A Game Theoretic Approach to Model Cyber Attack and Defense Strategies

Afraa Attiah*, Mainak Chatterjee†, Cliff C. Zou†
*†College of Engineering and Computer Science, University of Central Florida, Florida, USA
Email: *afraa.attiah@knights.ucf.edu, †{mainak, czou}@eecs.ucf.edu,

***Abstract*—Most of the cybersecurity research focus on either presenting a specific vulnerability or proposing a specific defense algorithm to defend against a well-defined attack scheme. Although such cybersecurity research is important, few have paid attention to the dynamic interactions between attackers and defenders, where both sides are intelligent and will dynamically change their attack or defense strategies in order to gain the upper hand over their opponents. This 'cyberwar' phenomenon exists among most cybersecurity incidents in the real world, which warrants special research and analysis. In this paper, we propose a dynamic game theoretic framework (i.e., hyper defense) to analyze the interactions between the attacker and the defender as a non-cooperative security game. The key idea is to model attackers/defenders to have multiple levels of attack/defense strategies that are different in terms of effectiveness, strategy costs, and attack gains/damages. Each player adjusts his strategy based on the strategy's cost, potential attack gain/damage, and effectiveness in anticipating of the opponent's strategy. We study the achievable Nash equilibrium for the attacker-defender security game where the players employ an efficient strategy according to the obtained equilibrium. Furthermore, we present case studies of three different types of network attacks and put forth how our hyper defense system can successfully model them. Simulation results show that the proposed game theoretical system achieves a better performance compared to two other fixed-strategy defense systems.**

***Keywords*—Security, game theory, network, attack, defense.**

I. Introduction

With the adoption of newer networking technologies for better connectivity, we are witnessing an era of unprecedented cyber attacks. Ensuring confidentiality, integrity, and availability (CIA) of data, devices, networks, and users have become utmost critical. This becomes even more challenging in resource-constrained environments, such as wireless sensor networks (WSNs), where energy, computing, and communication resources are strictly limited.

Most academic research have typically focused on a static model with a particular attack or defense on security without considering: (i) the dynamic attack intensity or the dynamic environmental conditions of the system, and (ii) the continuous interactions between the attackers and the defenders where each of them is constantly adjusting its attack/defense strategies in order to gain the upper hand. However, these two phenomena exist in almost all cybersecurity problems in the real world. Thus, besides finding a specific defense algorithm, it is equally or even more important to design a dynamic defense system that can adjust its strategies to achieve the best defense performance against intelligent attackers and under various attack situations. The goal of our research is to design a cyberwarfare framework, rooted in game theory, which considers dynamic interactions and evolutions between attackers and defenders.

In this paper, we introduce a novel approach for a defense mechanism against several types of attacks/threats on networks– a hyper defense mechanism that considers the limitation of the resources as well as the security value of the asset of the network. Our model provides suitable responses for a defender by considering different intensities of attacks and the relative cost to launch them. We model the interactions between the attackers and defenders as a cyber-warfare game as it has proven to be a highly efficient mathematical method for analyzing and modeling scenarios with conflicting objectives. Furthermore, in order to control future threats in security systems, game theory is useful in the suggesting various probable actions and in predicting their related outcomes. We present *a non-cooperative zero-sum attacker-defender* game. We formulate the security game between an attacker and defender to study the dynamic interactions between rational players with conflicting interests.

In addition, we attain optimal strategies for the defender and the attacker considering that they can dynamically choose their strategies in order to maximize their own payoff based on cost minimization. Generally speaking, we classify the actions of either attacking or defending into three categories: *level zero, level one, and level two*. The attacker can alternate between these three strategies, where level zero represents no attack, level one represents a low intensity of attack, and level two represents a high intensity of attack. Likewise, we classify the defender's actions into three corresponding defense levels. For level zero, the defender decides to not defend at all. The second one is a low level of defense, which could cost some of the resources (i.e., energy, or memory space, etc.). The third one is a high level of defense, which requires more computational, battery power, or memory, but gains strong countermeasures against the threats. In practice, the strategies of attackers and defenders for any cybersecurity problems could be categorized into more fine-grained levels, but for the sake of clarity and modeling purposes, we believe such a three-level classification of attack or defense is generalized enough and can well represent attack and defense activities in real practice.

Our contributions in this paper are:

- We emphasize the often-neglected research of the dynamic interactions and evolution among cybersecurity attackers and defenders.

Afraa Attiah is also affiliated with the Collage of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia.

- We present a non-cooperative zero-sum game in modeling the cyber warfare between attackers and defenders based on the generalized three-level attack/defense strategies game.
- We present the case study of three different types of network attacks to demonstrate how the proposed game theory can be applied in a broad range of cybersecurity problems.

