A SIMPLIFIED APPROACH FOR DYNAMIC SECURITY RISK MANAGEMENT IN CONNECTED AND AUTONOMOUS VEHICLES

Anhtuan Le*, Carsten Maple

Warwick Manufacturing Group, University of Warwick, Coventry, UK

Keywords: DYNAMIC RISK ASSESSMENT, DYNAMIC RISK MANAGEMENT, CONNECTED AND AUTONOMOUS VEHICLE

Abstract

Connected and autonomous vehicles (CAVs) have the potential to offer safer and more efficient transportation. However, such vehicles operate in complex heterogeneous environments and it is therefore essential to control the dynamic risks that the CAVs face during operation. Given that CAVs can be seriously impacted by cyber-attacks, their security issues have been investigated widely. However, existing approaches fail to adequately consider the dynamicity of the risks that arise and present methods to capture the changes in risks and adaptive mitigations. To bridge these gaps, this paper proposes a systematic approach, which comprises of three modules: a knowledge-based system to support the identification of the critical threats, a monitoring module to detect the changes in security context of the CAV and its surrounding environments, and a simplified assessment module to capture the dynamic risks and adjust the mitigations as needed. We investigate a case study of CAV platooning to evaluate our proposal.

1. Introduction

Internet of Things (IoT)-enabled CAVs can deliver better and new services to society. However, recent safety incidents from Tesla or Uber have raised the suspicion of whether this technology can safely and effectively replace conventional vehicles in the near future [1]. To gain public acceptance, CAVs require significantly more rigorous testing, verification, and especially risk control.

A CAV can be considered as a cyber-physical system which includes driving software supported by many embedded sensors (such as GPS, radar, LIDAR, ultrasonic) to sense the driving environments combined with actuators. Its awareness can also be extended by communicating with other entities, such as transportation infrastructure (V2I) and surrounding vehicles (V2V), to provide a shared understanding. It is known that cyberattacks can manipulate the CAV's sensors, software, and its external communications, to cause harmful effects. As such, cybersecurity risk assessments for CAV systems are becoming increasingly important.

Many works have addressed CAV risk assessment issues by considering vulnerabilities in the cyber physical technologies that CAVs employ. They also present different security objectives such as safety, privacy, financial or operational that require satisfying. Since CAVs operate in evolving heterogeneous environments, the security risks that they face are also dynamic. For example, a CAV can enter a new place where attackers with different goals and capabilities may launch some previously unknown attacks. Moreover, CAVs' functionalities can also be affected by environment conditions, which cause changes to the capabilities of the security system. Therefore, security assessment of CAVs should also be dynamic to capture these changes. However, challenges arise due to the complexity arising from the disparate fields of development [2], and the lack of support of the current methods for context awareness.

In this work, we develop a simplified approach to address the dynamic nature of cyber security risk in CAV systems, which focuses on identifying the most critical attacks that require monitoring and controlling as the environment changes. Contextual security information is communicated between the CAV and infrastructure to reflect the security situations during mobility. Our approach also gives flexibility for security assessment and adjustable mitigations as needed.

Our main contributions are:

- We propose a simplified approach to identify the most critical threats faced by CAVs' through monitoring the security context of both the CAVs and the environments they operate in. The contexts are analysed with the help of a knowledge-based system that extracts the most critical threats on which to focus.
- We propose a method to manage the dynamic risks, which include a lightweight strategy to reduce the need for risk reassessment. We also specify the need for reconsidering the mitigations when there are new risks or new road conditions that affect the CAV functionalities.
- We present a case study to compare dynamic and static risk assessment approaches.

This paper is structured as follows. Section 2 provides the background and presents a review of related work in CAV cyber security risk assessment. Section 3 discusses the requirements for an efficient dynamic risk assessment

approach, before Section 4 presents the proposed solution. In Section 5 we present and examine a case study for dynamic risk assessment in CAV systems, namely in platooning. Section 6 concludes the paper and discusses the future work.

