based on game theory will be created to establish the intrusion detection criteria of an IPS (Intrusion Prevention System) for networks, based on the review of previously developed related works.

2 Related Works

In 2016 Wang, Du, Yang, Zhu, Shen and Zhang propose an attack-defense game model for detecting malicious nodes in Embedded Sensor Networks (ESN) using a repeated game approach, where they define the function of rewards that attackers and defenders will receive for their actions [5]. To solve errors and absences in detection use a game tree model. They show that the game model does not have a pure Nash equilibrium but mixed strategy, where the nodes are changing due to the strategies of attackers and defenders so that they are in dynamic equilibrium, where limited resources are used and provided Security protection at the same. Finally, they perform simulations where they show that with the proposed model they can reduce energy consumption by 50% compared to the existing model All Monitor (AM) and improve the detection rate from 10% to 15% compared to the existing model Cluster Head (CH).

In 2013 Manshaei, Zhu, Alpcan, Bacar and Hubaux carry out a review of the investigations in privacy and security in communication and computer networks that have a game theory approach [6]. In their content they have a section of Intrusion Detection Systems where they present the different works found in the review of the literature; the way in which the IDS are configured; Networked IDS, where different IDSs operate in the network independently and the security of each subsystem that they individually protect depends on the performance of the other IDS; Collaborative Intrusion Detection System Networks, in this case in the network operate different IDS in collaborative way, that is, they share the knowledge of the new attacks they detect, but the system can be compromised if the control of an IDS is taken by an attacker and finally the response to intrusions, where they expose an intrusion response system based on Stackelberg stochastic game called Response and Recovery Engine (RRE).

3 Game Theory Models

The prevention of intrusions can be understood as an attack scenario - defense, in which the person in charge of the security of the network decides whether it is necessary or not to put in operation the system of prevention of intrusions, because this operation has a cost that would not be necessary if the network is not being attacked.

The defender has two strategies *(U_D)*: defend or not defend and in the case of the attacker *(U_A):* attack or not attack. The realization of these strategies has rewards and costs that will determine the way the two actors act. These costs and rewards are defined below:

- Cost of starting the IPS *Cm*
- Average loss when the system is attacked *Ci*
- Cost to attack by the attacker *Ca*
- Cost of not attacking by the attacker *Cw*
- Payment to the defender for taking an action strategy defensive *Ui*
- Payment to the attacker for taking an action strategy offensive *Ua*

Now you can understand that the reward of the attackers Pa is equal to average losses when the system is attacked, that is:

$$P_a = C_i \tag{1}$$

It is necessary to define when it is profitable for the attacker to carry out the attack:

$$C_w < P_a - C_a \tag{2}$$

The above equation means that the attacker will perform an attack when its reward minus the cost of attacking greater than the cost of not attacking.

On the other hand, the attacker will not make an attack when the cost of starting the IPS is much lower than the loss average when the system is attacked, because in this case surely the defender would have started the IPS, therefore this will be in operation and the attack will be detected and the attacker isolated from the network.

From this it is possible to define the reward matrix as:

$$\begin{bmatrix} P_a - C_a,\ U_i - C_i & -U_a,\ U_i - C_m \\ C_w,\ U_i & C_w,\ U_i - C_m \end{bmatrix}$$

Where the columns correspond to the strategies of the defender, that is, not defend and defend; and the rows do reference to the attacker's strategies, that is, attack and not attack.

They determine that there is no pure Nash equilibrium, therefore they analyze if the game model is in mixed Nash equilibrium.

Analyzing the mixed Nash equilibrium for the game they found the probability that the attacker attacks σ and the probability that the defender defends δ.

From Eq. (10) it is possible to find δ

$$\delta = \frac{P_a - C_a - C_w}{P_a - C_a + U_a} \tag{3}$$

From Eq. (11) it is possible to find σ

$$\sigma = \frac{C_m}{C_i} \tag{4}$$

With these rewards depending on the probability of taking the strategy of attacking and defending, they found the rewards of not attacking and defending as (1 − σ) and (1 − δ) respectively. Therefore, the strategies of the attackers under a mixed Nash equilibrium are:

$$(\delta, 1-\delta) = \left(\frac{P_a - C_a - C_w}{P_a - C_a + U_a}, \frac{U_a + C_w}{P_a - C_a + U_a}\right) \tag{5}$$

$$(\sigma, 1-\sigma) = \left(\frac{C_m}{C_i}, \frac{C_i - C_m}{C_i}\right) \tag{6}$$

To analyze the Nash equilibrium by mixed strategy, it is possible to start assuming that the probability of attacking *sigma* is high, so that $C_m \gg C_i$, that is, the attack occurs when it is not profitable to start the IPS, which makes the defense probability low.