II. Related Work

Security under a game theoretic framework is an interesting topic, where several probable actions along with the predicted outcome can be suggested through game theoretic methods in order to control future threats. Game theory is suitable for modeling various issues and have been successfully used in cyber security including communication networks [1] [2] [3]. Various issues in security and privacy in networking and mobile application have been addressed and modeled through game theoretic framework [4]. In [5], the author addresses the issue of defending against denial-of-service attacks in the network and proposes a puzzle-based defense solution that can be distributed or non-distributed using the concept of Nash equilibrium. The authors of [6] propose a Bayesian game approach for intrusion detection in wireless ad hoc networks to analyze the interactions between pairs of attacking and defending nodes. The concept of Nash equilibrium is utilized in both static and dynamic scenarios. A player can be either a malicious or regular node. In [7], a secure routing protocol is proposed by modeling the interaction of nodes in WSN and intrusion detection system as a Bayesian game formulation. Unlike most security mechanisms that focus on a particular attack or defense, we provide in this work a dynamic defense system that considers the variation in the intensity of attack and defense.

III. Non-cooperative attack-defense Game

This section discusses how an attacker-defender security game is formulated as a non-cooperative zero-sum game. In addition, we describe attacker and defender strategies and derive their solutions.Being rational players in the game, an attacker competes for the best action and his objective is to maximize his own utility. Therefore, the opponents are not bound to cooperate with each other where the malicious attacker would want to play a suitable strategy to maximize his chances of being successful and waste the resources of the system. In contrast, the defender would also like to play a suitable strategy to maximize his chances of protection against the opponents without overspending energy or computation on defending.

As discussed in the related work, most previous game theory research [1] [2] [4] model attackers and defenders with only two strategies, no attack/defense, or with attack/defense. In order to provide a broader modeling of attackers/defenders where they can adjust their attack/defense strategies with different intensities, in this paper, we model each player with three levels of strategies: no attack/defense, low level of intensity, and high level of intensity.

Attackers and defenders experience different cost to benefit affects in order to achieve their success in either attack or defense. Therefore, in our game, each attacker and defender have different levels of strategies instead of having just two levels, as suggested by most of the previous research. In our model, each of the players adopts zero level of intensity, low level of intensity, or high level of intensity.

A. Game Model

We consider a two-player non-coordination zero-sum security game represented by $\mathcal{G} =< (\mathcal{N}), (\mathcal{S}), (\mathcal{U}) >$, where $\mathcal{N} = \{A, D\}$ represents the two players: Player A is a malicious-node/attacker and the other player D is a defender. $\mathcal{S} = \{a_r, d_r | r \in \{0, 1, 2\}\}$ is the strategy space, which is the set of actions that are available for each player, and their utilities are given by $\mathcal{U}$.

As we mentioned above, the attacker and the defender can use one of the three levels of the available strategies during the game. For the attacker, level zero means that he decides not to attack, denoted by a_0 =*No-Attack*, level one is low intensity of attack, denoted by a_1 =*Attack-1*; and level two is a high intensity of attack, denoted by a_2 =*Attack-2*. Generally speaking, from the attacker's perspective, compared with the strategy *Attack-1*, the strategy *Attack-2* is more effective in generating successful attack, but takes more resources or cost more for the attacker to implement. Correspondingly, level zero for the defender means that he decides not to implement any defense, denoted by d_0 =*No-Defend*; level one is a low intensity of defense, denoted by d_1 =*Defend-1*; and level two is a high intensity of defense, denoted by d_2 =*Defend-2*.

Therefore, the attacker A has three strategies: a_0=*No-Attack*, a_1=*Attack-1*, and a_2=*Attack-2*. The defender D has three strategies as well: d_0=*No-Defend*, d_1=*Defend-1*, and d_2=*Defend-2*. Both players choose their strategies simultaneously without any collaboration, assuming common knowledge about the game (i.e., $\mathcal{U}$)/(gain and lost).

We assume that the value of the protected assets by the defender D is worth of ω_n, where $\omega_n > 0$ and $n \in \{1, 2\}$. ω_1 is the value of assets compromised by *Attack-1* strategy deployed by the attacker successfully; ω_2 is the value of assets compromised by *Attack-2* strategy deployed by the attacker successfully. According to zero-sum game, we assume that the gain of one player is equal to the loss of the opponent. Therefore, ω_n is the gain by the attacker if his strategy Attack-n is successful and $-\omega_n$ denotes the loss/damage by the defender. The value of this loss by defender refers to the degree/amount of damage such as, wasting energy, number of compromised/disabled nodes, loss of data integrity, etc.

Meanwhile, the attacker/defender also needs to make some effort (i.e., pay certain cost) to implement their attack/defense strategies. For the attacker, we denote the cost of attack as c_{an} where $n \in \{1, 2\}$: c_{a1} is the cost to deploy *Attack-1* strategy, and c_{a2} is the cost to deploy *Attack-2* strategy. Likewise, for the defender, we denote the cost of defense as c_{dn} where $n \in \{1, 2\}$: c_{d1} is the cost to deploy *Defend-1* strategy, and c_{d2} is the cost to deploy *Defend-2* strategy.

B. Model Assumptions

We make the following assumptions for our proposed three-level attack/defense strategy model:

- Value of security assets is always greater than the cost to defend or attack against them since otherwise the

TABLE I: Strategic form of Attack-Defense game.

