Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Two-layer Deception Model Based on Signaling Games Against Cyber attacks on Cyber-Physical Systems.

PRIVA CHASSEM KAMDEM[1], ALAIN ZEMKOHO[2], LAURENT NJILLA[3],(Member, IEEE) Marcelin Nkenlifack [4], Charles Kamhoua [5],(Senior Member, IEEE).

[1] Department of Mathematics, Computer Science, University of Dschang, BP 96 Dschang, Cameroon (priva.chassem@univ-dschang.org)
[2]School of Mathematical Sciences, University of Southampton, SO17 1BJ Southampton, UK (a.b.zemkoho@soton.ac.uk)
[3]Information Assurance Branch, Air Force Research Laboratory, Rome, NY, USA (laurent.njilla@us.af.mil)
[4]Department of Mathematics, Computer Science, University of Dschang BP 96 Dschang, Cameroon, (marcellin.nkenlifack@gmail.com)
[5]Charles Kamhoua Network Security Branch, DEVCOM Army Research Laboratory, delphi, MD, USA (charles.a.kamhoua.civ@army.mi)

Corresponding author: Priva Chassem Kamdem (e-mail: priva.chassem@univ-dschang.org).

The research was sponsored by the DEVCOM ARL Army Research Office and was accomplished under Grant Number W911NF-21-1-0326. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

ABSTRACT Cyber-physical systems (CPS) are increasingly vulnerable to sophisticated cyber-attacks that can target multiple layers within the system. To strengthen defenses against these complex threats, deception-based techniques have emerged as a promising solution. While previous research has primarily focused on single-layer deception strategies, the authors argue that a multi-layer approach is essential for effectively countering advanced attackers capable of perceiving information across both the application and network layers. In this work, we propose a two-layer deception model based on signaling games to enhance the defense of CPS. Our model captures the dynamic, non-cooperative interactions between the attacker and defender under conditions of incomplete information. Unlike existing approaches, our model expands the defender's action space to incorporate deception at both the application and network layers, while maintaining the attacker's uncertainty about the true system type. Through analytical and simulation results, we identify the Perfect Bayesian Nash Equilibrium (PBNE) strategies for both players. Our findings demonstrate that the two-layer deception model significantly outperforms single-layer deception in deceiving the attacker and improving system resilience, particularly against sophisticated adversaries capable of perceiving information across multiple layers.

INDEX TERMS Cyber-physical systems, Cyberattacks, Deception-based techniques, Defender's action space, Signaling games, Perfect Bayesian Nash equilibrium.

I. INTRODUCTION

Deception has a long history of effective use in the military domain and is now being deployed for the protection of information systems. As Cohen and Koike [1] point out, misleading attackers through deception techniques can significantly enhance the defensive mechanisms of information systems. Murphy, McDonald, and Mills [2] also explore the application of deception in cyberspace, highlighting strategies such as the obfuscation of operating systems, which allow for misdirecting attackers by complicating the target's perceptibility.

However, current deception techniques, especially in the realm of cyber-physical systems (CPS), are often limited to single-layer approaches that focus on either the application layer or the network layer individually. These one-dimensional techniques fail to fully address the multifaceted nature of CPS, where attackers can exploit vulnerabilities across both layers simultaneously. This limitation is particularly critical because CPS represent a complex integration of computing systems, networks, and physical systems, making them more vulnerable than conventional embedded systems. As pointed out by Yaacoub et al. [3], the increased con-

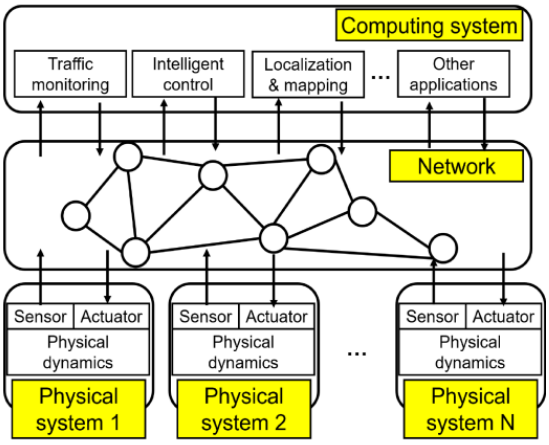


FIGURE 1. A hierarchical cyber-physical system structure [7]. This architecture represents a Cyber-Physical System (CPS) in three layers: the Application layer for user interfaces and interactions, the Network layer for communication and connectivity between systems, and the Physical layer for hardware components and control systems. This structure allows for seamless integration between the software and hardware aspects of the CPS.

nectivity of CPS exposes them to a wide range of attack vectors, targeting not only the information systems but also the network and physical components.

In a world where cyberattacks result in considerable economic losses, with the cost of cybercrime estimated to reach $1000 billion per year [4], it is crucial to develop advanced defense strategies. One-layer deception techniques, while useful, are insufficient to protect against intelligent and adaptive attackers who can perceive and exploit vulnerabilities across different layers. Sensitive sectors such as banking are frequent targets of attacks, particularly DDoS attacks, which can lead to significant financial losses [5]. In light of this, our research introduces a novel two-tier deception strategy that simultaneously applies deception at both the application and network layers. This approach allows the defender to mislead attackers across multiple dimensions, increasing the attacker's uncertainty and thus enhancing the overall security of the system.

In this context, the CPS model we propose draws inspiration from the hierarchical structure of the Purdue Enterprise Reference Architecture (PERA), which is widely used in industrial control systems [6]. In this architecture, the layer of physical systems corresponds to the lower layers of PERA, including the specification, detailed design, manifestation, and operation layers. The network layer is equivalent to the definition layer in PERA, while the application layer aligns with the upper layers, encompassing the conceptual and definition layers as shown in Fig. 1. It is important to note that an attacker can perceive the upper layers of the system from a distance, enabling them to analyze operations and exploit their exposure to orchestrate attacks.

Our research addresses a significant gap in current studies by introducing a two-tier deception model that applies deception at both the application and network layers. This results in a more robust and resilient defense system. Recent advances in event-triggered control have proven effective in enhancing the responsiveness of defenses in cyber-physical systems (CPS) by automatically triggering actions in response to attack signals, thus optimizing resource usage [8], [9]. Our research builds on these developments by introducing a two-layer deception strategy that simultaneously targets the application and network layers, increasing the attacker's uncertainty. While event-triggered control focuses on reactive measures, our proactive deception model further complicates the attacker's decision-making in CPS environments. Given the limitations of single-layer deception techniques identified in previous research [10], [11], [12], our goal is to propose a two-layer strategy to strengthen defenses. This strategy simultaneously applies deception at both the application and network layers, maintaining the attacker's uncertainty about the type of system they are interacting with. It provides a more comprehensive and effective solution for combating advanced cyberattacks targeting cyber-physical systems (CPS).

We model the interaction between the attacker and defender using a signaling game, a dynamic and non-cooperative framework where decisions are made based on incomplete information. By extending the defender's action space to incorporate deception across both layers, our model offers a more tailored response to the complexities of CPS. The optimal strategies for both the attacker and the defender are determined by solving for the Bayesian perfect Nash equilibrium, ensuring that neither party has an incentive to unilaterally deviate from their strategy. This two-tier strategy provides a more complete and effective solution for countering advanced cyberattacks, enhancing both the resilience and adaptability of the defense system in the face of complex threats.

In our simulations, we varied the attacker's beliefs about the system and assessed the level of deception in two scenarios: interaction with single-layer deception and interaction with two-layer deception. Our results show that two-layer deception significantly outperforms single-layer deception in terms of confusing and delaying the attacker, leading to more effective defensive outcomes.

To the best of our knowledge, this research is the first to propose a two-tier deception strategy for CPS security using a signaling game approach. This novel contribution addresses the limitations of one-layer deception techniques, which have been widely studied in the literature, by offering a more comprehensive and robust framework for defending against modern, sophisticated cyberattacks.