In case the probability of defense is high, it means that the IPS has probably been launched because the losses to be attacked are greater than the cost of having the IPS in operation, that is, $C_m \gg C_i$ which indicates that the attack probability must be low.

In conclusion, the probabilities of attack and defense are inversely proportional and the system will be in mixed Nash equilibrium when:

$$\sigma = \delta \tag{7}$$

Now Manshaei [6] explains a two-player Bayesian game, a defense node and a malicious or regular one. The malicious node can choose between attacking and not attacking, while the defense node can choose between monitoring and not monitoring. The security of the defender is quantifiable according to the property that protects w, therefore, when there is a security failure the damage is represented by −w. Then the payoff matrix is presented:

$$\begin{bmatrix} (1-\alpha)w - C_a, (2\alpha - 1)w - C_m & w - C_a, -w \\ 0, \beta w - C_m & 0, 0 \end{bmatrix}$$

In this matrix the columns represent the behaviors of the defender (monitor and not monitor) and the rows attacker behaviors (attack and not attack), C_a and C_m are costs of attacking and monitoring, α and β are the detection rate and the false alarm rate of the IDS respectively and μ_0 the probability that a player is malicious.

Finally they show that when $\mu_0 < \frac{(1+\beta)w + Cm}{(2\alpha + \beta - 1)w}$ the game supports a strategy of pure balance (attack if it is malicious, do not attack if it is regular), do not monitor, μ_0 and when $\mu_0 > \frac{(1+\beta)w + Cm}{(2\alpha + \beta - 1)w}$ the game does not have a pure strategy.

4 Proposed Model

From the model described by Manshaei and establishing that the two players are intruder and defender, since the intruder is ready to carry out the attack because has done a vulnerability study and has planned the different strategies to follow in order to enter authorized to the network, the time when no attack represents a C_w cost (waiting cost) because the network can change and the investment mentioned above both of time and of resources can be lost. Therefore, the payment matrix is:

$$\begin{bmatrix} (1-\alpha)w - C_a, (2\alpha - 1)w - C_m & w - C_a, -w \\ -C_w, -\beta w - C_m & -C_w, 0 \end{bmatrix}$$

The following explains each of the possible scenarios and the respective payments for the intruder and the defender:

- When the intruder attacks and the defender monitors: Reward of the attacker, the times the system fails of detection for the good that protects less the cost to attack; the defender's reward, the times the system works less the times it fails for the good that protects, all this except the cost of monitoring.
- When the intruder attacks and the defender does not monitor: the reward of the attacker, the good that one wants to obtain minus the cost of attacking; the defender's reward, in this case is the loss of good.
- When the intruder does not attack and the defender monitors: reward of the attacker, in this case it is the loss for waiting to perform the attack; the reward of defender, false alarm rate degrades the good and its It also has the cost of monitoring.
- When the intruder does not attack and the defender does not monitor: reward of the attacker, in this case it is the loss wait to perform the attack; the reward of the defender, in this case it is null since it does not spend on monitoring and it is not attacked.

Depending on the strategy that the other actor takes and the respective payments they obtain, it is possible to determine if there is a Nash equilibrium.

When the defender does not monitor, the attacker has two possible strategies: Attack, with gain $w - C_a$; and do not attack, where he gets $-C_w$, therefore you will always choose to attack.

When the defender also monitors the attacker can choose between attacking and not attacking, assuming a detection rate greater than 90%, attacking would lose the cost of attacking, while not attacking would lose the cost of waiting.

Generally the deployment of an attack to take control of the network or the information it contains is more expensive than carrying out a recognition and learning of the network and its vulnerabilities, therefore the attacker will choose not to attack.

$$-C_w > -C_a$$

Now it is necessary to fix the behavior of the attacker and analyze the possible strategies that the defender will perform.

First, when the attacker decides to attack and assuming a detection rate greater than 90%.

$$(2\alpha - 1)w - C_m > -w$$

This means that the defender will choose to monitor.

Second, when the attacker decides not to attack

$$-\beta w - C_m < 0$$

Then, the defender will always choose not to monitor.

After analyzing the different strategies, it is clear that in neither scenario will both actors be satisfied with their reward. Which prevents that pure Nash equilibrium exists in the proposed game.

5 Model Evaluation

Because there is no point in the rewards matrix in which both the defender and the attacker feel comfortable with the situation, it is necessary to determine if the model is in mixed Nash equilibrium, for this the probability that the attacker attack σ and the probability that the defender defends δ.