Attacker (A) \ Defender (D)	d_0	d_1	d_2
a_0	0 , 0	c_{d1} , $-c_{d1}$	c_{d2} , $-c_{d2}$
a_1	$\omega_1 - c_{a1}$, $c_{a1} - \omega_1$	$c_{d1} - c_{a1}$, $c_{a1} - c_{d1}$	$c_{d2} - c_{a1}$, $c_{a1} - c_{d2}$
a_2	$\omega_2 - c_{a2}$, $c_{a2} - \omega_2$	$\omega_2 + c_{d1} - c_{a2}$, $c_{a2} - c_{d1} - \omega_2$	$c_{d2} - c_{a2}$, $c_{a2} - c_{d2}$

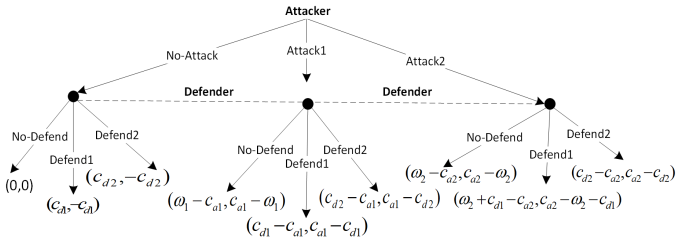


Fig. 1: Extensive form of the Attack-Defense Cyber security game.

defender or the attacker does not have any incentive to defend or attack, respectively; i.e, $\omega_n > c_{an}, c_{dn}, n \in \{1, 2\}$.

- Cost of attack strategy a_1=*Attack-1* is less than the cost of attack strategy a_2 =*Attack-2* for the attacker. Since *Attack-2* is a more aggressive and effective attack strategy than *Attack-1*, *Attack-2* takes more attacking efforts or cost to deploy. (i.e., $c_{a1} < c_{a2}$).
- Cost of defense strategy d_1 =*Defend-1* is less than the cost of strategy d_2 =*Defend-2* for the defender. Again, this is because *Defend-2* is a more aggressive and effective defense strategy than *Defend-1*. (i.e., $c_{d1} < c_{d2}$).
- Generally speaking, a more aggressive/effective attack will cause more damage to a target if the attack succeeds. Thus based on the definition of ω_n in previous subsection, it is safe to assume that ($\omega_2 \geq \omega_1$).

In addition, the game model requires us to define what is the outcome when the attacker deploys one specific attack strategy and the defender implements one specific defense strategy. We make the following assumptions on the game outcomes:

- Attack is successful under these scenarios: *Attack-1* vs. *No-Defend*; *Attack-2* vs. *Defend-1* or *No-Defend*.
- Defense is successful under these scenarios: *Defend-1* vs. *Attack-1* or *No-Attack*; *Defend-2* vs. *Attack-2* or *Attack-1* or *No-Attack*.
- Zero gain or loss when there is no attack and no defense deployed, i.e., *No-Attack* vs. *No-Defend*.

The above assumptions mean that the more aggressive defense strategy, *Defend-2*, is secure against all attacks. However, the low-level defense strategy, *Defend-1*, is good to defend the low-level attack, *Attack-1*, but is still vulnerable to deal with the aggressive attack, *Attack-2*. Table I illustrates the payoff matrix of the game in a strategic form.

C. Nash Equilibria Analysis for Non-cooperation Game

For the proposed security game, there is no Pure Strategy Nash Equilibrium (PSNE) where each player in the game always has the incentive to deviate to another strategy in order to gain higher payoff. We can argue that there is no pair of deterministic strategy that works for both players. Therefore, we derive Mixed Strategy Nash Equilibrium (MSNE) for our model. Figure 1 illustrates the extensive form of the game.

1) MSNE for Security Game with Three-level Strategies:
Definition 1: The Mixed Strategy Nash Equilibrium [8] of the security game is a probability distribution $\hat{P}$ over the set of pure strategies $\mathcal{S}$ for any player such that:

$$\hat{P} = (p_1, p_2, p_3, ..., p_r) \in \mathbb{R}^{\mathcal{R}} \geq 0, \quad \text{and} \quad \sum_{t=1}^{\mathcal{R}} p_t = 1 \quad (1)$$

For the attacker, let p_{a_0} be the probability of playing strategy a_0, p_{a_1} be the probability of playing strategy a_1, and $p_{a_2} = 1 - p_{a_0} - p_{a_1}$ be the probability for playing strategy a_2 for the attacker. In the same manner, for the defender let p_{d_0} be the probability of playing strategy d_0, p_{d_1} be the probability of playing strategy d_1, and $p_{d_2=1-p_{d_1}-p_{d_2}}$ be the probability for playing strategy d_2.

