Bayesian Game for Cyber Deception Against Remote Attack on Automotive Systems

Priva Chassem Kamdem *Department of Mathematics & Computer Science*
University of Dschang
BP 96 Dschang, Cameroon
priva.chassem@univ-dschang.org Alain Zemkoho *School of Mathematical Sciences*
University of Southampton
SO17 1BJ Southampton, UK
a.b.zemkoho@soton.ac.uk Laurent Njilla *Information Assurance Branch*
Air Force Research Laboratory
Rome, NY, USA
laurent.njilla@us.af.mil Marcelin Nkenlifack *Department of Mathematics & Computer Science*
University of Dschang
BP 96 Dschang, Cameroon
marcellin.nkenlifack@gmail.com Charles Kamhoua *Network Security Branch*
DEVCOM Army Research Laboratory
delphi, MD, USA
charles.a.kamhoua.civ@army.mil

***Abstract*—Cyber deception is a highly recommended technique in cyber defense and is being used more and more by cyber security experts to provide a more optimal network security defense. We propose a deception model adapted to cyber attacks on automotive systems that will not only thwart cyber attacks but also deceive the attacker who initiates the attack so that he is convinced of the success of his attack. However, the proposed model will allow the deception defense to lure the attacker into providing an optimal response while assuming that the attacker has beliefs about the possible responses for a given attack and also has a priority on responses with a high level of impact. Our aim is to build optimal responses to the defender that will satisfy the attacker's beliefs. We model this problem using a two-player Bayesian game where the attacker has uncertainty about the nature of the responses proposed by the deception defense. For a given attack, we find the optimal strategies or responses for the deception defense using Bayesian Nash equilibrium and then implement an algorithm to generalize the model over a finite set of attacks. We show that from the results of the model, the attacker's expected payoff on his belief update is always greater than his expected payoff on his belief initial, which justifies the optimality of the response provided. We then present a numerical result that effectively validates our deception approach on remote attacks that are very prevalent in automotive systems.**

***Index Terms*—Remote attacks, Automotive system, Belief updates, Cyber deception.**

I. Introduction

The security of automotive systems is a fast-growing field, as vehicles become increasingly connected and automated. With the evolution of connectivity on automotive systems, the number of attack vectors is growing, giving attackers more opportunities to launch remote attacks as in the case of the 10 km remote takeover of a Jeep Cherokee in 2015 [1]. Security in the current context of connected vehicles uses solutions adapted to the components and communication protocols of the automotive system. It is grouped into four categories: security interface, security gateway, security network, and security processing, and includes several techniques such as cryptography, firewalls, and intrusion detection systems (IDS) [2]. However, it is important to note that cyber-deception defense techniques are increasingly recommended by cyber-security experts [3], [4]. Cyber deception defense techniques refer to a set of techniques that can be implemented on a given attacker. It generally consists of masking information, dazzling, hiding, decoying, false information, and camouflaging [4],[5]. Remote attacks are the most common and recurrent attacks on automotive networks [6]. In remote attack scenarios [6], the system receives traffic from the outside; this information is then analyzed by the defender via IDS to identify malicious traffic. When automotive systems fall victim to cyber-attacks, they produce observations or response reactions specific to the attacker's objective [7] [6]. However, any remote attack produces physical reactions as well as logical reactions via a reception interface such as the dashboard, the vehicle's website or the mobile application connected to the vehicle's system[8]. Remote attacks or attacks on the network layer of automotive systems are defended by intrusion detection systems (IDS).

Work [9] [10] [11] has shown that IDS is an essential and highly effective countermeasure against threats at the network layer. However, the defense measures offered by IDS are limited, even though they detect anomalies in the information exchanged between components, they could enable defenders to have a more in-depth defense. For example, the defender could detect abnormal traffic entering the system and lure the attacker into believing the attack was successful by sending

false reactions or responses via its reception interface. Game theory provides a formal approach that helps us effectively model cyber-deception scenarios[12].