2. Background and Related Work

Two of the most well-known CAV security assessment guidelines are the SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [3] and the ENISA Cybersecurity and Resilience of Smart Cars [4]. SAE J3061 suggests a framework which relies on three risk assessment methods, including EVITA [5], TVRA [6], and HEAVEN [7], with similar processes to the Road Vehicle Functional Safety ISO 26262 [8]. In contrast, the ENISA method describes the possible threats and vulnerabilities of assets based on the typical architecture of smart vehicles.

The common risk assessment approaches try to list all the potential threats and assess their risks through the estimation of likelihood and impact. To prevent the possibility of overlooking potential attacks, many works apply systematic threat modelling techniques to the CAV system assets, which includes all the CAV components and communications [9-11]. The method often used by these works is STRIDE [12], a threat modelling method proposed by Microsoft. There are also efforts to extend the STRIDE model to capture more threats, for example, the work in [13] added the *Linkability* and *Confusion* category to the STRIDE methodology. Each threat's likelihood will be assessed through considering the attackers' capabilities and motivations, which assume that if an attack is easy to launch and attackers have motivations to launch it then its likelihood will be high, and vice versa. On the other hand, the impact of an attack is categorised into four aspects, including safety, privacy, financial and operational. For each aspect, different impact levels are defined. The final risks of each threat will be derived from reference tables, which will give risk level given the likelihood and impact inputs.

Systematically listing all the threats that apply to CAV assets can result in a large number of threats that can be difficult to assess and control. To reduce these complexities, the EVITA approach [5] has been employed to link the threats, threat agents, and goals through the use of attack trees. Overall, the majority of works in the literature try to address the large attack surfaces arising from different CAV technologies, but there is no efficient method to quickly address the critical threats (i.e. threats with high likelihood and high impact) when applying in specific systems, especially in dynamic security contexts.

Intelligent Transportation System (ITS) can be employed to monitor, record, and analyse security information of any transportation environment. Selected information can be exchanged to and between CAVs to extend their cyber security awareness of the environment that they are operating in. The coordination between ITS and CAVs will clearly support the ability to perform dynamic risk assessment, however, no method has been proposed to develop such assessments. We believe we are among the first to discuss a framework for the coordination between the CAVs and ITS for security analysis through risk profiles [14]. It should be noted that ITS can also be utilised to provide information for analysing privacy risks, as shown in [15].

In the next section, we will present some essential requirements for a dynamic risk management approach to bridge the aforementioned gaps.

3. Requirements of CAV Dynamic Risk Assessment

The essential capabilities of an efficient dynamic risk management approach for CAV are to:

- **Address high-risk (critical) threats effectively:** the ultimate aim of risk assessment after knowing all the possible options is to identify the high-risk threats (i.e. attacks with high likelihood and high impact). An efficient method to address these critical threats is needed to save security resource and to increase the reaction speed of the CAV, especially to handle dynamic risks.
- **Capture the changes of risks when the CAVs move to new environments:** the approach should establish the point in time when reassessments are required, and specify how to react to the dynamic nature of risks.
- **Allow the coordination with the transportation infrastructure** (that is, the ITS) to extend the CAVs' cyber security awareness.
- **Manage and control dynamic risks** at different levels and from different aspects [14].

In the next section, we will propose our approach to address these requirements.

4. Proposed Solution

We assume that the roads are clustered into different transportation environments and for each environment, there will be a corresponding infrastructure to manage the information regarding its security context. This information can be referred to as the *security profile* [14], which ideally should include the potential threats, their frequency and potential impact. Additionally, the infrastructure can maintain maps with pre-annotated information concerning road conditions, which can be used to examine the influence on typical CAV functionalities (e.g. reflective objects that may affect the radar or LIDAR functioning). The infrastructure can communicate this information through information exchange services such as the Basic Safety Messages (BSM) described in [16].

Our solution consists of the three modules as illustrated in Figure 1. Briefly, module A supports the CAVs to analyse the security context, module B monitors the changes to check whether to launch the risk management process, which is the responsibility of module C.

Details of the modules are presented as follows.