According to the MSNE definition, the opponents become indifferent about the choice of their strategies by making the expected payoffs equal. Therefore, in our proposed game, the mixed strategy makes each player indifferent among all three of their strategies when the expected utilities from playing strategies a_0, a_1, and a_2 are equal for the attacker, and the expected utilities from playing strategies d_0, d_1, and d_2 are equal for the defender, i.e.,

$$EU(p_{a_0}) = EU(p_{a_1}) = EU(p_{a_2}) \quad (2)$$

$$EU(p_{d_0}) = EU(p_{d_1}) = EU(p_{d_2}) \quad (3)$$

Then, from Table I, we find the expected utility of the attacker for playing strategy a_0, a_1, and a_2 as function of the mixed strategy which are given by:

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_1}(-c_{d1}) + p_{d_2}(-c_{d2}) \quad (4)$$

$$EU(p_{a_1}) = (p_{d_0})(\omega_1 - c_{a1}) + p_{d_1}(c_{d1} - c_{a1}) + p_{s_{d2}}(-c_{d2}) \quad (5)$$

$$EU(p_{a_2}) = (p_{d_0})(\omega_2 - c_{a2}) + p_{d_1}(\omega_2 + c_{d2} - c_{a2}) + p_{d_2}(c_{d2} - c_{a2}) \quad (6)$$

Substituting (4), (5), and (6) in (2), we have the probability distribution p_{a_0}, p_{a_1}, and p_{a_2} for the attacker such as:

$$p_{a_0} = \frac{c_{a1}}{\omega_1}, p_{a_1} = \frac{c_{a2}}{\omega_2} - \frac{c_{a1}}{\omega_1}, p_{a_2} = 1 - \frac{c_{a2}}{\omega_2} \quad (7)$$

Similarly, the expected utility of the defender for playing strategy d_0, d_1, and d_2 are a function of the mixed strategy which are given by:

$$EU(p_{d_0}) = (p_{d_0})(0) + p_{a_1}(c_{a1} - \omega_1) + p_{a_2}(c_{a2} - \omega_2) \quad (8)$$

$$EU(p_{d_1}) = (p_{a_0})(c_{d1}) + p_{a_1}(c_{a1} - c_{d1}) + p_{a_2}(c_{a2} - \omega_2 - c_{d1}) \quad (9)$$

$$EU(p_{d_2}) = (p_{a0})(-c_{d2}) + p_{a_1}(c_{a1} - c_{d2}) + p_{a_2}(c_{a2} - c_{d2}) \quad (10)$$

Substituting (8), (9), and (10) in (3), we have the probability distribution p_{d_0}, p_{d_1}, and p_{d_2} for the defender such as:

$$p_{d_0} = 1 - (\frac{c_{d2} - c_{d1}}{\omega_2} + \frac{c_{d1}}{\omega_1}), \quad p_{d_1} = \frac{c_{d1}}{\omega_1}, p_{d_2} = \frac{c_{d2} - c_{d1}}{\omega_2} \quad (11)$$

TABLE II: Strategic form of the Attack-Defense game with two strategies.

		Defender (D)	
		d_0	d_2
Attacker (A)	a_0	0 , 0	c_{d2} , $-c_{d2}$
	a_2	$\omega_2 - c_{a2}$, $c_{a2} - \omega_2$	$c_{d2} - c_{a2}$, $c_{a2} - c_{d2}$

The mixed strategy NE for the non-cooperation security game is given by the distribution $\{p_{a_0}, p_{a_1}, p_{a_2}\}$, and $\{p_{d_0}, p_{d_1}, p_{d_2}\}$ of equations (7) and (11) which means that each player will randomize his selection conformity with the probability distribution. Consequently, the opponents in the game will be indifferent about the outcomes of the play.

2) MSNE for Security Game with Two-level Strategies: In case $c_{a2} << \omega_2$, we could have $p_{a_1} < 0$ according to Equation 7, which means that the attacker would need to be putting a negative weight on a_1 strategy to make other player indifferent between his three strategies, and that is impossible. On the other hand, this negative probability implies that the attacker has no incentive to deploy the a_1 strategy at all, and has strong incentive to always play a_2 strategy (level 2 of attack) instead of a_1 strategy (level 1 of attack) when he attempts to attack the system in order to maximize his payoff. In contrast, the defender does not have any incentive to play d_1 strategy (level 1 of defense) which will minimize his payoff and cost him more due to the increasing of the security value. Thus, the two strategies a_1 and d_1 could be eliminated completely from the strategy space. As a result, the game will reduce to 2-strategy for each player with new MSNE.

In case the system is under aggressive attack with very small cost of attacking, the non-coordination zero-sum security game will be reformulated with the new strategy space $\mathcal{S} = \{a_r, d_r | r \in \{0, 2\}\}$. The attacker has two pure strategies: a_0 = *No-Attack*, and a_2 = *Attack-2*. Also, the defender has two pure strategies: d_0 = *No-Defend*, and d_2 = *Defend-2*. Table II illustrates the payoff matrix of the game with two strategies form.

The distribution $\{p_{a_0}, p_{a_2} = 1 - p_{a_0}\}$ for the attacker, and $\{p_{d_0}, p_{d_2} = 1 - p_{d_0}\}$ for the defender are mixed strategy NE for the non-cooperation security game. In this case, each player will randomize his selection of two strategies conformity with the probability distribution and he will be indifferent about the outcomes of the play as well.