II. RELATED WORK

Deception has become a key element in cybersecurity strategies, enabling analysts to steer attackers' actions in a way that facilitates their detection and capture. Game-theoretic models provide an ideal framework for analyzing the adversarial dynamics between defenders and attackers. Interactions under incomplete information in this context can be approached from two perspectives: robust game theory and the Bayesian

model. The former, as highlighted by Aghassi and Bertsimas [13], focuses on managing worst-case scenarios, whereas the latter introduces variability to represent the types of actors, allowing for the development of strategies and equilibria based on pre-existing beliefs [14].

Recent studies have examined various aspects of deception strategies within signaling games. For instance, Zhuang, Bier, and Alagoz [15] focus on mechanisms of deception and confidentiality in multi-stage signaling games, highlighting the complexity of these interactions. Pawlick and Zhu [16] developed a signaling game model that elucidates the interactions between these two parties in a network environment. Their research reveals that the equilibria in these signaling games are refined equilibria, ensuring that participants have no incentives to unilaterally change their strategies at equilibrium. Furthermore, Huang and Zhu [11] proposed a multi-stage Bayesian game model characterizing sophisticated, adaptive, and persistent attacks, while suggesting long-term optimal defensive policies. Another significant model, developed by Hu et al. [17], focuses on interactions using a two-way signaling game framework, exploring the confrontation between attackers and defenders. Their study also includes an algorithm to identify refined Bayesian equilibria, enriching the analysis of defense strategies. The issue of manipulating participants' beliefs is also addressed in deception games. Zhang and Zhu [18] examine a hypothesis testing game where the receiver assesses the nature of a binary system, while considering the possibility for the sender to manipulate the signal. This exploration is crucial for understanding how information manipulation can influence the decisions of involved parties.

More recently, advancements have also emerged in the context of cyber deception. Beltran et al. [19] provide a comprehensive analysis of Cyber Deception (CYDEC) mechanisms, proposing a taxonomy and reviewing solutions with and without Artificial Intelligence (AI). While their work offers a solid framework for classifying deception solutions, it does not sufficiently explore multi-layer deception scenarios, particularly the interactions between the cyber and physical layers, which are crucial in complex systems. Our model proposes an innovative approach by introducing coordination between these layers to maximize the effectiveness of defense strategies. Hemida et al. [20] investigate the application of game theory in designing deception strategies for early threat detection in cyber-physical systems. Their work highlights the importance of coordinated defense between cyber and physical layers to enhance the believability and effectiveness of deception strategies. However, while this work emphasizes the need for multi-domain coordination, it lacks a comprehensive modeling of the strategic interactions between these layers. Our approach addresses this gap by introducing a two-layer game model, where each layer (cyber and physical) adopts joint strategies to deceive attackers in a coordinated manner. Sayed et al. [12] presents a game model for honeypot allocation in dynamic tactical networks. This model incorporates attacker preferences and the evolving connectivity of networks, providing an optimized strategy to divert attacks toward decoy resources. However, this approach is limited to the cyber layer and does not address potential interactions with the physical layer in complex cyber-physical systems. In our work, we extend these concepts by introducing a multi-layer model that considers both the cyber and physical layers, enabling a more robust defense in environments where both layers are critical. The results of these studies underscore the importance of using deception and camouflage in network defenses. They show that sophisticated deception strategies can significantly enhance defense capabilities against intelligent attacks, notably through the use of decoys such as honeypots [21].

Despite the progress made in designing deception strategies for cyber-physical systems, several shortcomings remain. First, existing approaches primarily focus on the cyber layer, often neglecting the integration of other layers within these systems. Secondly, there is a lack of comprehensive modeling of strategic coordination between layers, which is essential for maximizing the effectiveness of defenses in complex environments where cyberattacks can target multiple layers. Our work addresses these gaps by proposing a two-layer signaling game model that captures the interdependencies between the cyber and physical domains, thereby providing a more robust and integrated defense strategy.

To the best of our knowledge, our current work constitutes the first attempt to model deception in network security within CPS by simultaneously considering two layers through a signaling game.

III. PROBLEM FORMULATION

Automotive systems represent a quintessential case of CPS due to their complex integration of physical mechanisms and digital processes. As modern vehicles, they combine sophisticated hardware components with advanced control systems, offering a multitude of safety, comfort, and connectivity features. This convergence between the physical and digital worlds is manifested through three fundamental layers:

- **The application layer:** This includes user interfaces, such as digital dashboards and mobile applications, which allow drivers to interact intuitively with the vehicle [22].
- **The network layer:** This manages communication between the various components of the vehiclefrom sensors to actuators, including embedded control systems ensuring smooth information exchange and effective coordination of actions [22] [23].
- **The physical layer:** This encompasses all hardware elements, such as engines, brakes, and sensors (including radars and LIDAR), which form the tangible foundation upon which the vehicle's performance and safety rely [23].

Together, these three layers perfectly illustrate the complex and dynamic interaction that characterizes modern CPS.

However, an automotive system can be targeted by an attacker seeking to gain remote control. Suppose that when the attacker successfully breaches the infotainment system,

thereby gaining access to the vehicle's control interfaces, the vehicle's defense system activates to deceive the attacker simultaneously on both the network and application layers in a coherent manner:

- **On the application layer:** The defender deploys a deceptive user interface, such as a fake mobile application showing seemingly optimized alternate routes. This interface presents fictitious data, created to correspond with modifications made at the network level.
- **On the network layer:** Simultaneously, the defender falsifies communication messages between the various elements of the vehicle. These modified messages are coordinated with the data displayed on the user interface to create a coherent illusion for the attacker.

Thus, despite having access to the system, the attacker is faced with misleading information on the two key layers of the system. As a result, they are unable to effectively take control of the vehicle, as the deception mechanisms deployed by the defender lead them astray in a synchronized manner.

IV. SIGNALING GAME FOR TWO-LAYER DECEPTION

In this section, we intend to explore the concept of signaling game applied to a two-layer deception model. This type of game highlights the strategic dynamics between the different actors involved.

A. TWO-SENDER SIGNALING GAME

We aim to model our deception system using a two-sender signaling game, where the players are the defender (D) and the attacker (A). The defender represents the vehicle's security mechanisms, capable of deploying deceptive strategies across two critical layers: the application layer and the network layer. These layers act as senders in the game. The first sender, the application layer (s_1), can send signals such as a deceptive user interface displaying fake routes to the attacker. The second sender, the network layer (s_2), can simultaneously send falsified communication messages between the vehicle's components, aligned with the fictitious data presented by S1. The attacker observes the signals from both senders and must decide whether to trust the information and proceed with their control strategy or abort the attack. The defender has the option to adopt different signaling strategies: either honest signaling, where the signals correspond to the true state of the system, or deceptive signaling, where the signals are coordinated to mislead the attacker by presenting a coherent but false system state.

This two-sender signaling game framework effectively captures the interaction between the defender and the attacker in a modern automotive cyber-physical system, where deception is used to protect the system from unauthorized control. Fig. 2 illustrates the interaction between the application and network layers within the signaling game model, showing how signals are coordinated to deceive the attacker.

Fig.2 shows the two-sender signaling game model, where the application and network layers send coordinated signals

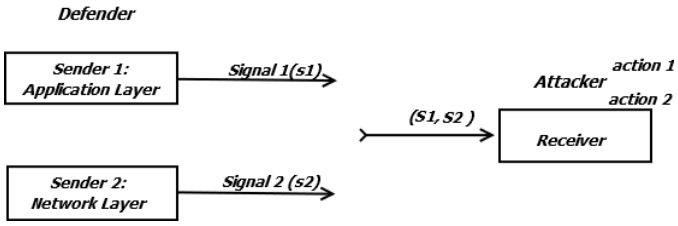


FIGURE 2. Signaling Game Model for Two-layer in an Automotive Cyber-Physical System

to deceive the attacker. The attacker then decides on an action based on the received signals.