4.1. Module A: Knowledge-based System

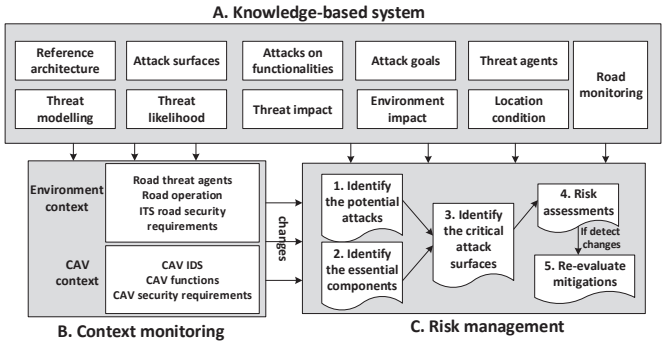

Figure 1. The proposed dynamic risk assessment model for CAV

The knowledge-based system should comprise of the following essential parts regarding the security knowledge:

- **A reference architecture for CAV operation:** As most of the cyberattacks target the functionalities of a system (e.g. to create disruption or system abuse), the security assessment should start from understanding the system's intended functionalities and how they can be attacked. Ideally for this purpose, security analysts will need to be provided with a system architecture, which is "the descriptive representation of the system's component functions and the communication flows between these components" [17]. This architecture needs to cover all the CAV's essential components and functionalities to support the functional analysis of any specific CAV system. As such a full reference architecture can provide the context of where the CAV system sits within the Internet of Vehicles system of systems. While there exist different reference architectures for CAVs [5, 10, 18, 19], they either failed to consider some critical functions of the system or the scope is too broad or too detailed, leading to difficulties in application. We have therefore developed a new reference architecture that focuses specifically on the areas that allow effective security analyses. As CAV technologies are still being developed, this reference architecture will need to be maintained.
- **A comprehensive attack surface analysis of the reference architecture:** information of security threats (likelihood and impact of testing, and a record of real attacks) are collected and grouped according to the components, functions, and communications in the reference architecture. For example, reported cyber physical attacks regarding the sensors (camera, LIDAR, radar, etc.) are recorded and annotated at the relevant components. The aim of maintaining the attack surface knowledge is to support effective cross-referencing of any relevant vulnerabilities for all components.
- **Typical attack goals and sub-goals:** the exploitation of attack surfaces is linked to the typical attack goals, which are represented through the attack tree. Attack trees allow to trace back the motivations behind the attack and to check the conditions whether the attackers can achieve their goals.
- **Threat agent analysis**: this includes a list of potential threat agents, their goals and capabilities. This information can be obtained from the literature but needs to be reviewed periodically to ensure it is up-to-date. The threat agent analysis allows an understanding of the motivations, methods and capabilities of the attackers when exploiting the attack surfaces.

Note that the knowledge-based system also collects information regarding the relationships between the parts (see Figure 2), represented through the attack trees [5]. For example, a threat agent will have typical attack goals, which are aimed to disrupt specific CAV functionalities (sub-goals). The likelihood of achieving a sub-goal can be retrieved from the attack surface information that lists the vulnerabilities of the corresponding components. On the other hand, when an attack is detected, the system will be able to determine the likely relevant goals and further techniques that are required to reach these goals. This information can suggest the threat agents behind this attack. Checking the profiles of these threat agents (i.e. goals and capabilities), the system can predict other high likelihood attacks that have not yet occurred (i.e. similar attacks caused by the same agent).

The knowledge-based system can support and shape the focus of security analysis from different levels such as components, functionalities, threat agents, or stakeholders. For example, to analyse a system with specific components and functions, the knowledge-based system can suggest a reduced list of threats to focus, instead of the large number of threats derived from traditional threat modelling. Given this reduced list, analysis of the intersections between the stakeholders' interest and attackers' goals will help to further identify the most critical threats among the others.

The knowledge-based system is also responsible for monitoring and communicating the real time security context of environment to CAVs that are in transportation. Typical information includes recent threats or incidents reported by monitoring system or other CAVs; potential threat impacts; and environment or location conditions that may create impact to CAV functionalities. This information will be useful to suggest mitigation update to adapt with security incident that happens.