In order to compute these probabilities for the attacker, we calculate the expected utility as function of the mixed strategy which are given by:

$$EU(p_{d_0}) = (p_{a_0})(0) + p_{a_2}(c_{a2} - \omega_2) \tag{12}$$

$$EU(p_{d_2}) = (p_{a_0})(-c_{d2}) + p_{a_2}(c_{a2} - \omega_2) \tag{13}$$

The expected utility of the defender for playing strategy d_0, and d_2 are a function of the mixed strategy which are given by:

$$EU(p_{a_0}) = (p_{d_0})(0) + p_{d_2}(c_{d2}) \tag{14}$$

$$EU(p_{a_2}) = (p_{d_0})(\omega_2 - c_{a2}) + p_{d_2}(c_{d2} - c_{a2}) \tag{15}$$

As we mentioned above, the expected utilities of playing the two strategies of each player are equal and no player has incentive to change his strategy. Thus,

$$EU(p_{d_0}) = EU(p_{d_2}) \tag{16}$$

$$EU(p_{a_0}) = EU(p_{a_2}) \tag{17}$$

Then, substituting (12), and (13) in (16), and (14), and (15) in (17) and solving the expression in order to find the probabilities that correspond to the equilibrium, we get:

$$p_{a_0} = \frac{\omega_2 - c_{d2}}{\omega_2}, p_{a_2} = 1 - \frac{\omega_2 - c_{d2}}{\omega_2} \tag{18}$$

$$p_{d_0} = \frac{c_{d2}}{\omega_2}, p_{d_2} = 1 - \frac{c_{d2}}{\omega_2} \tag{19}$$

IV. Case Study of the Attack-Defense Game

In this section, we study several types of network attacks and discuss what strategies attackers or defenders can take with minimum resource consumption. In the following subsections, we introduce three concrete attack defense scenarios to illustrate how attack-defense strategies and their dynamic interactions can be modeled via our game theoretic framework.

A. Defense System Against Hello Flood Attack

Hello flood attack [9] is one of the common attacks in the network layer that a wireless sensor network (WSN) could face, where the attacker will be able to create an illusion of being a neighbor to other nodes or a base station. The hello flood attack can be implemented by an attacking node by sending or replying the hello packets, which are used for neighbor discovery, with significantly high transmission power. This action will convince the nodes in the network that the adversary node is their neighbor.

1) Attack Strategies: In our security game, the hello flood attacker will play the game by employing one of the two levels of attack in case he decides to attack the system as we mentioned above (i.e., Level one or two). In the low intensity level-one attack, the adversary node sends hello message to sensor nodes and convince them that the adversary is one of their neighbors. Thus, the attacker will behave as a false neighbor node [10]. On the other hand, in the high intensity level-two attack, the adversary node rebroadcasts the received Route Request Packet (RREQ) with high power to a large number of nodes and convinces the nodes that the attacker node is their base station. More specifically, the communication of the sensor nodes with the base station usually occurs through their neighbors. Thus, when the attacker succeeds in creating a false node as base station, and broadcasts a message to all nodes with a high power transmission, the regular node will be confused, convinced that the message came from its neighbor, and assume that this is shortest path from the base station. The adversary in this case can control the entire network through being a false base station [11] [12].

2) Defense Strategies: In contrast, the defender has one of the two levels of defense against this type of attack. The level-one defense, which is suitable for dealing with the level-one attack, does not require high computational power or battery power to implement. This low level of defense is based on response timing, which is correlated with the transmission distance. There is a predefined time threshold and a normal node should reply a hello message within that time interval. In case the reply message sent by a node is not received in that

time by the hello message requesting node then the responding node will be treated as a malicious node [10] [11].

The second level defense strategy is a more advanced detection technique against the aggressive hello flood attack and requires more computational power and battery power than the level-one defense strategy. The level-two defense strategy could be Signal Strength plus hello message based client puzzles scheme (MBCP) [12]. In this scheme, the nodes are classified as friends according to the signal strength, where each node checks the signal strength of the received hello message with respect to a known reference signal strength. Therefore, if the received signal strength of hello message is the same as the predefined fixed signal strength in the radio range, then the requesting node is a legal node. Otherwise, the node will be classified as a stranger and needs to be further validated. In order to check the validity of a suspicious node, short client puzzles will be used; and with the increasing number of hello messages sent, the difficulty of solving the puzzle will rise as well [12]. Another technique could be applied as a level-two defense for WSN is location verification scheme, which verifies the locations of abnormal nodes by filtering the nodes into normal node or malicious node. The detection of the attack utilizes the greedy filtering by matrix location verification scheme [13]. In summary, the game theoretic strategies of this attack and defense game are as follows:

- **Attacker** a_1 : Behave as a false neighbor
- **Attacker** a_2 : Behave as a false base station
- **Defender** d_1 : Response timing scheme
- **Defender** d_2 : Signal strength and hello message based client puzzles scheme (MBCP); or location verification scheme

B. Defense System Against Malware Attack

Malware is one of the major threats faced by our cyber-world. It is powerful enough to cause a substantial damage. Throughout the cyber warfare between malware attackers and defenders, malware has evolved with more advanced propagation, compromising, and stealthy techniques, and has be widely used by various attackers to disrupt business operation, steal sensitive information, gain unauthorized access or any other targeted behavior [14].