The mixed strategy of the attacker is:

$$U_A = [(1-\alpha)w - C_a]\delta\sigma + [w - C_a](1-\delta)\sigma + (-C_w)\delta(1-\sigma) + (-C_w)(1-\delta)(1-\sigma) \tag{8}$$

The mixed strategy of the defender is

$$U_I = [(2\alpha - 1)w - C_m]\delta\sigma + (-w)(1-\delta)\sigma + [-\beta_w - C_m]\delta(1-\sigma) \tag{9}$$

Using the extreme value method to solve the strategy of the Nash mixed model, the equations are derived (17) and (18) regarding δ and σ respectively and are equal to zero.

$$\frac{\partial U_A}{\partial \sigma} = -\delta\alpha w + w - C_a + C_w = 0 \tag{10}$$

$$\frac{\partial U_I}{\partial \sigma} = 2\sigma\alpha w - \beta w - C_m + \sigma\beta_w = 0 \tag{11}$$

From the Eq. (19) its possible find δ:

$$\delta = \frac{w - C_a + C_w}{w\alpha} \tag{12}$$

From the Eq. (20) its possible find σ:

$$\sigma = \frac{\beta w + C_m}{2\alpha w + \beta_w} \tag{13}$$

To analyze the Nash equilibrium by mixed strategy, you can start assuming that the probability of attacking δ be high, for this to be $Cm \gg 2\alpha w$, this means that the attacker could attack comfortably when the goods that protects the defender are not so valuable to him, which is why I will not have activated the IPS. In the case where you come from protect are valuable the defense probability will increase and the probability of attack will decrease.

Therefore, it is found again that the probabilities of attack and defense are inversely proportional and the system will be in mixed Nash equilibrium when:

$$\delta = \sigma \tag{14}$$

Additionally, in case the probability of defense be high, this situation occurs when the cost of waiting for attacker is greater than the cost of attacking, that is, when it is more profitable for the attacker to effect his attack than to follow waiting for the right moment.

Below is presented a graphical function analysis that defines the probability that the attacker attacks vs the cost of monitoring under certain parameters.

Initially, the good that seeks to protect (w) was set up as 100 and the cost of monitoring varied from 0 to 100 per 1, this was established because it is illogical to use more resources protecting a good than the value for the defender. The alpha value was also set at 95% and different beta values were used to analyze the behavior of the probability that the attacker attacks based on the false alarm rate, this behavior is presented in Fig. 1.

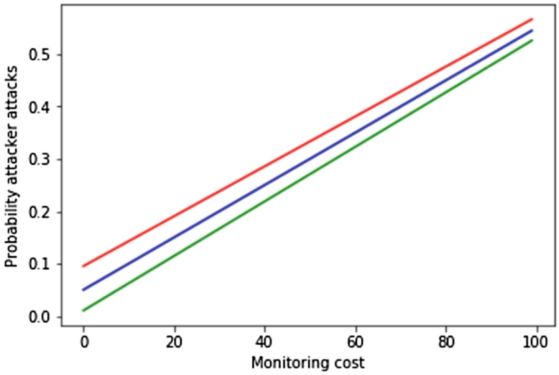

Fig. 1. Probability attacker attacks vs monitoring cost with: w = 100, alpha = 95%, beta = 20% (red), beta = 10% (blue) and beta = 2% (green) (Color figure online)

When analyzing Fig. 1 it can be observed that by decreasing the false alarm rate (beta) the probability of the attacker attacking is diminished, which is because if the IPS is more efficient the attacker will tend not to carry out an attack until you are sure that it will not be detected.

Second, w = 100 and beta = 2% were set to observe the behavior of the probability of the attacker attacking with different values of detection rate, this can be seen in Fig. 2.

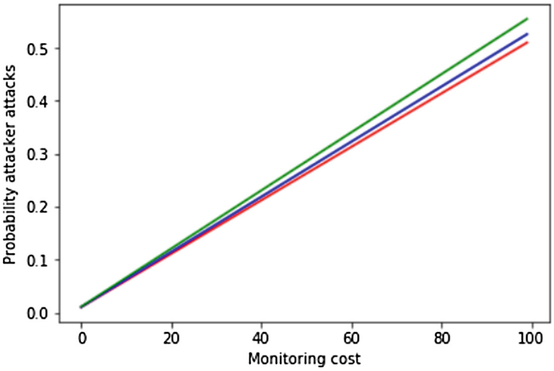

Fig. 2. Probability attacker attacks vs monitoring cost with: w = 100, beta = 2%, alpha = 98% (red), alpha = 95% (blue) and alpha = 90% (green) (Color figure online)

Figure 2 shows that by decreasing the detection rate the probability that the attacker will attack will be greater, this happens in the same way as in the previous case, because if the system becomes less efficient it will be more profitable for the attacker to make an attack, therefore, the probability that the attacker will attack will increase.