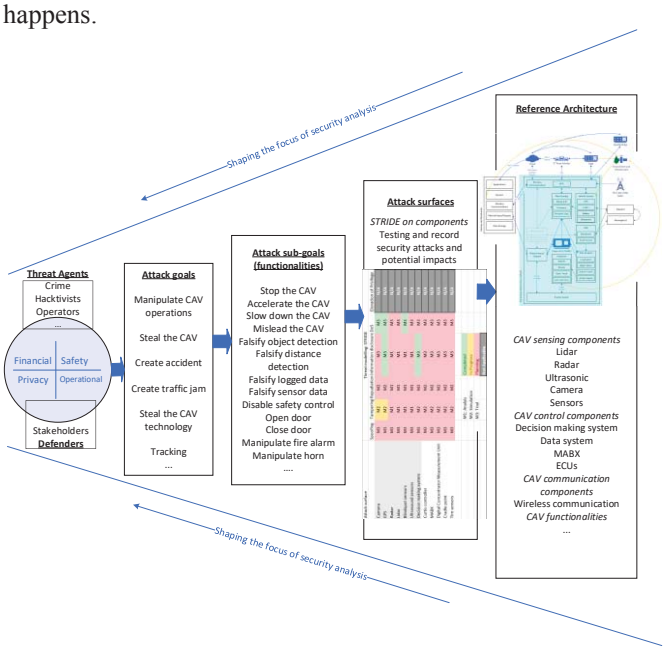

Figure 2. The knowledge-based system of security risk assessment

4.2. Module B: Context Monitoring

Before operation, the initial security risks and corresponding mitigation plan of the CAV will be obtained from the security requirements (i.e. the combination of stakeholders' security interest such as essential functions) and knowledge of potential threat agents. When the CAV is in operation, module B is responsible for monitoring the contextual information from the infrastructure and the state of the CAV. When receiving information from new environments, it will compare with the previous contexts to detect changes that need to be forwarded to module C to process. Potential changes include: changes in threats (either be informed by infrastructure or be detected by the CAV itself through its intrusion detection system), changes in requirements (from infrastructure or from CAV stakeholders), or changes in internal functionalities (such as road conditions that affect the CAV functionalities informed by the infrastructure; or changes in the driving algorithms). When detecting these changes, module B will pass the corresponding information to module C for reassessment. On the other hand, if the new information does not imply any changes, it is not necessary to invoke module C.

4.3. Module C: Risk Management

This module comprises of five steps to manage risk inputs from module B as can be seen in Figure 1. Note that Step 1 and 2 are independent so they can be conducted in any order, and in parallel.

Step 1: Identify the potential attacks. Given the security context provided by the infrastructure, module C can derive the potential attacks with the support of module A. In case there is no information about the threat agents, for example if there is no reported attack in the environment, our system suggests that the attack likelihood can be considered to be very small, hence, the risks can also be considered low. Note that this suggestion only reflects security knowledge at assessed time and it does not mean that the system is free from risks. Our design gives stakeholders flexibility to monitor other attacks that they concern (such as attacks which have high impact upon stakeholders' knowledge) by adjusting their security requirements (see module B). However, too much monitoring can deplete security resources and impact on the reaction speed of the system. Moreover, in case of incidents, the system can still quickly update the context and communicate around the area to reduce the impacts.

Step 2: Identify the CAVs' essential components. The essential components are specified based on an understanding of the CAV operations. Note that the selection of essential components is dependent not only on the physical architecture, but also on the software. Two CAVs with the same physical design can still have different essential components due to the differences in the driving algorithms. For example, both CAVs are equipped with the same sensors but one CAV may rely on the GPS when driving, while the other CAV may depend on the predictions of trajectory and a local map. In such cases, the components that are in use will be essential. Stakeholders can also select their own components for monitoring if these are essential for them.

Step 3: Identify the critical attack surfaces to monitor. This step combines the results of the first two steps to select critical threats. In particular, only attack from Step 1 that target the essential functions identified in Step 2 will be considered. Other attacks which target the non-essential components (low impact attacks), or other components with no potential attacks (low likelihood attacks) are considered low risk, so they can be skipped for simplicity.

