




Intrusion Prevention Model for WiFi Networks

Julián Francisco Mojica Sánchez¹, Octavio José Salcedo Parra^{1,2} ,
and Alberto Acosta López²

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, aacosta}@udistrital.edu.co

Abstract. WIFI technology has consolidated in the market with a wide range of devices connected at different distances, frequencies and with different characteristics. Despite progress in the creation of new devices and improvements in technology, although security has some protective measures is lagging behind and more vulnerabilities are being discovered every day of the networks with these devices. Therefore, it is essential the research and development of security measures and tools to ensure information security, this document proposes a game theory model that could be the basis of an algorithm for the prevention of intrusions in WIFI networks.

Keywords: Intrusion prevention system · Game theory · Vulnerabilities · WIFI

1 Introduction

WIFI technology has been imposed in recent years over other types of connection in local networks due to its versatility and low cost compared to wired networks, this has allowed the creation of different network configurations from small home and office networks up to business networks, with a considerable amount of devices sharing information at all time. This versatility has been achieved leaving behind security, therefore it is necessary to work on tools and protocols that increase the security of WIFI networks [1].

Currently, the security protocols designed by IEEE for WIFI networks are the 802.11 family, where the most used form of encryption due to its efficiency is WPA2. In spite of the efforts made by IEEE, the advance in new devices has been much greater than the advance in the creation, implementation and updating of security protocols so that each time new attacks are created taking advantage of this gap. Intrusion prevention systems are used in large companies and it is not feasible to implement them in public networks with a large number of connected devices sharing information at all times and in different locations. As for office and home networks, router security mechanisms are obsolete against various types of attacks [2].

This document proposes a game theory model that could be the basis of an algorithm for the prevention of intrusions in WIFI networks, based on two intrusion detection models.

2 Related Works

In 2013 Manshaei, Zhu, Alpcan, Bacar and Hubaux conduct a review of research on privacy and security in communication and computer networks that have as their focus game theory. They present a review of the different works found in the literature, the way in which IDS are configured, Networked IDS, where in the network operate different IDS independently and the security of each subsystem they protect individually depends on the performance of the other IDS, Collaborative Intrusion Detection System Networks, in this case in the network operate different IDS collaborative way, i.e. share the knowledge of new attacks that detect, but the system may be compromised if the control of an IDS is taken by an attacker and finally the response to intrusions, where they expose a system of response to intrusions based on Stackelberg stochastic game called Response and Recovery Engine (RRE) [3].

In 2016 Sharma, Moon, Moon and Park designed a DFA-AD (distributed framework architecture for the detection of advanced persistent threats), in which one of the 4 traffic classification modules was Dynamic bayesian game model Based, in this case the game model is dynamic since each player selects his behavior depending on the current state of the system and the information he possesses. The attackers identify users and special targets of the system in an exhaustive way, therefore, the attackers have more data about the module than the protectors, which creates a system in incompleteness and asymmetry [4].

In 2016 Wang, Du, Yang, Zhu, Shen and Zhang propose an attack-defense game model to detect malicious nodes in Embedded Sensor Networks (ESNs) using a repeat game approach, define the reward function that attackers and defenders will receive for their actions. To fix detection errors and detection absences they use a game tree model. They demonstrate that the game model does not have a Nash balance of pure strategy but mixed, where the nodes are changing due to the strategies of attackers and defenders so that they are in dynamic balance, in this balance is made use of limited resources and security protection is provided at the same time. Finally they perform simulations of the proposed model from which they conclude that they can reduce energy consumption by 50% compared to the existing All Monitor (AM) model and improve the detection percentage from 10% to 15% compared to the existing Cluster Head (CH) model [5].