1) Attack Strategies: The attacker in the proposed game model can alternate between two different intensities of malware attacks according to his effort and cost of the attacks. The first level attack (i.e., level-one attack) is to generate malware by reusing existing malicious code. Such a malware is easy to produce without requiring significant skill from the attacker, but at the same time it is easy to be detected by signature-based security systems as well.

The second level malware attack (i.e., level-two attack) is more destructive and harder to defend, where the malware is generated by using zero-day vulnerability, or advanced attacking techniques such as polymorphism or metamorphism. Polymorphic malware changes its appearance and creates a countless number of distinct decryptors, and metamorphic malware can automatically re-code itself each time it spreads out by making the best use of obfuscation techniques [15] [16]. By dynamically changing the code format and signature, these advanced attacking techniques make it much harder for defenders to detect a malware.

2) Defense Strategies: The level-one defense against malware attacks, which is suitable to protect a security system against the level-one malware attack, utilizes the signature-based security system known as static analysis. It relies on its own signature dataset to detect and block recognized malware [15]. Existing signature-based security systems, such as various anti-virus software, as long as they have updated signature database, are fast and effective for fending off level-one malware described above. However, this type of defense will be insufficient against level-two malware attacks where the attacker uses new variants of malware to avoid signature based detection.

Therefore, the level-two defense is the more advanced strategy that has higher requirements on computation power, Internet connectivities, detection response time, and security staff skill/knowledge, etc. This level of defense utilizes dynamic malware analysis techniques, such as Sandbox, to diagnose malware by utilizing a virtual system to analyze the suspected files. The operating principle of this virtual system is to monitor the real running status of a suspicious file, and determine whether or not the file is malicious based on its observed behavior [17] [18]. In summary, the game theoretic strategies of this attack and defense game are as follows:

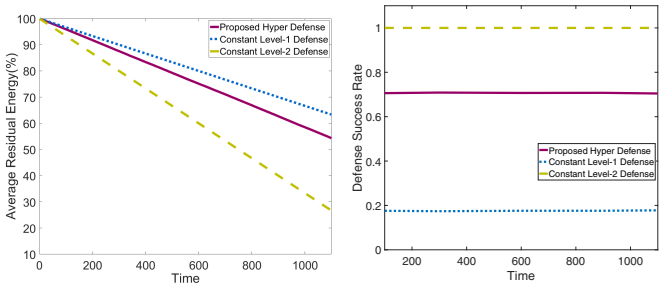
- **Attacker** a_1**:** Malware generated using existing malicious code
- **Attacker** a_2**:** Malware generated by using zero-day vulnerability, polymorphic or metamorphic coding techniques
- **Defender** d_1**:** Static Analysis (i.e.,signature-based security system)
- **Defender** d_2**:** Dynamic malware analysis techniques (Sandbox)

C. Defense System Against Password Guessing Attack

Authentication is an essential element of any security model. Most real-world cyber systems rely on password for authentication. A common threat for password-based authentication is password guessing attack, which is a brute force attack that attempts to discover a user password by systematically trying every possible combination of the password.

1) Attack Strategies: The first level attack is a low intensity of password guessing trials that require no skill from an attacker. The attacker will behave as a normal user and send one login attempt one at a time. This type of password guessing attack is slow in password trial, and hence, could take a very long time for an attacker to discover the correct password.

The second level attack is a high intensity of password guessing trials by utilizing more advanced techniques, such as using the multiple virtual clients scheme [19]. Using such a scheme, an attacker could create many virtual clients from one computing device. These virtual clients behave as completely independent normal users. In this way, an attacker could try many passwords concurrently and thus dramatically speed up the password guessing process.



(a) (b)

Fig. 2: Average residual energy and defense success rate when ω is higher than c_{an} and c_{dn} (i.e, $\omega_n > c_{an}, c_{dn}, n \in \{1, 2\}$), and the cost of attack and defense are equal (i.e., $c_{an} = c_{dn}$), respectively.

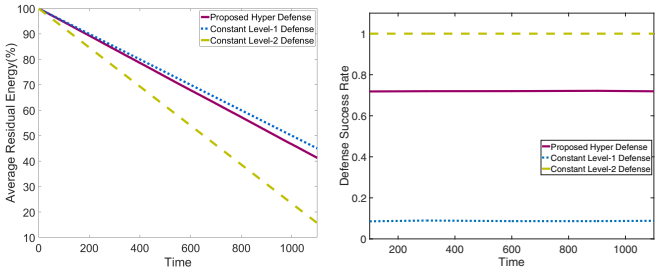
2) Defense Strategies: The low level of defense is login throttling scheme. Basically speaking, this scheme limits the frequency of failed login attempts. It can simply put an upper limit on the number of failed login attempts within a given time period, or ask the client to compute the response for a given challenge in order to ensure that the client is not able to launch a large number of password trials in a small amount of time. A large number of password guesses in a small time interval will be eliminated by Making password guessing action a time consuming and costly for an adversary [20].