However, cyber-deception security games [13] provide mathematical tools that can allow us to assess the uncertainty of an attacker facing a response that he perceives on a given attack. Providing false information is not sufficiently studied in the literature in the context of cyber deception for automotive network security. To address these uncertainty issues, we propose a mathematical model defined on a Bayesian game that evaluates an attacker's uncertainty by proposing strategies to maximize the attacker's beliefs on the perceived responses so that he is convinced of the attack's success.

In this paper, a security game is modeled based on the detection of malicious traffic, which then requires a response from the defender to convince the attacker of the success of the attack. We introduce a Bayesian game that models the attacker-defender interaction and the attacker's uncertainty about the nature of the perceived responses.

Our security game is the modeling of a response attack scenario that takes into account an attack on the automotive network and sends a feedback or response to the attacker on its reception interface. Our aim is to build optimal responses to the defender that will satisfy the attacker's beliefs. Motivated by the nature of the response, the defender chooses the best strategy to convince the attacker.

Implementing this game requires the defender to take into account all the possible observations or reactions that an automotive system presents during an attack.

To our knowledge, this paper is one of the first to introduce the notion of cyber deception in automotive cyber security. The contributions of this paper are :

- We propose a security model for automotive systems that generalizes all cyber-attacks or remote attacks. Our model takes into account all threats and attacks on the automotive network layer detected via an IDS that was previously used to detect anomalies in information traffic.
- We formulate a new two-player game model: a Bayesian game for cyber deception against remote attacks on automotive systems, which consists of studying the uncertainty of the attacker in front of the answers which it perceives of the deception defense.
- We present a complete algorithm that generalizes the resolution of the game model on a finite set of attacks by giving the mechanism for obtaining the strategies (responses) at the Bayesian Nash equilibrium.
- Finally, we present numerical results for the analysis of remote attacks based on our approach which shows the effectiveness of the strategies or responses obtained in the Bayesian Nash equilibrium.

The rest of the paper is organized as follows: In Section 2, we present the model system by defining the game model and the proposed algorithm for remote attacks. The numerical results are presented in Section 3 and we conclude our work by giving future directions in Section 5.

II. System Models

We are proposing a security game that describes the interaction between a cyber attack (controlled by a malicious person) and the automotive system (defender), which aims to thwart the cyber attack.

A. Problem Description

An attacker is trying to launch a cyber attack to damage the vehicle or achieve his malicious goal. This attack is a remote attack that targets the cyber layer of the automotive system, the attacker's objective is to damage the vehicle's components electronics control units (ECU) which are mainly physical (brakes, speed, doors, etc.) for the most part but also cyber (private information, calls, sms, entertainment, etc.). The attacker's strategy is to infiltrate the vehicle's network and transmit malicious packets that will propagate to reach different targets depending on their objectives. However, each cyber attack on the vehicle creates reactions or observations that materialize the impact of the attack. We assume that the attacker perceives the reactions following his attack to have a confirmation of the success of the attack, since we are interested in the remote we also assume that the attacker perceives the responses or reactions of the system via a reception interface like the web page of the vehicle, the web application of the vehicle or the dashboard of the vehicle which are all controlled by the attacker. To deal with this threat, the defender combines two solutions:

- An IDS is implemented in the vehicle's network to monitor incoming traffic as well as traffic between vehicle system components. The role of IDS is to filter malicious information by identifying the sources and destinations of the various interrupted packets. These packets are then analyzed to identify the nature of the attack.
- When an attack is identified and then blocked, the defender simulates false information to transmit to the attacker's reception interface to convince him of the success of his attack.

This scenario is repeated for all attacks identified on the automotive network. For each threat, the defender must provide a false response to convince the attacker.

When an attack is identified and responded to, we assume that deception is achieved when this attack is no longer identified by the system for a certain period of time. The main purpose of this cyber deception is to have more information in order to improve the detection system.

B. Model

When IDS intercepts malicious traffic, from the information collected and analyzed on this traffic it can estimate the nature of the attack and communicate this to the defender's deception module, as shown in Fig.1. The role of the defender's deception module is to provide false reactions or responses to the various interfaces of the external components that communicate with the vehicle's network, its objective being to lure the attacker into believing that the attack in question has succeeded. In order to carry out this work effectively,

we have conducted a study of the possible responses that can be proposed by the defender's deception module. Without losing any generalities, we have restricted ourselves to 10 cyber-attacks TableIII that are among the most common cyber-attacks on automotive networks [14]. At the end of our study, we counted a total of 40 possible responses TableII for these cyber-attacks, TableV gives us the generalization of each cyber-attack with its response vector, on the rows we have the attacks, and on the columns, we have the responses.