B. GAME MODEL

The signaling game for two-layer deception in a defense strategy can be represented by a six-tuple $G_D = \{N, \Theta, M, S, p, J\}$, where:

- **Players** (N):
  - Defender (D): The player responsible for deploying deception strategies on two layers to protect Automotive System.
  - Attacker (A): The player attempting to compromise the Automotive System by interpreting the signals from the application and network layers.
- **Types** (Θ):
  - $\Theta = \{\text{Honeypot (H)}, \text{Normal (N)}\}$.
  - The defender knows their own type, which determines whether the system components are real (Normal) or deceptive (Honeypot). The attacker, however, is unaware of the defender's type and must infer it from observed signals.
- **Signals** (M):
  - $M = M_1 \times M_2$, where:
    - M_1: Signal from the application layer, which could be manipulated to show false information to the attacker.
    - M_2: Signal from the network layer, which could be falsified messages that correspond to the deception strategy of the application layer.
- Defender's Strategies (S_D): $S_D = S_{D1} \times S_{D2}$, where:
  - S_{D1}: Set of actions on the application layer (normal signal:"n" or honeypot signal:"h").
  - S_{D2}: Set of actions on the network layer (normal signal:"n" or honeypot signal:"h").
  - The defender's combined strategy is represented by pairs $(s_1, s_2) \in S_{D1} \times S_{D2}$, resulting in two possible actions:
    - (n, n): Sending a normal signal on both layers.
    - (h, h): Simultaneous deception on both layers in a coherent manner.

    The other combinations (n, h) and (h, n) are not relevant because they involve a mixture of "normal" and "decoy" signals on the two layers. Such an

inconsistency between the layers would be easily detectable by the attacker, rendering the deception attempt ineffective.

- Attacker's Strategies (S_A):
  - $S_A = \{a\}$, where:
    - $a \in \{\text{Attack (v)}, \text{Not Attack (nv)}\}$, representing whether the attacker decides to launch an attack based on the observed signals.
- **Prior Belief** (p):
  - $p = P(\theta)$ avec $\theta \in \Theta = \{H, N\}$, representing the attacker's belief about the likelihood of the system being a honeypot. This belief influences the attacker's strategy by updating it based on the signals received.
- **Payoff Functions** (J):
  - Defender's Payoff (J_D): $J_D : \Theta \times S_D \times S_A \to \mathbb{R}$.
    - The payoff function J_D for the defender depends on the true type $\theta \in \Theta$, the chosen actions $(s_1, s_2) \in S_D$ on the two layers, and the attacker's action $a \in S_A$. It reflects the effectiveness of the deception strategy and the cost or benefit derived from it.
  - Attacker's Payoff (J_A): $J_A : \Theta \times S_A \to \mathbb{R}$.
    - The payoff function J_A for the attacker is influenced by the true type $\theta \in \Theta$, the signals $(m_1, m_2) \in M$ observed from the two layers, and the action $a \in S_A$. It represents the success or failure of the attack and the associated costs or rewards.

C. ASSUMPTIONS

To further analyze this signaling game, we introduce the following hypotheses related to the signals and the deception layers employed by the Defender:

1) **assumptions 1: Consistency and Synchronization with Honeypot Signals**
When both generated signals (m_1 and m_2) are decoys, the Defender ensures consistency and synchronization between the two deceptions. This means that the actions taken on the application and network layers are designed to align with a singular strategic deception aimed at luring the attacker into a false sense of security.
2) **assumptions 2: Cost difference between application and network layer honeypots**
The cost of implementing a honeypot on the network layer is lower than that of the application layer, because the application layer is the highest layer and the first one perceived by the attacker. In a single-layer deception scenario, the application-layer honeypot will take precedence over the network honeypot, thus influencing the attacker's perception in a single-layer deception scenario.

D. PAYOFF FUNCTION

The attacker's payoff function, denoted J_A, depends on the defender's actions a_{d1} and a_{d2}, the attacker's action a_a, and the defender's type θ. Let $a_d = (a_{d1}, a_{d2})$. The payoff function is defined as follows:

$$J_A(a_d, a_a, \theta) = \begin{cases} v_a - c_a & \text{if } \theta = N \text{ and } a_a = v \\ -c_0 - c_a & \text{if } \theta = H \text{ and } a_a = v \\ 0 & \text{if } a_a = nv \end{cases} \quad (1)$$

The attacker aims to maximize their profit by targeting the normal system, where they have the opportunity to compromise the system and receive a reward v_a. However, if the attacker is misled into attacking a honeypot, they incur significant costs c_0 in addition to the attack costs c_a. This situation creates a strong incentive for the attacker to accurately identify the defender's type. Misidentification could lead to targeting a honeypot and incurring substantial costs without gaining the expected reward. Therefore, understanding the defender's type is crucial for the attacker to optimize their strategy and minimize losses.

The defender's payoff function, denoted J_D, depends on the defender's actions a_{d1} and a_{d2}, the attacker's action a_a, and the defender's type θ. Let $a_d = (a_{d1}, a_{d2})$. Let $J_D(a_d, a_a, \theta) = J_D^\theta$, the payoff function is defined as follows:

$$J_D^\theta = \begin{cases} b_w - c_h, & \text{if } a_a = v, \theta = H, a_d = (h,h) \\ b_w - c_h - c_1 - c_2, & \text{if } a_a = v, \theta = H, a_d = (n,n) \\ -c_c - c_1 - c_2, & \text{si } a_a = v, \theta = N, a_d = (h,h) \\ -c_c, & \text{if } a_a = v, \theta = N, a_d = (n,n) \\ -c_h, & \text{if } a_a = nv, \theta = H, a_d = (h,h) \\ -c_h - c_1 - c_2, & \text{if } a_a = nv, \theta = H, a_d = (n,n) \\ b_{cs} - c_1 - c_2, & \text{if } a_a = nv, \theta = N, a_d = (h,h) \\ b_{cs}, & \text{if } a_a = nv, \theta = N, a_d = (n,n) \end{cases}$$

When the defender is of the honeypot type ($\theta = H$), they gain a benefit b_w by luring the attacker into targeting the honeypot rather than the normal system. This benefit is offset by the cost of implementing the honeypot across both layers, denoted by c_h, as well as the costs of generating deception signals on both layers (c_1 and c_2). Therefore, if the defender chooses not to deceive the attacker ($a_1 = nv$), they incur a net cost equal to the sum of the costs for the deception signals without reaping the expected benefit, which represents an economic disadvantage.

On the other hand, when the defender is of the normal type ($\theta = N$), they suffer a loss c_c if the normal system is attacked. This loss is further increased by the costs of deception signals (c_1 and c_2). Thus, the defender has a strong incentive to prevent an attack on the normal system. However, if they manage to deter the attacker from acting ($a_1 = nv$), they receive a benefit b_{cs} that more than compensates for the costs of the deception signals. By avoiding the attack, the defender