The high level of defense against the level-two password guessing attack described above is intrusion detection system that has efficient detection mechanism and high speed of detection. The defender will be able to determine the true source of attacker's requests by extracting the device fingerprint. "Device fingerprinting is the process of gathering device information to generate device-specific signatures and using them to identify individual devices" [21]. These fingerprints can be extracted from the traffic (transmitted signal) by utilizing an advanced analysis across the protocol stack in order to identity spoofing [21]. In summary, the game theoretic strategies of this attack and defense game are as follows:

- **Attacker** a_1**:** Behave as one normal user and sends one login request at a time.
- **Attacker** a_2**:** Utilize virtual client techniques in order to send many login requests concurrently at a time.
- **Defender** d_1**:** Throttling authentication attempts scheme
- **Defender** d_2**:** An advanced intrusion detection system that can identify login request real sources (device fingerprint)

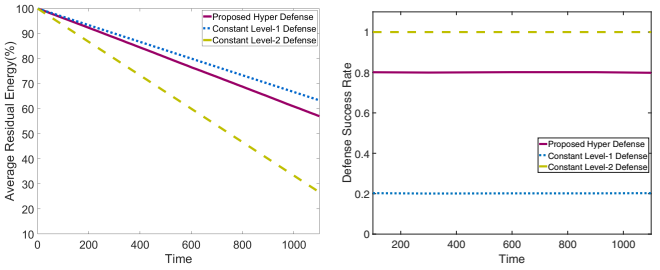
V. Performance Evaluation

In this section, we have simulated our proposed approach (i.e., hyper defense) for wireless sensor network scenario and compared it with two "always-on" constant defending systems in order to validate the performance of our model. The first constant defending system employs the low intensity (level-one) defense all the time, and the second constant defending system employs the high intensity (level-two) defense all the time as well. We assume that all the nodes in the network have the same initial battery energy in the beginning of the game. We also take into account a network where the nodes consider the battery life as the priority requirement, and where



(a) (b)

Fig. 3: Average residual energy and defense success rate when ω is higher than c_{an} and c_{dn} (i.e, $\omega_n > c_{an}, c_{dn}, n \in \{1, 2\}$, and $c_{an} < c_{dn}$)



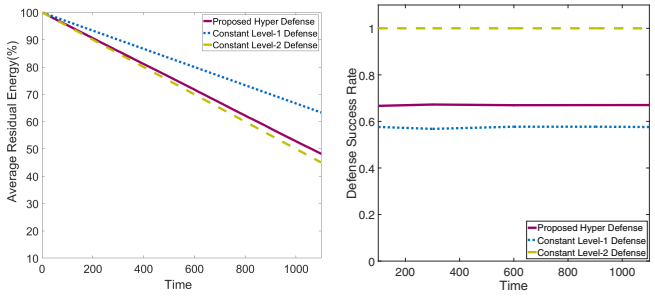
(a) (b)

Fig. 4: Average residual energy and defense success rate when ω is higher than c_{an} and c_{dn} (i.e, $\omega_n > c_{an}, c_{dn}, n \in \{1, 2\}$, and $c_{an} > c_{dn}$).

the nodes defend against resource consumption attacks. The attacker aims at attacking the network and destroying/reducing the lifetime of the network. In such circumstances, the security value ω may be represented by the conserved energy by success defense action. The attacker and defender will play the game according to the equations in section III-C.

The proposed attack-defense model (i.e., hyper defense) tries to achieve a suitable defense strategy for the system as well as to consider the limitation of the resources. We evaluate system performance by identifying two metrics: average residual energy, and defense success rate. Furthermore, we consider the variety of security value ω_n compared to the cost of attack c_{an} and cost of defense c_{dn} in order to show the impact of this variable ω_n on the performance of the model in two experiments.

In the first experiment, we assume that the security value ω_n is higher than the attacking and defending cost (i.e., $\omega_n > c_{an}$ and $\omega_n > c_{dn}$) while considering the variety of the attack and defense cost as illustrated in Figures 2, 3, and 4. In Figure 2, the cost of attack and defense are assumed to be equal (i.e., $c_{an} = c_{dn}$). In Figure 3, the attacking cost is assumed to be less than the defending cost (i.e., $c_{an} < c_{dn}$). Inversely, the cost of attack is assumed to be higher than the cost of defense (i.e., $c_{an} > c_{dn}$) in Figure 4. The proposed hyper defense achieves a higher percentage of average residual energy than the constant level-2 defense. In the proposed hyper defense, the defender still has $55\%, 40\%$, and 58% of the energy in the three scenarios (i.e., Figures 2(a), 3(a), and 4(a)) of different defending/attacking cost, respectively. However, the defender has $29\%, 18\%$, and 28% of the energy in the constant the constant level-2 defense as shown in Figures 2(a), 3(a), and



(a) (b)

Fig. 5: Average residual energy and defense success rate when ω is significantly higher than c_{an} and c_{dn} (i.e, $\omega_n >> c_{an}, c_{dn}, n \in \{1, 2\}$).

4(a), respectively.

In addition, the constant level-1 defense consumes less amount of energy, but we notice that the defense success rate is too low compared with our proposed model. The hyper defense produces a good defense success rate (i.e., 0.7, 0.7, and 0.8) as illustrated in Figures 2(b), 3(b), and 4(b), respectively, compared with the constant level-1 defense as well as achieving a higher residual energy compared with the constant level-2 defense approach.