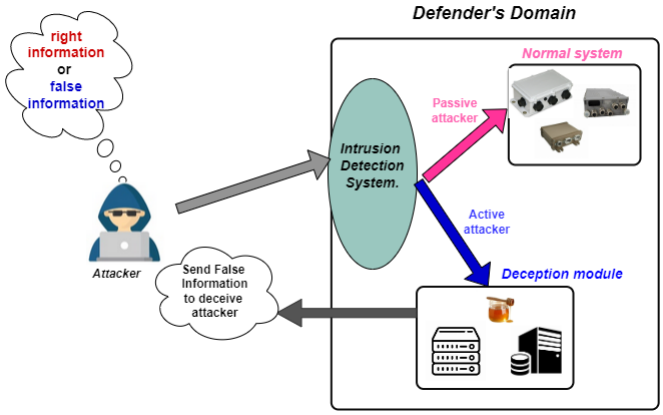

Fig. 1. The attack-defense model with a disappointment-defense reaction.

We assume that the attacker has knowledge that allows him to be uncertain about the nature of the responses proposed by the defender's deception module. For an attack given in table V, we have a response vector that gives responses of three types: type (*) which means that this response must absolutely be present in the response vector, type (+) which means that the response must be present with a certain probability and finally type () where the cell is empty, in this case, the response must not be present in the response vector. The objective of the deception defense module for a given attack is to construct an optimal response vector which will be made up of all the absolute responses (*) and/or the probabilistic responses (+). To do this, the defender must choose the probabilistic responses that will be able to provide an optimal response in order to lure the attacker. This problem can be modeled with a two-player Bayesian game where the attacker emits uncertainties about the nature of the response vectors proposed by the defender's deception module. The Bayesian approach will allow us to treat the problem in a more complete probabilistic framework. Our Bayesian model is represented by the tuple:

$$\Gamma = (G, A_1, A_2, U_1, U_2)$$

Where :

- $G = (A, R)$ Represents our database tableV with A a set of known attacks and R a set of possible responses to these attacks.
- $A_1 = A$ and A_2 the set of possible actions of the attacker and defender respectively, $A_1 \times A_2$ the possible set of action profiles.
- $U_1 : A_1 \times A_2 \to R$ The attacker's payoff function
- $U_2 : A_1 \times A_2 \to R$ The defender's payoff function

This set is the same for each cyber-attack in tableIII chosen by the attacker.

C. Model Description

We give more details in this section to better understand our proposed model.

1) Actions: The attacker chooses an action (attack) $a_i \in A_1 = A$ from a finite set of attacks that we defined in tableV. The defender observes the attacker's action a_i and then chooses his action $R_i^j \subseteq R_i \subset R$ or R_i is made up of the defender's possible responses to the attack a_i.
The vector R_i is made up of the absolute responses and the probabilistic responses of the attack a_i. For attack a_i the defender has $\left|2^{|\widetilde{R_i}|}\right|$ vectors of possible responses with $\widetilde{R_i}$ the set of probabilistic responses for attack a_i we, therefore, have $R_i^j \in R_i' \cup 2^{|\widetilde{R_i}|}$ with R_i' the set of absolute actions as illustrated in Figure2. Finally, we can pose $A_2^i = R_i' \cup 2^{|\widetilde{R_t}|}$ and $A_2 = \prod_{i \in A_1} A_2^i$ as the set of actions of the defender for the set of attacks A_1.