Third, alpha = 98%, beta = 2% was set and the value of w was varied to analyze how the probability that the attacker attacks with respect to the variation of the cost of the desired good is affected. opt to make the attack. Said analysis was carried out starting from Fig. 3.

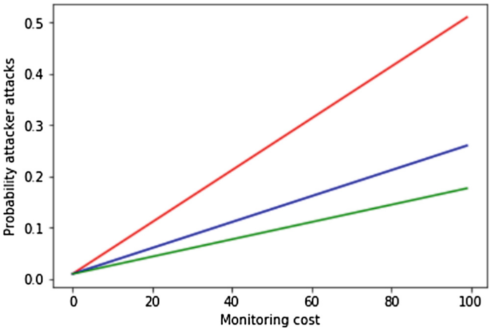

Fig. 3. Probability attacker attacks vs monitoring cost with: alpha = 98%, beta = 2%, w = 100 (red), w = 200 (blue) and w = 300 (green) (Color figure online)

Figure 3 shows that increasing the cost of the good that the attacker wants to obtain, the likelihood that the attacker attacks is reduced, this seems to go against the logic but it is because if the good is much more valuable than the cost of monitoring, the defender will always want to protect said good by starting the IPS and therefore it will be more complex for the attacker to violate the security of the system.

Below is a graphical function analysis that defines the probability that the defender defends vs the cost of attack under certain parameters.

In a similar way to the previous case we started by initially establishing the good that we want to protect w as 100 and varying the cost of attack from 0 to 100 every 1, this was defined in that way because it was assumed that the attacker has an idea of how Valuable is the good that you expect to obtain when making an attack and is not willing to spend more than the value of said good.

The value of alpha was also set at 95% and different values of C_w were used to analyze the behavior of the probability that the defender defends with respect to the cost of waiting to carry out the attack, this behavior is presented in Fig. 4.

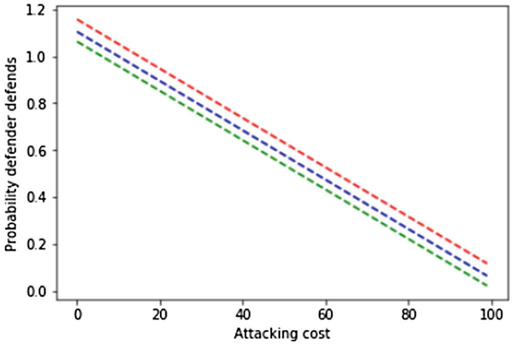

Fig. 4. Probability defender defends vs attacking cost with: w = 100, alpha = 95%, Cw = 10 (red), Cw = 5 (blue) and Cw = 1 (green) (Color figure online)

Figure 4 shows that by decreasing the value of the waiting cost to carry out the attack, the probability that the defender defends will also decrease. This is because the attacker is so clear about the vulnerabilities of the network that it is very cheap for him to wait for the attack, therefore the defender must activate the IPS as soon as possible to correct the failures in network security.

Second, $w = 100$ and $C_w = 10$ were set to observe the behavior of the probability that the defender defends with different values of detection rate, this can be seen in Fig. 5.

When looking at Fig. 5 it is understood that when the detection rate of the IPS decreases the probability that the defender defends increases, this behavior is due to the fact that when the IPS is less efficient the defender must have it active for a longer time in order to detect the intrusions and therefore the probability that the defender defends will be greater.

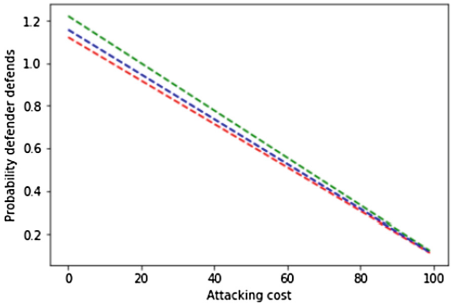

Fig. 5. Probability defender defends vs attacking cost with: w = 100, Cw = 10, alpha = 98% (red), alpha = 95% (blue) and alpha = 90% (green) (Color figure online)

Finally $alpha = 98\%$ and $C_w = 10$ were set to see how the cost of the good that protects the defender impacts the probability that the defender defends, this was done by variations in w and can be seen in Fig. 6.