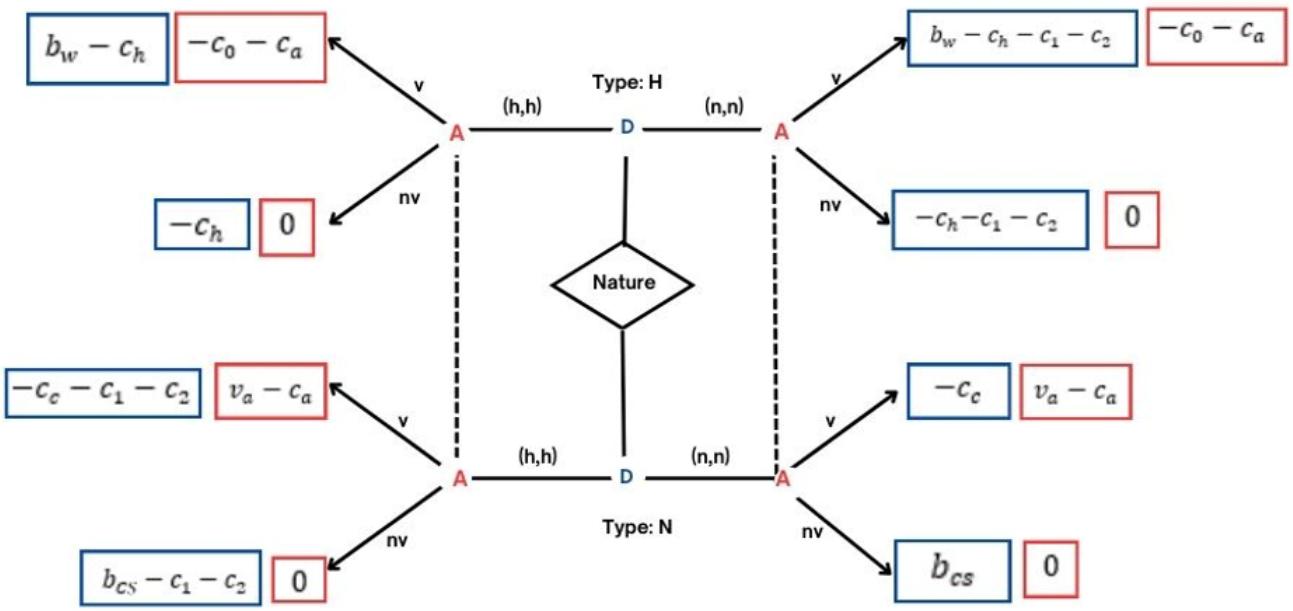


FIGURE 3. Extensive Form of the Two-Sender Signaling Game.This image illustrates the extensive form of the signaling game involving two distinct senders. Each sender represents a layer of the game, with its own possible strategies and payoffs. The extensive form representation allows visualizing all possible combinations of actions and responses between the two senders, as well as the associated gains or payoffs. This form of representation is useful for analyzing in detail the dynamics and strategic interactions of the two-layer signaling game.

protects the normal system and improves their financial situation, even after incurring the costs of implementing deception measures.

Remark IV.1. *The conflicting motivations between the defender and the attacker in this signaling game arise from their opposing objectives. The defender aims to deceive the attacker by concealing their true type, which can be achieved either through the deployment of decoys (such as honeypots) or by generating deceptive signals across two distinct layers. On the other hand, the attacker seeks to accurately discern the defender's true type in order to maximize their payoff, choosing either to attack a normal system or avoid falling into a trap.*

TABLE 1. Symbols and Their Meanings

Symbol	Meaning
θ	Defender's type (H for honeypot, N for normal)
p	attacker's belief about the defender's type ($p(0)$ for Honeypot, $p(1)$ for normal)
v	Attacker's action to continue the attack
nv	Attacker's action to stop the attack
b_w	Defender's benefit from observing the attacker in the honeypot
c_h	Defender's cost to implement the honeypot on both layers
b_{cs}	Defender's benefit from avoiding the attack on the normal system
c_c	Defender's loss when the normal system is compromised
c_1	Defender's cost to generate the deception signal on the first layer
c_2	Defender's cost to generate the deception signal on the second layer
c_a	Defender's cost to implement the attack
c_0	Attacker's cost of being in the honeypot
v_a	Attacker's benefit from compromising the normal system

V. PERFECT BAYESIAN NASH EQUILIBRIUM

We consider the Perfect Bayesian Nash Equilibrium (PBNE) [24] as the solution concept for our signaling game. This approach is relevant because the PBNE captures the asymmetry of information between the two players as well as the asynchronous optimizations of the decisions made by each. The PBNE also allows for the characterization of the players' Bayesian beliefs in our model. Each player forms beliefs based on prior distributions over the types of the other player, which are then updated based on the information observed during the game. This dynamic is a key element in understanding how players strategically adjust as new information becomes available.

For each action of the defender (m_1, m_2), the attacker aims to optimize their expected payoff given the belief $p^1(\cdot|(m_1, m_2))$. Therefore, we have:

$$a \in \arg\max_{a \in S_A} \sum_{\theta \in \Theta} p^1(\theta|(m_1, m_2)) J_A(m_1, m_2, \theta) \qquad (2)$$

Thus, the attacker's action is the result that follows from their pure strategy $a^* : S_D \to S_A$, i.e., $a = a^*(m_1, m_2)$.

For each type $\theta \in \Theta$ chosen by nature for the defender, the defender must send a message $(m_1, m_2) \in S_D$ that maximizes their utility by anticipating the attacker's action a^*. Let $(m_1^*, m_2^*) = (m_1, m_2)^*$. Therefore:

$$(m_1, m_2)^* \in \arg \max_{(m_1, m_2) \in S_D} J_D(a^*(m_1, m_2), (m_1, m_2), \theta) \qquad (3)$$

Thus, the defender's action is the result that follows from their pure strategy $(m_1, m_2)^* : \Theta \to S_D$. Note that their action for type θ is $(m_1, m_2) = (m_1, m_2)^*(\theta)$.

The strategies adopted by the defender can take three forms [25]:

1) **Two-sided Separating Equilibrium (TSE)**:
This is a bilateral equilibrium, meaning that both layers send different messages for the two types, or both layers adopt separating strategies. We have $m_i^*(H) \neq m_i^*(N)$ for all $i = 1, 2$ (both layers). In this case, the attacker can learn privileged information about S_i by observing the action of either layer (S_i). That is, the attacker can infer the type of S_i; more explicitly, the choice of the defender's action on S_i provides clues about their type.
2) **One-sided Separating Equilibrium (OSE)**:
This is a unilateral equilibrium, meaning that only one layer adopts the separating strategy. We have $m_i^*(H) \neq m_i^*(N)$ and $m_j^*(H) = m_j^*(N)$ with $i \neq j$. In this case, the attacker can learn privileged information only by observing the action of S_i.
3) **Pooling Equilibrium**:
This is the case where both layers adopt pooling strategies, meaning $m_i^*(H) = m_i^*(N)$ for all $i = 1, 2$ (both layers). In this case, the attacker cannot learn any privileged information by observing the defender's actions.

Our model relates specifically to the concepts of pooling and two-sided separation equilibrium. Indeed, the defender's actions are limited to either (n, n) or (h, h), in order to ensure a consistent deception strategy between the two layers. So the concept of one-sided separating will not enter our analysis.

We extend the concept of pure strategies to include mixed strategies. Define the mixed strategy $\sigma_A : S_D \to \Delta S_A$ for the attacker, and similarly, for the defender, we have $\sigma_D : \Theta \to \Delta S_D$.

When a defender's action (m_1, m_2), executed with a probability σ_D, is initiated, the attacker assigns a probability $\sigma_A(m_1, m_2, a)$ to their action a. This probability satisfies the following constraints:

$$\sum_{a \in S_A} \sigma_A(m_1, m_2, a) = 1, \quad \forall (m_1, m_2) \in S_D \tag{4}$$

and

$$\sigma_A(m_1, m_2, a) \geq 0, \quad \forall a \in S_A, \quad (m_1, m_2) \in S_D \tag{5}$$

The objective functions for the two players in mixed strategies are defined as follows:

$$\max_{\sigma_A(.)} \sum_{\theta \in \Theta} p^1(\theta | m_1, m_2) \sum_{a \in S_A} \sigma_A(m_1, m_2, a) J_A(m_1, m_2, \theta), \tag{6}$$

$\forall m = (m_1, m_2) \in S_D$.
For the defender:

$$\max_{\sigma_D(.)} \sum_{a \in S_A} \sigma_A(m_1, m_2, a) \sum_{m \in S_D} \sigma_D(m_1, m_2, \theta) J_D(m_1, m_2, \theta), \tag{7}$$

$\forall \theta \in \Theta$.

Since the action (m_1, m_2) of the defender is a function of the type θ, observing this action should reveal information about the type. Thus, the attacker updates the initial belief $p(\cdot)$ to form the posterior belief $p^1(\theta \mid m_1, m_2)$ using Bayes' rule.