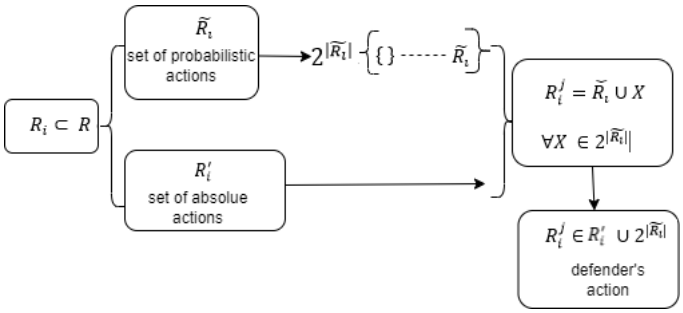

Fig. 2. Diagram of the defender's actions for a given attack.

2) Beliefs Formulation: For an action a_i by the attacker, the defender has a set of responses $R_i \subset R$ which are perceived as the reactions of the system to the attack. Since the attacker has uncertainty about the nature of the defender's response, it will have to form a belief about the probabilistic responses $\widetilde{R_i}$ with $\widetilde{R_i} \subset R_i$. Let $b_1^0 : \widetilde{R_i} \mapsto \Delta\widetilde{R_i}$ denote the attacker's belief about probabilistic actions satisfying the following conditions $b_1^0(o_k) \geq 0, \quad \sum_{o_k \in \widetilde{R_i}} b_1^0(o_k) = 1$.
For an attack a_i, from the attacker's beliefs about each probabilistic action we can compute an attacker's belief about each type of response R_i^j with $R_i^j \in A_2^i$.
For an attack a_i let us denote $b_2^0 : A_2^i \mapsto \Delta A_2^i$ the attacker's belief about the response types satisfying the following conditions $b_2^0\left(R_i^j\right) \geq 0, \quad \sum_{R_i^j \in A_2^i} b_2^0\left(R_i^j\right) = 1$. We assume that the responses are considered independent events so we have the following:

$$b_2^0\left(R_i^j\right) = \prod_{o_k \in \widetilde{R_i}} \left(b_1^0(o_k) * 1_{\{o_k \in R_i^j\}}\right) * \prod_{o_k \notin \widetilde{R_i}} \left(\left(1 - b_1^0(o_k)\right) * 1_{\{o_k \notin R_i^j\}}\right) \quad (1)$$

3) Payoffs: For any attack $a_i \in A_1$, each response provided by the defender aims to convince the attacker that the attack was successful. However, we assume that the attacker has a

preference for probabilistic responses that can cause a strong impact on the system. In the context of this work, a response is linked to an observation made on a component or module, and we assess the level of impact by the critical level of this module or component. We carried out a study on the critical state of the components or modules of the automotive system, from this study we proposed TableIV which gives an evaluation on a scale from 0 to 4 on the critical level of the components then we assign a weight to each response according to the critical level related to the component. $o_k \in \widetilde{R_i}$ Let us note $G(o_k)$ the impact of the response o_k on the system. The impact on each type of response is defined as follows:

$$G\left(R_i^j\right) = \sum_{o_i \in \widetilde{R_i}} G\left(o_i\right) * 1_{\left\{o_i \in R_i^j\right\}}, \tag{2}$$

We denote $U_D\left(a_i, R_i^j\right)$ and $U_A\left(a_i\right)$ the defender's losses and the attacker's payoffs respectively.

$$U_A\left(a_i\right) = \sum_{R_i^j \in R_i} b_2^0\left(R_i^j\right) * G\left(R_i^j\right) - C_A\left(a_i\right) \tag{3}$$

Where $C_A\left(a_i\right)$ represents the cost to the attacker of launching the attack a_i.

$$U_D\left(a_i, R_i^j\right) = b_2^0\left(R_i^j\right) * G\left(R_i^j\right) + C_D\left(R_i^j\right) \tag{4}$$

Where $C_D\left(R_i^j\right) = \sum_{o_i \in \widetilde{R_i}} C\left(o_i\right) * 1_{\left\{o_i \in R_i^j\right\}}$ represents the cost to the defender of implementing the response R_i^j. We assume that all responses have the same implementation cost because the defender simulates a packet for all responses to send as a response to the attacker.

D. Solution Description

The attacker has knowledge that allows him to have uncertainties about the nature of the response sent by the defender. However, the defender defines the losses of his actions from the attacker's beliefs about each response and the weights. However, the defender defines the losses of its actions based on the attacker's beliefs about each response and the weights assigned to these different responses, which allows the defender to be closer to its objective. So for a given attack $a_i \in A_1$, the resolution of the game consists of the defender maximizing his losses in order to estimate the action that will convince the attacker. Fig3 shows the architecture of our response model.