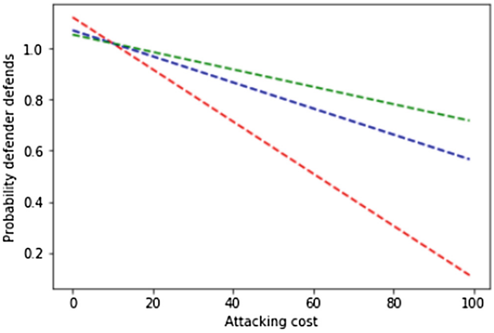

Fig. 6. Probability defender defends vs attacking cost with: alpha = 98%, Cw = 10, w = 100 (red), w = 200 (blue) and w = 300 (green) (Color figure online)

6 Discussion

The presented model is based on the model described by Manshaei [6] but this does not have a pure Nash equilibrium because in this new model it is defined that there are two players: a defender and an attacker, while in the presented by Manshaei it is possible that the attacker is not malicious in which there is a pure balance and is not to attack and not monitor.

Regarding the model presented by Wang [5] the same conclusion was reached that the system will be in equilibrium when the probability of attacking:

$$\sigma = \frac{\beta w + C_m}{2\alpha w + \beta w} \tag{15}$$

Equal to the probability of defending:

$$\delta = \frac{w - C_a + C_w}{w\alpha} \tag{16}$$

And in case these are not equal the model is regulated to over time until you reach this balance even though you in this case the detection rate and false are taken into account IPS alarms, which is raised in the model described by Manshaei [6] and makes the model closer to reality.

The analysis of the probability functions that the attacker attacks and that the defender defends allows to obtain a clearer view of the decisions that the players of this game can take and the reasons to act in a certain way.

7 Conclusions

- This model of game theory adds a new feature to intrusion prevention systems, where you can evaluate how complex it is to perform a vulnerability analysis on the network that is defending itself. Because if it is much less expensive to perform the analysis than the attack, it will be more profitable for the attackers to launch their attack plan and therefore the IPS must be in operation to prevent such attacks and avoid loss of information, money and reputation.
- The proposed model is regulated over time until reaching the equilibrium point at which the probability of attacking σ is equal to the probability of defending δ.

$$\sigma = \frac{\beta w + C_m}{2\alpha w + \beta w} = \frac{w - C_a + C_w}{w\alpha} = \delta$$

- Decreasing the false alarm rate (beta) the probability of the attacker attacking is diminished.
- Decreasing the detection rate the probability that the attacker will attack will be greater.
- Increasing the cost of the good that the attacker wants to obtain, the likelihood that the attacker attacks is reduced.
- Decreasing the value of the waiting cost to carry out the attack, the probability that the defender defends will also decrease.
- When the detection rate of the IPS decreases the probability that the defender defends increases.
- When the cost of the good that the defender protects increases, the probability that the defender defends also increases.

References

1. Michaels, S., Akkaya, K., Selcuk Uluagac, A.: Inducing data loss in Zigbee networks via join/association handshake spoofing. In: 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, pp. 401–405 (2016). https://doi.org/10.1109/cns.2016.7860527
2. Sforzin, A., Marmol, F.G., Conti, M., Bohli, J.M.: RPiDS: raspberry Pi IDS - a fruitful intrusion detection system for IoT. In: Proceedings - 13th IEEE International Conference on Ubiquitous Intelligence and Computing, 13th IEEE International Conference on Advanced and Trusted Computing, 16th IEEE International Conference on Scalable Computing and Communications, pp. 440–448 (2017). https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoPSmartWorld.2016.0080
3. Sharma, P.K., Moon, S.Y., Moon, D., Park, J.H.: DFA-AD: a distributed framework architecture for the detection of advanced persistent threats. Clust. Comput. **20**(1), 597–609 (2017). https://doi.org/10.1007/s10586-016-0716-0
4. Chen, J., Chen, C.: Design of complex event-processing IDS in internet of things. In: Proceedings - 2014 6th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2014, pp. 226–229 (2014). https://doi.org/10.1109/ICMTMA.2014.57
5. Wang, K., Du, M., Yang, D., Zhu, C., Shen, J., Zhang, Y.: Game-theory-based active defense for intrusion detection in cyber-physical embedded systems. ACM Trans. Embed. Comput. Syst. **16**(1), 121 (2016). https://doi.org/10.1145/2886100
6. Manshaei, M.M.H., Zhu, Q., Alpcan, T., Bacar, T., Hubaux, J.-P.: Game theory meets network security and privacy. ACM Comput. **45** (2013). https://doi.org/10.1145/2480741.2480742