Step 4: Conduct risk assessment on the critical attack surfaces. It is difficult to identify threat agents, however, as their activities and behaviours (e.g. launched successful attack) are recorded by ITS, it is possible to justify their capabilities. In [5], attacker capabilities are assessed through five fundamental factors, including elapsed time, attacker expertise, knowledge of system, windows of opportunities, and equipment. To launch a specific attack successfully, attackers need to bypass the system withstand (defender capabilities), which are also represented by the same factors [10]. As a result, the successful attacks can suggest the potential of the attackers without the needs of knowing their types.

The following part will describe our method to justify the attacker capabilities. Assume that for a specific area, the system records a list of n successful threats $T = \{t_i, i = \overline{1,n}\}$ launched by m unknown attackers $A = \{a_j, j = \overline{1,m}\}$. For each threat t_i in T, the ITS knows the corresponding defender capability vector $DC_i = [DC_i^{et}\ DC_i^{ex}\ DC_i^{k}\ DC_i^{w}\ DC_i^{eq}]$ which represents the system withstand regarding elapsed time, expertise, knowledge, windows of opportunities, and equipment respectively. Similarly, assume that each attacker j will have capability vector of $AC_j = [AC_j^{et}\ AC_j^{ex}\ AC_j^{k}\ AC_j^{w}\ AC_j^{eq}]$. In the worst case scenarios, attackers can collaborate to improve their potential. As a result, instead of identifying capabilities for all attackers, we only need to estimate the maximum capabilities of all attackers in the group, which can be represented by GA: $GA = [GA^{et}\ GA^{ex}\ GA^{k}\ GA^{w}\ GA^{eq}]$ in which $GA^{f} = \max_{f\in\{et,ex,k,w,eq\};j=\overline{1,m}}\{AC_j^{f}\}$. To launch T_i successfully, the attackers should be able to bypass the system withstand for T_i, which means their group attack capability GA should be greater than defender capabilities DC_i: $GA^{et} \geq DC_i^{et}, GA^{ex} \geq DC_i^{ex}, GA^{k} \geq DC_i^{k}, GA^{w} \geq DC_i^{w}, GA^{eq} \geq DC_i^{eq}$. For simplicity, we will assume that the capability of attacker at the time of launching T_i successfully equal to the system withstand. We consider attacker capability a dynamic risk element which is assessed by attack records. Consequently, this element can be updated if more sophisticated attacks are being detected during operations. Therefore, given n successfully launched threats, the maximum attacker capability can be estimated as $GA = \max_{i=1,n}\{DC_i\} = [DC_{max}^{et}\ DC_{max}^{ex}\ DC_{max}^{k}\ DC_{max}^{w}\ DC_{max}^{eq}]$ in which $DC_{max}^{f} = \max_{f\in\{et,ex,k,w,eq\};i=\overline{1,n}}\{DC_i^{f}\}$. Information regarding attacker capabilities in each area are maintained by the corresponding ITS. For risk assessment, this information will be provided to every CAV in transportation.

A common strategy to monitor dynamic risks is to reassess whenever there are changes in risk inputs. When the CAV is moving, reassessment may be needed frequently, which can compromise security resources. To prevent that, the CAV can pre-define thresholds which indicate the level of risks that it can tolerate. When coming to a new area, it will only reassess the risks if attacker capability in this area pass the pre-defined thresholds. Similarly, if attacker capability in the new area is less than that of the previous area while the CAV was confident of controlling the risks in the previous area, reassessing risks will be not necessary because risk level is not increased.

Step 5: Re-evaluate the mitigations. New mitigations should be considered to add in case there are new risks. Moreover, when the new environments inform the road conditions that may affect certain CAV functionalities, the mitigations that are related to these functions also need to be revised.

In the next section, we will present a case study that employs our approach to manage the dynamic security risks.

5. Case Study

The scenario in this case study is built based on the use case presented in [20]. We also obtained relevant knowledge of CAV functionalities, attacks and potential impacts from this reference.