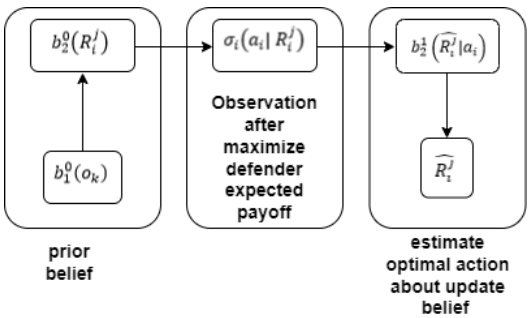

Fig. 3. Optimal response scheme for our model.

1) Defender's Problem : The defender's pure strategies are defined according to each type of response $R_i^j \in A_2^i$ chosen with knowledge about the attacker's actions, The defender seeks to maximize the impacts according to its utility to be very close to its objectives i.e.

$$\max_{R_i^j \in A_2^i} U_D\left(a_i, R_i^j\right) \tag{5}$$

We can extend the defender's pure strategies into mixed strategies $\sigma_i : A_2^i \mapsto \Delta A_2^i$. After observing the attacker's action a_i, the defender assigns a probability $\sigma_i\left(a_i, R_i^j\right)$ to his action R_i^j with feasibility constraints $\sum_{R_i^j \in A_2^i} \sigma_i\left(a_i, R_i^j\right) = 1$ avec $\sigma_i\left(a_i, R_i^j\right) \geq 0$, $\forall a_i \in A_1$.

The objective function expected of the defender under the mixed strategies is defined as follows:

$$\begin{aligned} &\max_{\sigma_i(.)} \sum_{R_i^j \in A_2^i} \sigma_i\left(a_i, R_i^j\right) * U_D\left(a_i, R_i^j\right), \\ &\qquad \forall a_i \in A_1 \text{ and } \forall R_i^j \in A_2^i \end{aligned} \tag{6}$$

2) Attacker's Analysis: For each attack a_i, the attacker should perceive a response R_i^j that maximises its expected payoffs under its belief $b_2^1(.|a_i)$ with anticipation on the defender's action $a_i = \widehat{a}_i\left(R_i'\right)$. The attacker's expected payoffs are given as follows:

$$\overline{U_A}\left(a_i\right) = \sum_{R_i^j \in A_2^i} \sigma_i\left(R_i^j \mid a_i\right) * b_2^1\left(R_i^j\right) * G\left(R_i^j\right) - C_A\left(a_i\right) \tag{7}$$

3) Belief Consistency: We seek to update the attacker's initial beliefs about the different types of response in order to have the most optimal beliefs for an observed attack. By applying Bayes rules, we calculate the probabilities of each type of response taking into account the observed attack. This approach will allow us to optimize the attacker's beliefs about the best response for an observed attack. Attacker updates its initial beliefs $b_2^0(.)$ To a posteriori beliefs $b_2^1\left(. \mid a_i\right)$ via the Bayes rule.

$$\begin{aligned} b_2^1\left(R_i^j \mid a_i\right) &= \frac{b_2^0\left(R_i^j\right) * \sigma_i\left(a_i \mid R_i^j\right)}{\sum_{R_i^j \in A_2^i} b_2^0\left(R_i^j\right) * \sigma_i\left(a_i \mid R_i^j\right)}, \\ &\text{if } \sum_{R_i^j \in A_2^i} b_2^0\left(R_i^j\right) * \sigma_i\left(a_i \mid R_i^j\right) > 0 \\ b_2^1\left(R_i^j \mid a_i\right) &= \text{ any probability distribution,} \\ &\text{if } \sum_{R_i^j \in A_2^i} b_2^0\left(R_i^j\right) * \sigma_i\left(a_i \mid R_i^j\right) = 0 \end{aligned} \tag{8}$$

We apply this procedure to Algorithm 1 to obtain the optimal response strategies for the given attacks.