The update of the attacker's beliefs, $p^1(\theta \mid m_1, m_2)$, is performed via Bayes' rule:

$$p^1(\theta \mid m_1, m_2) = \frac{p(\theta) \cdot \sigma_D(m_1, m_2 \mid \theta)}{\sum_{\theta' \in \Theta} p(\theta') \cdot \sigma_D(m_1, m_2 \mid \theta')}, \tag{8}$$

if $\sum_{\theta' \in \Theta} p(\theta') \cdot \sigma_D(m_1, m_2 \mid \theta') \geq 0$. Otherwise,

$$p^1(\theta \mid m_1, m_2) = \text{any probability distribution over } S_D, \tag{9}$$

if $\sum_{\theta' \in \Theta} p(\theta') \cdot \sigma_D(m_1, m_2 \mid \theta') \leq 0$.

The attacker and defender in pure strategy must also satisfy the Bayesian update of beliefs. Note that while the attacker can observe the message (m_1, m_2), which is a realization of σ_D, they cannot directly update their belief via (8) if the signaling game is played only once. However, (8) contributes to the Perfect Bayesian Nash Equilibrium (PBNE) of the signaling game, serving as a consistency constraint for beliefs.

Definition 1. *A Perfect Bayesian Nash Equilibrium in pure strategies of the signaling game is a pair of strategies* $(a^*; (m_1, m_2)^*)$ *and belief* p^1 *that satisfy* (2), (3), *and* (8). *A Perfect Bayesian Nash Equilibrium in mixed strategies of the signaling game is a pair of strategies* $(\sigma_A^*; \sigma_D^*)$ *and belief* p^1 *that satisfy* (6), (7), *and* (8).

VI. EQUILIBRIUM RESULTS

In this section, we determine the PBNE of our signaling game.

Lemma VI.1. *According to the assumptions described in Remark IV.1, the signaling game does not admit any perfect Bayesian Nash equilibrium (PBNE) in pure strategies.*

Proof. Given the conflicting objectives of the defender and the attacker, as described in Remark IV.1, Neither the Pooling Equilibrium nor the Two-sided Separating Equilibrium can exist stably in this model. In each case, the attacker's best response leads to a situation where the defender suffers significant losses, prompting them to change their strategy, which demonstrates the instability of these equilibrium concepts. This breakdown can be detailed through the following observations:

- **Pooling Equilibrium:** In a Pooling Equilibrium, the defender chooses the same action for both types ($\theta = H$ and $\theta = N$), preventing the attacker from distinguishing between these types by merely observing the defender's action. Suppose the defender adopts the action (h, h) for both types. If the attacker decides to attack ($a_1 = v$), the attacker's payoff will be $-c_0 - c_a$ for a honeypot system ($\theta = H$) and $v_a - c_a$ for a normal system ($\theta = N$). If the attacker chooses not to attack ($a_1 = nv$), their payoff is zero, regardless of the system type. Since

the attacker can still benefit from attacking a normal system, they are incentivized to choose to attack. This results in losses for the defender, amounting to $b_w - c_h$ for $\theta = H$ and $-c_c - c_1 - c_2$ for $\theta = N$. Therefore, faced with constant attacks, the defender would be inclined to change their strategy, showing that this Pooling Equilibrium is unstable. A similar reasoning applies if the defender chooses (n, n) for both types, but in this case, the attacker's incentive to attack is even stronger, leading to significant losses for the defender. These considerations indicate that the defender will not maintain such a strategy, thus proving the non-existence of a stable Pooling Equilibrium.

- **Two-sided Separating Equilibrium (TSE):** Regarding the Two-sided Separating Equilibrium, the defender would choose (h, h) for a honeypot system $(\theta = H)$ and (n, n) for a normal system $(\theta = N)$, allowing the attacker to perfectly distinguish the defender's type. In this scenario, the attacker would choose not to attack a honeypot ($a_1 = nv$), as this would result in a zero payoff, which is better than a potential loss from attacking. Conversely, the attacker would attack a normal system, as this would yield a net gain of $v_a - c_a$. However, this situation leads to significant losses for the defender: $-c_h$ in the case of a honeypot and $-c_c$ in the case of a normal system. Faced with these losses, the defender would be incentivized to deviate from this strategy, demonstrating that the Two-sided Separating Equilibrium is also not stable.

□

Switching to mixed strategies allows the defender to keep the attacker in a position of uncertainty, making it difficult for the attacker to choose an optimal strategy that works in all scenarios. By randomizing their actions, the defender complicates the attacker's ability to predict and exploit a specific strategy.

VII. ANALYSIS OF AUTOMOTIVE SYSTEM DEFENSE USING TWO-SENDERS SIGNALING

To evaluate the effectiveness of the two-sender signaling model in defending automotive systems, we conducted simulations using the parameters summarized in Table 2. The data used for the simulations in this study are identical to those employed in the one-layer deception model proposed by Pawlick et al. [21]. These data have been adjusted for our model by considering the assumptions defined in Section (IV-C).

In this scenario, the attacker cannot distinguish honeypots from normal systems. Simulation results show that the attacker's behavior and the defender's utility vary based on the proportion of normal systems in the network, represented by the belief $p(1)$ of the system being of the normal type. When $p(0) < 50\%$, the attacker is strongly discouraged from attacking. The probability of encountering a honeypot is high enough that the attacker prefers to withdraw from all systems,

TABLE 2. Parameters Used for Simulations

Parameter	Value	Description
b_w	25	Benefit for the defender from observing the attacker in the honeypot
c_h	15	Cost of implementing the honeypot across both layers
c_{h1}	9	Cost of implementing the honeypot on first layers
c_{h2}	7	Cost of implementing the honeypot on second layers
b_{cs}	8	Benefit for the defender from avoiding an attack on the normal system
c_c	10	Loss for the defender when the normal system is attacked
c_1	3	Cost for the defender to generate the deception signal on the first layer
c_2	5	Cost for the defender to generate the deception signal on the second layer
c_a	10	Cost for the defender to implement the attack
c_0	20	Cost of being in the two-layer honeypot
c_{01}	12	Cost of being in the second layer honeypot
c_{02}	15	Cost of being in the first layer honeypot
v_a	25	Benefit for the attacker from compromising the normal system

reducing their utility to zero. For the defender, this means their utility remains stable since no attacks occur. When the proportion of normal systems exceeds 50%, or $p(0) > 50\%$, the attacker is incentivized to attack all system components indiscriminately. The lack of differentiation in the signals received by the attacker drives them to attack, increasing their utility as the proportion of normal systems rises. Conversely, the defender experiences a decline in utility, as they shift from a scenario with no attacks to one where they are consistently targeted.

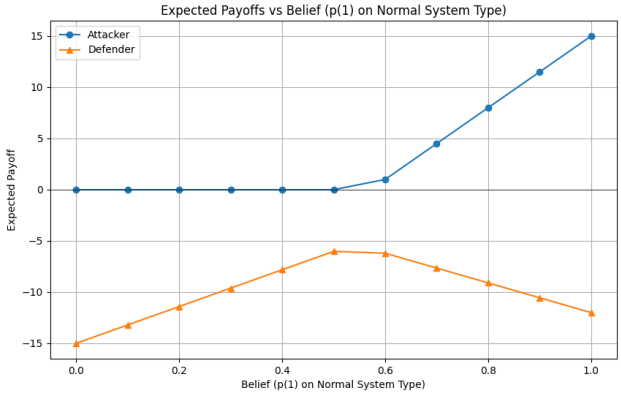


FIGURE 4. Impact of the belief $p(1)$ (representing the normal system type) on the expected utilities of the attacker and defender.

In the context where the attacker is unable to detect honeypots, the defender should aim for a proportion of normal systems close to 50% to maximize their utility. Any significant deviation from this proportion can result in substantial losses for the defender due to an increase in attacks.