In the second experiment, we consider the diversity of security value compared with attacking and defending cost. We assume that security value ω_n is significantly higher than c_{an} and c_{dn}, and assume that $c_{an} = c_{dn}$. This means that if the attacker succeeds, the system will be at a very high risk and suffer a big loss. Figure 5 presents the average residual energy and defense success rate when the security value ω_n is significantly higher than the cost of attack c_{an} and cost of defense c_{dn}. It is interesting to observe that hyper defense still has a higher average residual energy than the constant level-2 defense approach as shown in Figure 5(a).

Moreover, from Figure 5(b), we see that the proposed hyper defense achieves a higher defense success rate than the constant level-1 defense. Because of the high security value, the defender's chances of activating/utilizing the Defend-2 strategy also increase, and the chance of utilizing each strategy will be dynamically adjusted according to the variable cost in our proposed model. This implies that the equilibrium of the proposed security game is fairly robust on the performance of the hyper defense system. As a final comment, the proposed hyper defense system saves energy and achieves a high rate of success concurrently instead of turning on the defense system 100% of the time, especially for a network that emphasizes on energy efficiency.

VI. Conclusions

In this paper, we proposed a non-cooperative attack-defense security game to model the continuous and evolving interactions and cyberwar activities between attackers and defenders. In this game, we have used a three-level attack/defense strategy model to provide a generalized modeling of the strategy choices by attackers and defenders. From the game model we have derived the mixed strategy Nash equilibrium. Finally, we have shown the performance of the proposed model when compared with two different constant defense systems as demonstrated in our experiments.

VII. Acknowledgment

This work is supported by National Science Foundation (DGE-1723587).

References

[1] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," in *IEEE First International Conference on Data Science in Cyberspace (DSC)*, June 2016.

[2] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *43rd Hawaii International Conference on System Sciences*, pp. 1–10, Jan 2010.

[3] A. E. Chukwudi and I. C. Eze Udoka, "Game theory basics and its application in cyber security," *Advances in Wireless Communications and Networks*, vol. 3, no. 4, pp. 45–49, 2017.

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys (CSUR)*, vol. 45, no. 3, p. 25, 2013.

[5] M. Fallah, "A puzzle-based defense strategy against flooding attacks using game theory," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, pp. 5–19, Jan 2010.

[6] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proceeding from the 2006 workshop on Game theory for communications and networks*, p. 4, ACM, 2006.

[7] M. Mohi, A. Movaghar, and P. M. Zadeh, "A bayesian game approach for preventing dos attacks in wireless sensor networks," in *Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on*, vol. 3, pp. 507–511, IEEE, 2009.

[8] D. Fudenberg and J. Tirole, "Game theory. 1991," *Cambridge, Massachusetts*, vol. 393, 1991.

[9] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," *IJCSI International Journal of Computer Science Issues*, vol. 7, no. 11, pp. 23–27, 2010.

[10] A. Dubey, D. Meena, and S. Gaur, "A survey in hello flood attack in wireless sensor networks," *Int. J. Eng. Res. Technol*, vol. 3, 2014.

[11] M. S. Haghighi and K. Mohamedpour, "Securing wireless sensor networks against broadcast attacks," in *Telecommunications, 2008. IST 2008. International Symposium on*, pp. 49–54, IEEE, 2008.

[12] R. Singh, D. J. Singh, and D. R. Singh, "Hello flood attack countermeasures in wireless sensor networks," 2016.

[13] R. S. Hassoubah, S. M. Solaiman, and M. A. Abdullah, "Intrusion detection of hello flood attack in wsns using location verification scheme," *International Journal of Computer and Communication Engineering*, vol. 4, no. 3, p. 156, 2015.

[14] R. Rehman, G. Hazarika, and G. Chetia, "Malware threats and mitigation strategies: a survey," *Journal of Theoretical and Applied Information Technology*, vol. 29, no. 2, pp. 69–73, 2011.

[15] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, pp. 297–300, Nov 2010.

[16] A. Sharma and S. K. Sahay, "Evolution and detection of polymorphic and metamorphic malwares: A survey," *arXiv preprint arXiv:1406.7061*, 2014.

[17] J. Kim, S. Lee, J. M. Youn, and H. Choi, "A study of simple classification of malware based on the dynamic api call counts," in *International Conference on Computer Science and its Applications*, pp. 944–949, Springer, 2016.

[18] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," *ACM computing surveys (CSUR)*, vol. 44, no. 2, p. 6, 2012.

[19] O. Nakhila and C. Zou, "Parallel active dictionary attack on ieee 802.11 enterprise networks," in *MILCOM IEEE Military Communications Conference*, pp. 265–270, Nov 2016.

[20] V. Goyal, V. Kumar, M. Singh, A. Abraham, and S. Sanyal, "Compchall: addressing password guessing attacks," in *Information Technology: Coding and Computing, ITCC. International Conference on*, vol. 1, pp. 739–744, IEEE, 2005.

[21] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 94–104, Firstquarter 2016.