Algorithm 1 Deception defense

Input: $G(A_1, R)$ Input Knowledge Base (Table V)
Output: $\widehat{a_j}$
  for $a_i \in A_1$ **do**
    for $r \in \widehat{R_i}$ **do**
      $b_1^0(r) \leftarrow \frac{1}{|\widehat{R_i}|}$
    end for
    Define A_2^i defender's action for attack $a_i(section\text{II-C1})$
    for $a_j \in A_2^i$ **do**
      $b_2^0(a_j) \leftarrow$calculate prior belief of action $a_j(eq1)$
      $b_2^1(a_j|a_i) \leftarrow$compute update belief of action $a_j(eq8)$
    end for
  end for

The attacker has an initial belief about the possible probabilistic responses to a given attack. When the attacker initiates an attack, the a priori beliefs about the probabilistic actions related to this attack may or may not be equiprobable depending on the attacker's knowledge. If we assume that the a priori beliefs about the probabilistic responses follow a uniform distribution, for an attack $a_i \in A_1$ we have :

$$\sum_{r \in \widetilde{R_i}} b_1^0(r) = 1 \text{ with } b_1^0(r) = \frac{1}{\left|\widetilde{R_i}\right|}, \forall r \in \widetilde{R_i}$$

The attacker makes an observation on each response vector (II-C1) or prioritizes responses with a high impact, taking into account the attacker's initial beliefs about the different responses (II-D1).
The attacker updates his beliefs about the different response vectors by analyzing observations on the possible response vectors, which may reveal the optimal response vector. For each response vector, the attacker updates his beliefs after one observation using the Bayes rule.
The attacker can then use Maximum a posteriori (MAP) to find the most likely final response for an attack:
for $a_i \in A_1$, we define MAP as

$$\widehat{a_j} \in \text{argmax}_{a_j \in A_2^i} \, b_2^1 \left(a_j \mid a_i\right)$$

(II-D3) details updates beliefs.

III. Numerical Results

In this section, we present the numerical results that validate our proposed model. Within the framework of these experiments, we considered 8 cyberattacks, which are listed in tableIII. With regard to the responses proposed in tableII, which are linked to the automotive components, we have defined in tableIV the weights assigned to each module or component according to its critical level (impact level). Based on the proposed model, we have assessed the level of relevance of the responses to the 08 cyberattacks. As illustrated in Fig4, we can see a significant improvement in the attacker's beliefs between his initial beliefs (prior belief) and his updated beliefs (posterior belief), which are assessed on the basis of the attacker's expected payoffs. Fig4 we can deduce that the responses provided by the deception module are optimal because, based on the attacker's beliefs, they satisfy the attacker's expectations.

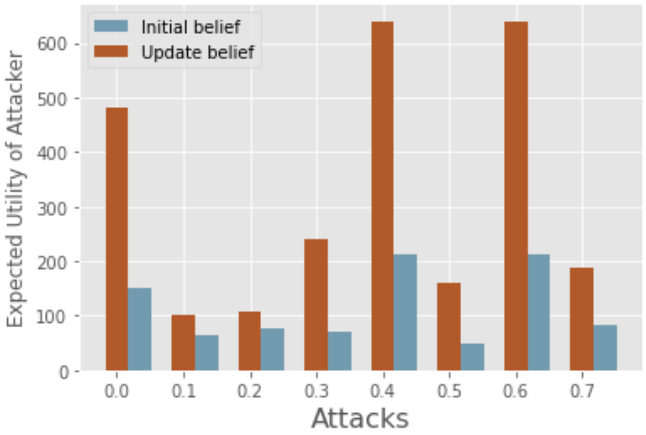

Fig. 4. Analysis of proposed responses to cyber-attacks on automotive systems

As mentioned above, very little research has been proposed in the field of honeypots for automotive systems. In the table I we make a comparative analysis of the few honeypot techniques.

TABLE I
COMPARATIVE STUDY OF HONEYPOT APPROACHES ON AUTOMOTIVE SYSTEMS.