3 Game Theory Models

Intrusion prevention can be understood as an attack-defense scenario, in which the network security manager decides whether or not it is necessary to implement the intrusion prevention system, because such operation has a cost that would not be necessary if the network is not being attacked. The game consists of a defender (the one in charge of starting or not the IPS) and an attacker (which seek to enter the network and take

advantage of the intrusion), this was taken from the model proposed by Wang in 2016 but limited to a single attacker and defender, as it took multiple attackers and defenders in multiple nodes and time periods [5].

As for the defender, he has two strategies (*UD*): defend or not defend and in the case of the attacker (*UA*): attack or not attack. Carrying out 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 C_m
- Average loss when the system is attacked C_i
- Cost to attack by the attacker C_a
- Cost of not attacking by the attacker C_w
- Payment to the defender for taking an action strategy defensive U_i
- Payment to the attacker for taking an action strategy offensive U_a

Now it can be understood that the reward of the attackers P_a is equal to the average losses when the system is attacked, that is:

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

Now it is necessary to define when it is profitable for the attacker to perform 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. It is now necessary to analyze Nash’s balance by analyzing each actor’s payoffs depending on the strategy taken by the other actor. When the defender does not defend the attacker has two possible strategies, but by Eq. (1) we know that:

$$C_w < P_a - C_a \tag{3}$$

Therefore, the attacker will always choose to attack.

Secondly when the defender defends the same mind the attacker can choose between attacking and not attacking, but how:

$$U_i - C_a < U_i - C_m \quad (4)$$

The defender will always choose to defend.
 Second, when the attacker decides not to attack

$$U_i > U_i - C_m \quad (5)$$

Therefore, the defender will always choose not to defend.

From analyzing the previous strategies that the actors will take depending on the behavior of the other it can be said that there is no pure Nash balance, since there is no place in the matrix in which both actors are satisfied with their reward. Because there is no pure Nash balance it is necessary to analyze if the game model is in mixed Nash balance, for this you define the probability that the attacker attacks σ and the probability that the defender defends δ .

The attacker's mixed strategy is

$$U_A = (P_a - C_a)(1 - \delta)\sigma + (-U_a)\delta\sigma + C_\omega(1 - \sigma) \quad (6)$$

The defender's mixed strategy is

$$U_I = (U_i - C_i)(1 - \delta)\sigma + (U_i - C_m)\delta + U_i(1 - \delta)(1 - \sigma) \quad (7)$$

$$U_I = U_i - C_i\delta\sigma - C_i\sigma - C_m\delta \quad (8)$$

Now using the extreme value method to solve the strategy of the Nash mixed model, Eqs. (6) and (8) are derived with respect to σ and δ respectively.

$$\frac{\partial U_A}{\partial \sigma} = (P_a - C_a)(1 - \delta) + (-U_a)\delta - C_\omega = 0 \quad (9)$$

$$\frac{\partial U_I}{\partial \delta} = C_i\sigma - C_m = 0 \quad (10)$$

From Eq. (9) it is possible to find σ

$$\delta = \frac{P_a - C_a - C_\omega}{P_a - C_a + U_a} \quad (11)$$

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

$$\sigma = \frac{C_m}{C_i} \quad (12)$$

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 Nash's mixed equilibrium when $\sigma = \delta$.

Manshaei [3] discusses a two-player Bayesian game, a defense node and a malicious or regular one. The malicious node can choose between attacking and non-attacking, while the defense node can choose between monitoring and nonmonitoring. The security of the defender is quantifiable according to the goods it protects w , therefore, when there is a security breach the damage is represented by $-w$. The rewards matrix is presented below:

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

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 $\mu_0 < \frac{(1 + \beta)w + C_m}{(2\alpha + \beta - 1)w}$ 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 $\mu_0 > \frac{(1 + \beta)w + C_m}{(2\alpha + \beta - 1)w}$ 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:

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

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:

$$U_A = [(1 - \alpha)\omega - c_a]\delta\sigma + [\omega - c_a](1 - \delta)\sigma + (-c_w)\delta(1 - \sigma) + (-c_w)(1 - \delta)(1 - \sigma) \quad (13)$$