VIII. DISCUSSION

When the defender's signalling cost $c_2 = 0$, the deception does not include layer 2 and the defender builds his deception only on layer 1. Similarly, when $c_1 = 0$ the deception is

based solely on layer 2. Fig. 5 illustrates the simplification of our single-layer deception model, where payoffs are structured in the same way as in the two-layer model. This single-layer structure is inspired by the [26] model of deception against DoS (denial of service) attacks.

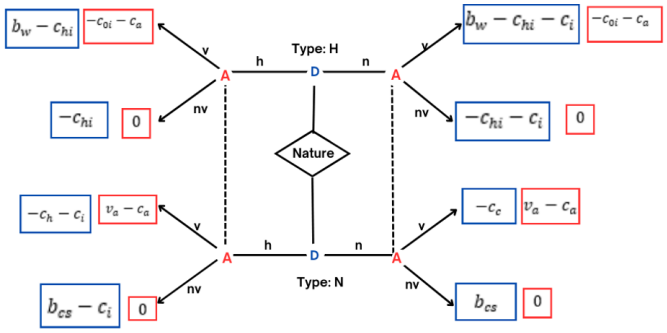


FIGURE 5. Simplification of the two-layer deception model to a single layer, where the payoffs are organized similarly to those in the two-layer structure. This figure demonstrates the reduction in complexity while maintaining the core strategic interactions.

In our simulations, adjustments were made to the honeypot component. We defined the implementation cost of the honeypot as being lower in the single-layer deception model than in the two-layer model ($c_{h1} < c_h$ and $c_{h2} < c_h$). We also assume that the attacker's losses in a single-layer deception are lower than in a two-layer deception. One of the reasons is that in the single-layer model, the attacker has only one signal to analyze, resulting in lower costs compared to the two-layer model, where the attacker faces additional costs associated with analyzing the second layer ($c_{01} < c_0$ and $c_{02} < c_0$).

A. ATTACKER BEHAVIOR

In a context where the attacker believes with a low probability (Fig.6) that they are interacting with a normal system, the two deception models (one-layer and two-layer) have a similar impact. Indeed, when the belief $p(1)$ is less than 40%, the optimal strategy for the attacker is to "**not attack (nv)**", as the risks associated with interacting with a honeypot are too high. In this scenario, adding a second layer of deception does not offer any significant advantage to the attacker, resulting in similar expected payoffs for both models. However, when the attacker develops a strong belief that they are interacting with a normal system $p(1) \geq 50\%$, the two-layer deception becomes the ideal approach. In this case, the increased complexity of the model significantly reduces the attacker's potential gains, which benefits the defender. By coordinating actions between the two layers, the attacker is more likely to be misled, thereby reducing their effectiveness and chances of success. This reduction in the attacker's gains provides a significant strategic advantage to the defender, who maximizes their chances of success by making the deception more credible and harder to evade.

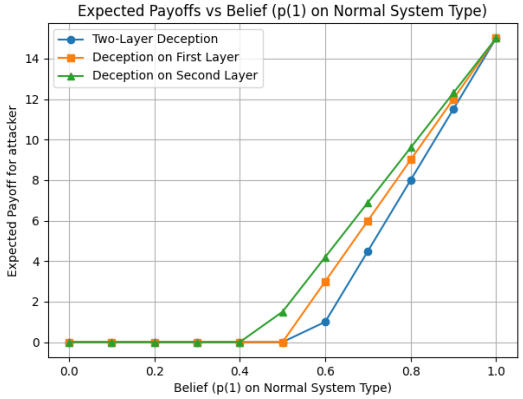


FIGURE 6. Expected Payoffs for the Attacker vs Belief $p(1)$ on Normal System Type.

B. DETERRENCE LEVEL

The effective deterrence $D_{\text{eff}}(p)$ is a combined measure that takes into account the attacker's expected payoff $A(p)$ and the probability of deterrence $f(p)$. This function evaluates the overall effectiveness of the deception implemented by the defender. The model is defined as follows:

$$D_{\text{eff}}(p) = A(p) \cdot f(p) \tag{10}$$

We model the probability of deterrence $f(p)$ using a sigmoid function, which describes how the probability that the attacker is deterred varies with their belief p about the system (normal or decoy). This sigmoid function is defined by:

$$f(p) = \frac{1}{1 + e^{-\lambda(p - p_0)}} \tag{11}$$

Here, $p - p_0$ represents a tipping point where the attacker is indifferent between attacking and not attacking. In other words, at $p = p_0$, the attacker is uncertain about the nature of the system and is equally likely to attack or not attack. Based on our experiments (Fig.6), for our deception model, we define $p_0 = 0.5$and for the other two deceptions (layer 1 and layer 2) are respectively 0.5 and 0.4. The parameter λ controls the steepness of the transition between deterrence and attack states. A high value of λ indicates a sharp transition between these states, while a low value signifies a more gradual transition. This modeling captures the effect of the belief level p on the attacker's decision. Fig. 7 shows the defender's payoffs for different deception strategies, such as one-layer honeypot and two-layer deception, based on the attacker's belief p. The performance of the "First-Layer Deception" and "Second-Layer Deception" strategies is similar when $p(1)$ exceeds 60%. In this scenario, when the attacker has a strong belief in the success of their attack, their best strategy is to **attack** (v)**,** resulting in a loss for the defender. In the case of single-layer deception, the defender's payoff is conditioned by Assumption 2. This is why the payoff associated with second-layer deception is slightly higher than that of first-layer deception. However, this difference remains minimal,

given the costs associated with implementing honeypots at each layer.

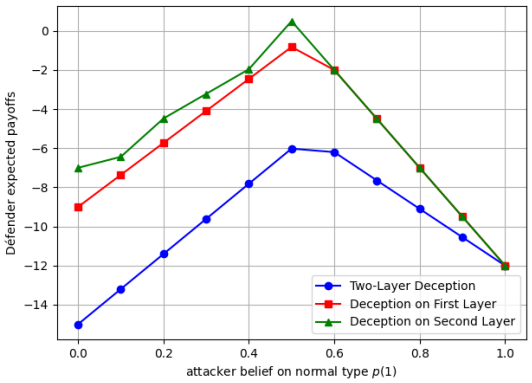


FIGURE 7. Defender's Payoffs as a Function of the Attacker's Belief p.

This figure compares the costs incurred by the defender based on the adopted deception strategy. A strategy with a higher cost, such as two-layer deception, may be justified as it significantly reduces the risk of attack by increasing the level of deterrence for the attacker.

Fig. 8 illustrates the effective deterrence $D_{\text{eff}}(p)$ for different deception strategies. It shows how the combination of the attacker's payoff and the probability of deterrence affects the overall effectiveness of the deception strategy:

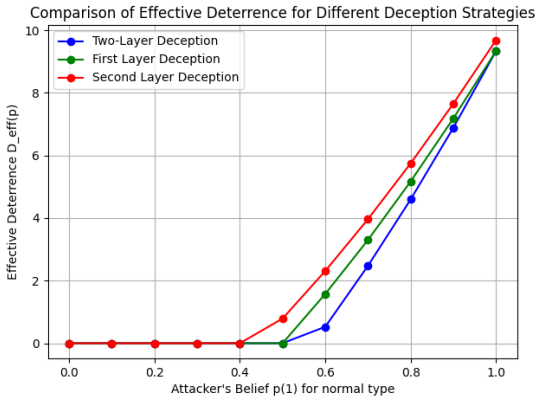


FIGURE 8. Effective Deterrence $D_{\text{eff}}(p)$ for Different Deception Strategies.

This figure highlights the effectiveness of various deception strategies. A higher curve for $D_{\text{eff}}(p)$ indicates better deterrence, which can justify the higher cost of more complex strategies like two-layer deception. the lower the attacker's gain, the less likely he is to attack the normal system.