	Our Approach	[15]	[16]
IDS	yes	no	yes
Low-Interaction Honeypot	low	low	low
Objectives	misleading	Data Gathering	Data Gathering
Number of Honeypots	one	one	many
High-Interaction Honeypot	no	no	no

IV. Conclusion and Future Works

This work is a possible transition between the tasks carried out by the IDS and the vehicle system, in order to take a more in-depth look at network defense. With security problems in the automotive industry becoming more acute by the day, the concepts of cyber-security solutions proposed are numerous, but the one studied in this work is deception defense. This article is one of the first to introduce the notion of deception defense against cyberattacks in automotive networks. We are interested in a technique based on deception that aims to disappoint an attacker when he launches a cyberattack on an automotive network. Our model is based on a Bayesian game, which is different from traditional security games based on Bayesian games because in our scenario the uncertainty is fixed on the actions, contrary to the existing approach where the uncertainty is fixed on the type of players. Despite the concept of uncertainty in the actions, which is a new concept in security games in this paper, we managed to adapt the concept of solution of Bayesian games to prove that we can obtain optimal responses from the attacker's beliefs update. This work is still evolving and could open up many new possibilities in the field of deception defense in automotive networks. The game model proposed is very effective but does not include the repeated aspect of the game, which is a very important aspect in cyber defense systems. Therefore, we would like to

TABLE II
THE VARIOUS COMPONENTS OF THE AUTOMOTIVE SYSTEM WITH POSSIBLE ANSWERS

Components	N0:	Comment	Components	N0:	Comment
GPS	1	Navigation: location, time, and date	Chassir Sensor	18	Speed (manipulation)
	2	Map data for route planning modified to suit the new destination		19	Acceleration (manipulation)
	3	Relevant alerts or notifications linked to the vehicle's GPS position, such as geofencing alerts if the vehicle enters or exits certain areas (tunnels, bridges, etc.) in relation to the speed and new destination.		20	Notification of Airbag (collision)
	4	The direction in which the vehicle is moving : Step-by-step instructions for turn-by-turn navigation on the new route based on the vehicle's speed		21	Notification of suspension: notification of any impact or shock detected by this sensor.
	5	Calculation of arrival time at the new destination		22	Braking (applying the brakes)
	6	Traffic or diversions notifications	Audio	23	The name of the station currently playing
	7	Historical data such as the route taken by the vehicle in the past.		24	Volume level reduction
Doors	8	State of doors (open/closed)	Engine	25	Diagnostic status, error code
	9	Notification if a door is open for a long period or unexpectedly		26	Real-time engine speed (RPM) parameter
	10	Time of last closing or opening		27	Coolant temperature
Headlights	11	Brightness level		28	Fuel consumption level
	12	Notification Headlights on or off		29	Battery voltage
Steering Control	13	Indicating the steering angle		30	Alert from the Engine Control system
Temperature	14	Setting and adjusting the temperature		31	Indicator alert or notification
	15	Interior temperature: current temperature inside the vehicle	Brake Control	32	Status alerts or notification of ABS (worn brake pads, low brake fluid level)
Air conditioning	16	Air conditioning on/off		33	Maintenance status notifications
	17	Set and adjust fan speed			
Active Safety	34	Lane departure warning	Wiper	38	Windscreen wiper status (on or off)
	35	Collision warning		39	Operating mode (intermittent, continuous, variable speed)
	36	Status of automated emergency braking		40	Wiper speed
	37	Adaptive cruise control status			

improve this work by taking into account the repeated aspects of the game. In future work we will take into account the repeated and dynamic aspects of the game, where interactions between attacker and defender occur several times.

ACKNOWLEDGMENT

The research was sponsored by the 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.

REFERENCES

[1] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, pp. 1–91, 2015.

TABLE III
LIST OF CYBER-ATTACKS STUDIED IN OUR WORK.

N0:	Attacks
1	Brake activation (to create an accident)
2	Door Control (Lock or Unlock)
3	Operating the headlights (Lighting operation)
4	Change GPS data (Send new GPS data)
5	Handling Windscreen wipers (Checking or blocking the vehicle's windscreen wiper when on the move and when it is raining)
6	Controlling the steering wheel (To force the driver to turn or stop)
7	Handling the air conditioning
8	Controlling the radio volume
9	Switching off the engine
10	Remote start (Start a remote boot)

TABLE IV
AUTOMOTIVE COMPONENTS AND THEIR CRITICAL LEVELS.