The mixed strategy of the defender is

$$U_I = [(2\alpha - 1)\omega - c_m]\delta\sigma + [-\omega](1 - \delta)\sigma + [\beta\omega - c_m]\delta(1 - \sigma) \quad (14)$$

Using the extreme value method to solve the strategy of the Nash mixed model, the equations are derived (16) and (17) regarding δ and σ respectively and are equal to zero.

$$\frac{\partial U_A}{\partial \sigma} = -\delta\alpha w + w - C_a + C_w = 0 \quad (15)$$

$$\frac{\partial U_I}{\partial \sigma} = 2\sigma\alpha w - \beta w - C_m + \sigma\beta_w = 0 \quad (16)$$

From the Eq. (18) its possible find δ :

$$\delta = \frac{w - C_a + C_w}{w\alpha} \quad (17)$$

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

$$\sigma = \frac{\beta w + C_m}{2\alpha w + \beta_w} \quad (18)$$

To analyze the Nash equilibrium by mixed strategy, you can start assuming that the probability of attacking δ be high, for this to be $C_m \gg 2\alpha w$, 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:

$$\delta = \sigma \quad (19)$$

It is known that

$$0 \leq P(a) \leq 1 \quad (20)$$

Then

$$\delta = \frac{\omega - c_a + c_\omega}{\omega\alpha} \leq 1 \quad (21)$$

$$\sigma = \frac{\beta\omega - c_m}{2\alpha\omega + \beta\omega} \leq 1 \quad (22)$$

From Eq. (23)

$$C_m \leq 2\alpha\omega \quad (23)$$

Equation 25 indicates that when the detection rate or value of the good to be protected decreases in the same way, the detection cost used to protect the good should decrease. From Eq. (24)

$$C_\omega \leq C_a - (1 - \alpha)\omega \quad (24)$$

Equation 26 indicates that the attacker's maximum wait cost is directly linked to the undetected rate of the intrusion prevention system, as that rate increases the maximum wait cost should decrease. From Eq. (21)

$$\omega = \frac{(-C_a(2\alpha + \beta) + C_m\alpha - C_\omega(2\alpha + \beta))}{\alpha(\beta - 2) - \beta} \quad (25)$$

6 Conclusions

The game theory model for intrusion prevention adds the waiting cost of the attacker and it is shown theoretically that it is a decisive factor in the prevention of an attack. This is because if the attacker spends several resources planning the attack, it is possible for the defender to make modifications in the network that prevent the initially planned attack or simply migrate the information desired by the attacker, in which case the attacker will have spent more resources than he is going to get when he succeeds in violating the security of the defender.

Describes the condition to be in Mixed Nash Equilibrium, it means that each player has the same probability in their options of behavior.

$$\omega = \frac{(-C_a(2\alpha + \beta) + C_m\alpha - C_\omega(2\alpha + \beta))}{\alpha(\beta - 2) - \beta} \quad (26)$$

References

1. Koliass, C., Kambourakis, G., Stavrou, A., Gritzalis, S.: Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. *IEEE Commun. Surv. Tutor.* **18**(1), 184–208 (2016). <https://doi.org/10.1109/COMST.2015.2402161>
2. Huang, H., Hu, Y., Ja, Y., Ao, S.: A whole-process WiFi security perception software system. In: 2017 International Conference on Circuits, System and Simulation, ICCSS 2017, pp. 151–156 (2017). <https://doi.org/10.1109/CIRSYSSIM.2017.8023201>
3. Manshaei, 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>
4. Sharma, P.K., Moon, S.Y., Moon, D., Park, J.H.: DFA-AD: a distributed framework architecture for the detection of advanced persistent threats. *Cluster Comput.* **20**(1), 597609 (2017). <https://doi.org/10.1007/s10586-016-0716-0>
5. Wang, K., Du, M., Yang, D., Zhu, C., Shen, J., Zhang, Y.: Gametheory-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>