C. COST-DETERRENCE TRADE-OFF

The trade-off between the cost of the honeypot and the level of deterrence can be measured by considering the ratio of the honeypot cost to the effectiveness of the deterrence obtained. This can be formalized as follows:

$$\text{Trade-off} = \frac{c_{\text{total}}}{D_{\text{eff}}(p)} \tag{12}$$

where $c_{\text{total}} = c_h + c_s$ represents the total cost associated with implementing the honeypot strategy. For the two-layer deception, c_s is defined as $c_1 + c_2$, representing the costs associated with the additional layers of deception. The effective deterrence $D_{\text{eff}}(p)$ is a function of the attacker's payoff, which varies with p and the probability of deterrence $f(p)$. A higher cost for the honeypot can be justified if it leads to a substantial reduction in attack risks. Fig. 9 illustrates the cost-deterrence trade-off for different deception strategies, showing how the total cost of implementing each strategy compares to the effective deterrence obtained.

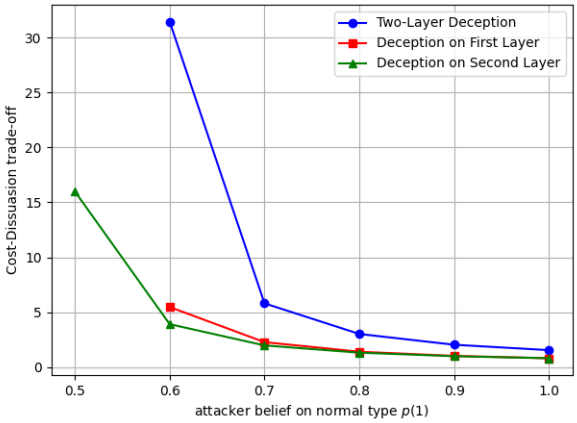


FIGURE 9. Trade-off between the Cost of the Honeypot and Effective Deterrence for Different Deception Strategies. We adapt the trade-off formula using the deception approach. For the one-layer deception approach we have the total cost equal to $c_{hi} + c_i$ and for the two-layer deception approach we have $c_h + c_1 + c_2$.

This figure shows the ratio between the total cost of each deception strategy (including the costs of implementing the honeypot and additional layers for two-layer deception) and the effective deterrence. The curves illustrate how the total cost varies with the effectiveness of deterrence for each approach. A strategy with a more favorable cost-deterrence trade-off is one that offers a better cost-deterrence ratio, thus justifying higher expenditures if they lead to a substantial reduction in attack risks. The results show that while two-layer deception strategies may incur higher costs, they can provide more effective deterrence, making these investments more justified in terms of reducing risks to the defense system.

Fig. 7, 8, and 9 demonstrate that more costly deception strategies, such as two-layer deception, can offer more effective deterrence. This cost-effectiveness trade-off is crucial in environments where security is a priority. Thus, although the implementation cost is higher, these strategies can be justified by their ability to effectively deter attackers, thereby reducing risks to the defense system.

D. MITIGATING CYBER-ATTACK RISKS THROUGH THE TWO-LAYER DECEPTION MODEL

The complexity of cyber-physical systems requires a comprehensive security approach [27], employing more robust defense strategies capable of deceiving and deflecting attacks before they impact physical operations. Our simulation results demonstrate that the two-layer deception model significantly mitigates the risks associated with cyber-attacks. This model enhances the defender's overall security posture by introducing an additional layer of complexity that the attacker must navigate. First, the coordination between the two layers allows for more sophisticated manipulation of the attacker's perceptions. When the attacker believes they are interacting with a normal system, their confidence often drives them to adopt aggressive strategies. However, the two-layer model complicates their decision-making process, increasing the likelihood of misjudgment. By presenting two distinct layers of information, the defender can effectively confuse the attacker, making it more difficult for them to discern the true nature of the system they are targeting. Moreover, the increased complexity of the two-layer deception model directly impacts the attacker's expected gains. As our results show, when the attacker's belief $p(1)$ exceeds 60%, their optimal strategy shifts toward attacking, leading to a loss for the defender. However, the additional layer of deception ensures that the attacker's potential gains are significantly reduced compared to single-layer strategies. This reduction in potential rewards serves as a deterrent, discouraging attackers from pursuing their plans. The two-layer deception model serves as a crucial mechanism for reducing cyber-attack risks by complicating the attacker's decision-making process and minimizing their potential gains. These results underscore the importance of adopting sophisticated deception strategies in modern cybersecurity frameworks.

IX. CONCLUSION

In this paper, we developed and analyzed a two-layer signaling game model applied to automotive system defense. This model captures the complex dynamics of interaction between a defender and an attacker in a cybersecurity context, particularly in the presence of asymmetric information. By employing the concept of Bayesian Perfect Nash Equilibrium, we formalized and examined the optimal strategies for both players.

The introduction of a two-sender (two-layer) signaling model in this context adds a new dimension to defense system modeling. This approach allows for the simulation and analysis of various concealment and detection scenarios, thereby enhancing resilience against sophisticated cyberattacks. Our results show that, within the framework of pure strategies, neither pooling nor bilateral separation provides a stable solution, highlighting the importance of mixed strategies. These strategies enable the defender to maintain a high level of deterrence by making it more challenging for the attacker to predict actions.

This study demonstrates that the use of two-sender signaling models is a promising approach for defending automotive systems against cyberattacks. Simulations reveal that finding a strategic balance in the proportion of normal systems is crucial for maximizing the defender's utility while effectively deterring attackers. Although two-layer deception strategies are costly, they offer superior protection by increasing the likelihood of deterrence, thus justifying their expense in contexts where security is paramount.

Furthermore, our analysis highlights an inherent trade-off between the level of deterrence the defender can achieve and the costs associated with different strategies. The results underscore the importance of designing adaptive and robust defenses to counter emerging threats, emphasizing the need to invest in advanced security strategies to ensure the integrity of automotive systems in the face of increasingly sophisticated attacks.

This work opens several avenues for future research, including the integration of machine learning mechanisms to dynamically adjust the defender's strategies, or the exploration of other types of signaling games in similar contexts. A more detailed analysis of the costs associated with different strategies could also help refine recommendations for designing even more robust defense systems.

In summary, our model demonstrates the potential of multi-layer signaling games to improve automotive system security against emerging threats, while emphasizing the need for adaptive approaches to counter evolving attacker strategies.

REFERENCES

[1] F. Cohen and D. Koike, "Misleading attackers with deception," in Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. IEEE, 2004, pp. 30–37.

[2] S. Murphy, T. McDonald, and R. Mills, "An application of deception in cyberspace: Operating system obfuscation1," in International Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2010, p. 241.

[3] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocessors and microsystems, vol. 77, p. 103201, 2020.

[4] M. Eling, M. Elvedi, and G. Falco, "The economic impact of extreme cyber risk scenarios," North American Actuarial Journal, vol. 27, no. 3, pp. 429–443, 2023.

[5] H. Razavi, M. R. Jamali, M. Emsaki, A. Ahmadi, and M. Hajiaghei-Keshteli, "Quantifying the financial impact of cyber security attacks on banks: A big data analytics approach," in 2023 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2023, pp. 533–538.

[6] T. J. Williams, "The purdue enterprise reference architecture," IFAC Proceedings Volumes, vol. 26, no. 2, pp. 559–564, 1993.

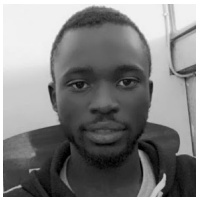
[7] S. Kim and K.-J. Park, "A survey on machine-learning based security design for cyber-physical systems," Applied Sciences, vol. 11, no. 12, p. 5458, 2021.

[8] N. Zhao, Y. Tian, H. Zhang, and E. Herrera-Viedma, "Fuzzy-based adaptive event-triggered control for nonlinear cyber-physical systems against deception attacks via a single parameter learning method," Information Sciences, vol. 657, p. 119948, 2024.