Criticality level	Component	Fixed weight
Level 0	Non-critical components: Interior trim or display functions.	[0,10]
Level 1	Components with a minor impact on safety, such as audio components or rear-view mirrors.	[10,20]
Level 2	Components with a greater impact on safety : · Power steering,· Suspension system	[30,40]
Level 3	Safety-critical components · Airbags, seatbelts or anti-theft system. · Stability control systems. · Braking system. · Air conditioning/heating system. · Electrical and electronic system (battery, alternator, wiring harness, etc.). · Navigation or GPS system	[50,60]
Level 4	Safety-critical components, without which the vehicle cannot function. · The engine. · Transmission system and gearbox	[70,80]

TABLE V
SUMMARY STUDIES OF CYBER-ATTACKS AND POSSIBLE RESPONSES.

Responses to the Attack		A 1	2	3	4	5	6	7	8	9	10
GPS	1	*					+			*	+
	2				*						
	3				*						
	4				*		+				
	5				+						
	6				+						
	7				+						
Doors	8		*								*
	9		+								
	10		+								
Head-lights	11			+							
	12	*		*		+					
Stee-ring	13				*		*				
Tempe-rature Con-trol	14							*			
	15							*			+
Air condit-ioning	16							*			
	17							*			
Chassir Sensor	18	*			*	+					
	19	*				+					
	20	+		+		+	+			+	
	21	+				+				+	
	22	*				+				+	
Audio	23								+		
	24								*		
Engine	25									*	*
	26									*	
	27									*	
	28									+	
	29									*	*
	30									+	
	31									+	
Brake Control	32	*									
	33	+									
Active Safety	34						*				
	35					+				+	
	36	+									
	37	+				+	+			+	
Wiper	38					*					
	39					*					
	40					*					

[2] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020.

[3] S. Jajodia, V. Subrahmanian, V. Swarup, and C. Wang, "Cyber deception," *Cham, Switzerland: Springer*, 2016.

[4] L. Zhang and V. L. Thing, "Three decades of deception techniques in active cyber defense-retrospect and outlook," *Computers & Security*, vol. 106, p. 102288, 2021.

[5] C. Wang and Z. Lu, "Cyber deception: Overview and the road ahead," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 80–85, 2018.

[6] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, p. 94, 2014.

[7] S. E. Shladover, C. A. Desoer, J. K. Hedrick, M. Tomizuka, J. Walrand, W.-B. Zhang, D. H. McMahon, H. Peng, S. Sheikholeslam, and N. McKeown, "Automated vehicle control developments in the path program," *IEEE Transactions on vehicular technology*, vol. 40, no. 1, pp. 114–130, 1991.

[8] K. Mohammed, M. Abdelhafid, K. Kamal, N. Ismail, and A. Ilias, "Intelligent driver monitoring system: An internet of things-based system for tracking and identifying the driving behavior," *Computer Standards & Interfaces*, vol. 84, p. 103704, 2023.

[9] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.

[10] D. Kuipers and M. Fabro, "Control systems cyber security: Defense in depth strategies," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2006.

[11] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in *2015 6th international conference on modeling, simulation, and applied optimization (ICMSAO)*. IEEE, 2015, pp. 1–6.

[12] K. Ferguson-Walter, S. Fugate, J. Mauger, and M. Major, "Game theory for adaptive defensive cyber deception," in *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, 2019, pp. 1–8.

[13] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. A. Kamhoua, and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2460–2493, 2021.

[14] S. Malik and W. Sun, "Analysis and simulation of cyber attacks against connected and autonomous vehicles," in *2020 International Conference on Connected and Autonomous Driving (MetroCAD)*. IEEE, 2020, pp. 62–70.

[15] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, "An approach to using honeypots in in-vehicle networks," in *2008 IEEE 68th vehicular technology conference*. IEEE, 2008, pp. 1–5.

[16] E. Eriksson and L. Fahlbeck, "Investigating the use of honeypots in vehicles," 2022.