[9] M. Jamali, H. R. Baghaee, M. S. Sadabadi, G. B. Gharehpetian, and A. Anvari-Moghaddam, "Distributed cooperative event-triggered control of cyber-physical ac microgrids subject to denial-of-service attacks," IEEE Transactions on Smart Grid, vol. 14, no. 6, pp. 4467–4478, 2023.

[10] J. Pawlick, E. Colbert, and Q. Zhu, "Modeling and analysis of leaky deception using signaling games with evidence," IEEE Transactions on Information Forensics and Security, vol. 14, no. 7, pp. 1871–1886, 2018.

[11] L. Huang and Q. Zhu, "Dynamic bayesian games for adversarial and defensive cyber deception," Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings, pp. 75–97, 2019.
[12] M. A. Sayed, A. H. Anwar, C. Kiekintveld, and C. Kamhoua, "Honeypot allocation for cyber deception in dynamic tactical networks: A game theoretic approach," in International Conference on Decision and Game Theory for Security. Springer, 2023, pp. 195–214.
[13] M. Aghassi and D. Bertsimas, "Robust game theory," Mathematical programming, vol. 107, no. 1, pp. 231–273, 2006.
[14] G. Bonanno and K. Nehring, "Understanding common priors under incomplete information," in Proceedings of the 7th conference on Theoretical aspects of rationality and knowledge, 1998, pp. 147–160.
[15] J. Zhuang, V. M. Bier, and O. Alagoz, "Modeling secrecy and deception in a multiple-period attacker–defender signaling game," European Journal of Operational Research, vol. 203, no. 2, pp. 409–418, 2010.
[16] J. Pawlick, S. Farhang, and Q. Zhu, "Flip the cloud: Cyber-physical signaling games in the presence of advanced persistent threats," in Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings 6. Springer, 2015, pp. 289–308.
[17] C. Hu, J. Huang, Q. Wang, E. Weare, and G. Fu, "Truthful but misleading: Advanced linguistic strategies for lying among children," Frontiers in Psychology, vol. 11, p. 676, 2020.
[18] T. Zhang and Q. Zhu, "Hypothesis testing game for cyber deception," in Decision and Game Theory for Security: 9th International Conference, GameSec 2018, Seattle, WA, USA, October 29–31, 2018, Proceedings 9. Springer, 2018, pp. 540–555.
[19] P. Beltrán López, M. Gil Pérez, and P. Nespoli, "Cyber deception: State of the art, trends and open challenges," arXiv e-prints, pp. arXiv–2409, 2024.
[20] A. Hemida, A. B. Asghar, C. Kamhoua, and J. Kleinberg, "A game theoretic framework for multi domain cyber deception," in 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2024, pp. 443–447.
[21] J. Pawlick and Q. Zhu, "Deception by design: evidence-based signaling games for network defense," arXiv preprint arXiv:1503.05458, 2015.
[22] D. P. Möller, R. E. Haas, D. P. Möller, and R. E. Haas, "Mobile apps for the connected car," Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications, pp. 379–438, 2019.
[23] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1243–1274, 2018.
[24] D. Fudenberg and J. Tirole, "Perfect bayesian equilibrium and sequential equilibrium," journal of Economic Theory, vol. 53, no. 2, pp. 236–260, 1991.
[25] J.-Y. Kim, "Signal jamming in games with multiple senders," Contributions in Theoretical Economics, vol. 3, no. 1, 2003.
[26] H. Çeker, J. Zhuang, S. Upadhyaya, Q. D. La, and B.-H. Soong, "Deception-based game theoretical approach to mitigate dos attacks," in Decision and Game Theory for Security: 7th International Conference, GameSec 2016, New York, NY, USA, November 2-4, 2016, Proceedings 7. Springer, 2016, pp. 18–38.
[27] J. Fitzgerald and C. Morisset, "Can we develop holistic approaches to delivering cyber-physical systems security?" Research Directions: Cyber-Physical Systems, vol. 2, p. e2, 2024.



PRIVA KAMDEM CHASSEM received his Bachelor's of pure mathematics in 2017 and his Master's degree in 2020 at the University of Ngaoundéré (Cameroon). He is currently working toward a Ph.D. in cyber security at the University of Dschang, Cameroon. His research interests include game theory applied to Cybersecurity, defense measures against cyber and physical attacks in an automotive system, and cyber-deception mechanisms against cyber and physical attacks in an automotive system.

ALAIN B. ZEMKOHO is an Associate Professor at the School of Mathematical Sciences at the University of Southampton where he is affiliated to the Operational Research Group and CORMSIS. Before joining the University of Southampton, he was a Research Fellow at the University of Birmingham and had previously worked as a Research Associate at the Technical University of Freiberg. He is a Fellow of the Alan Turing Institute for Data Science and Artificial Intelligence, a Fellow of the Institute of Mathematics Its Applications, and a Fellow of the UK Higher Education Academy. His research interests are around the theory and methods for nonconvex, nonsmooth, and bilevel optimization, as well as their applications, including in machine learning, security games, healthcare, and medicine.

LAURENT NJILLA (MEMBER, IEEE) received the B.S. degree from the Department of Computer Science, University of Yaoundé, Yaoundé, Cameroon, the M.S. degree from the University of Central Florida, Orlando, FL, USA, and the Ph.D. degree from the Electrical and Computer Engineering Department, Florida International University, Miami, FL, USA. He is currently a Research Engineer with the Air Force Research Laboratory, Department of Defense, Rome, NY, USA. His current research interests include cyber security, game theory, hardware and network security, blockchain technology, cyber threat information, and advanced computer networking.

MARCELLIN NKENLIFACK is the Head of the Computer Science Department, Institute of Technology of the University of Dschang, Cameroon, and a Professor. He received an M.A. degree in Computer Science, followed by a Ph.D. in Computer Engineering and Control from the National Polytechnic Institute, University of Yaounde I. He had been a visiting researcher at Institut Scientifique et Polytechnique Galilee, Universite de Paris 13 (2001) and SUPELEC - Rennes, France (2003). He is the author of research papers on novel aspects of Software Engineering, Computer Applications in Industry and Engineering, Object-oriented Modeling and Simulation, Meta-modeling, Hybrid Control Systems, Distributed Control, computers in Education, E-learning, and E-governance. He designed and developed a "Simulation Environment for Hybrid Control Systems" and a "Software for the Management of Students and Academic Issues, at the Universities of Cameroon". He actually contributes to developing a "Platform for Modernization of computer science teaching methods in secondary schools" and a "Platform for Teaching of National Languages and Cultures through ICT in Cameroon".

CHARLES A. KAMHOUA Charles A. Kamhoua is a Senior Electronics Engineer at the Network Security Branch of DEVCOM Army Research Laboratory (ARL) in Adelphi, MD, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining the DEVCOM Army Research Laboratory in 2017, he was a researcher at the U.S. Air Force Research Laboratory (AFRL), Rome, New York for 6 years. He has held visiting research positions at the University of Oxford and Harvard University. He has co-authored more than 250 peer-reviewed journal and conference papers that include 6 best paper awards. He has been at the forefront of several new technologies, co-editing five books at Wiley-IEEE Press entitled "Automated Cyber Resilience", "Game Theory and Machine Learning for Cyber Security", "Modeling and Design of Secure Internet of Things", "Blockchain for Distributed System Security", and "Assured Cloud Computing". He has been recognized for his scholarship and leadership with numerous prestigious awards, including the 2023 US Army Civilian Service Commendation Medal, the 2022 US Department of Defense's Laboratory University Collaboration Initiative (LUCI) Fellowship, the 2021 IEEE-USA Harry Diamond Memorial Award, and the 2020 Sigma Xi Young Investigator Award. He received a B.S. in electronics from the University of Douala (ENSET), Cameroon, in 1999, an M.S. in Telecommunication and Networking from Florida International University (FIU) in 2008, and a Ph.D. in Electrical Engineering from FIU in 2011. He is currently a senior member of ACM and IEEE.