5.1. Scenario Description

We consider a CAV that moves in a platoon, which is operated under Cooperative Adaptive Cruise Control (CACC). A typical CACC includes GPS, radar sensors, and Dedicated Short Range Communication (DSRC) devices to communicate with other CAVs in the platoon [20]. The platoon operations are illustrated in Figure 3. In particular, the radar sensors are used to measure the distance between the subject vehicle and its preceding vehicle; the GPS provides the location of other adjacent vehicles; while the DSRC devices are utilised for communication with nearby vehicles [20]. The platoon is moving on a road as represented in Figure 4. The goal is to manage the dynamic security risks when the subject CAV (the red vehicle in the platoon in Figure 4) moves in the road.

Figure 3. The operation of CCAV in platooning [20]

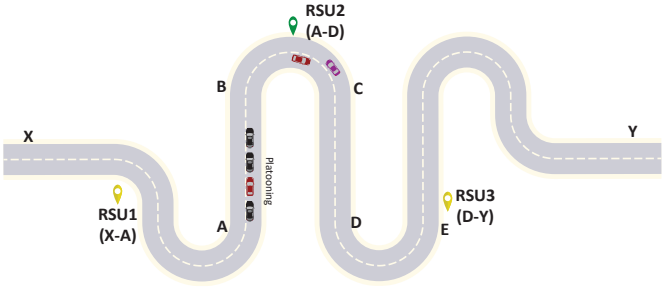

Figure 4. A platooning scenario for dynamic risk assessment

The road XY can be divided into three areas: (XA), (ABCD), and (DEY). Assume that each area has a Road Side Unit (RSU) to communicate its security context to the subject CAV. Essential security information for communicating includes a list of attacks that need to be considered (i.e. attacks with high likelihood according to history record or attacks with high impact if happen in the area) and road conditions that may affect the CAV functionalities. The RSU will need to update the context information by constantly collecting and analysing real time reports from different entities such as CAVs operating in the area or monitoring sensors along the road. The BSM [16] can be extended to store and deliver the security context information to all the CAVs that are in transportation. In this example we may have that the security contexts of the three areas are: (XA) No particular cyber threat to be concerned (e.g. the area has no record of cyberattacks or incidents); (ABCD) There is concern of spoofing attacks on LIDAR (e.g. these attacks have happened recently); (DEY) There is concern of spoofing attacks on ultrasonic sensors (e.g. these attacks were recorded with high frequency).

5.2. Static Versus Dynamic Risk Assessment

Static risk assessment approaches give no clear guidelines of which attack surfaces to focus. Furthermore, the threat agents are unknown and therefore, it is not clear how to identify their capabilities to estimate the risks. Any initial risk assessment of the CAV will remain constant during the time it moves on the road since there are no guidelines of when and how to update the assessment.

We now apply our approach for dynamic risk assessment. We will use knowledge regarding the attack trees to predict the relevant attacks and system withstands to estimate attacker capabilities. An example of the attack tree can be shown in Figure 5, while the system withstands for attacks in this tree are shown in Table 1. Assume that the CAV is only interested in safety (module B). It is obvious that the essential components to focus on are radar and GPS (Step 2 in module C).

In (XA), as there is no attack of concern and the system suggests that the risk up to the assessed time can be considered to be very low.

In (ABCD), given the spoofing attacks on LIDAR, the knowledge-based system suggests that attackers aim to spoof nearby objects, which is part of a larger aim of slowing down the CAV (e.g. see the attack tree in Figure 5). On the other hand, LIDAR spoofing is the only attack that is recorded, therefore we assume that attacker capabilities equal to system withstand for this attack, which is [1 3 0 0 4] as can be seen in Table 1. We will need to look for attacks which are not only have the same aim, but also can be launched with the assumed capabilities. From Figure 5 and Table 1, we can obtain camera spoofing, tampering, and DoS (attacks 7, 8, 9 in Table 1); LIDAR jamming attack (attack 6); and GPS jamming (attack 13). Given the vehicle specification, only attack 13 targets one of its critical components, which is GPS. While there are other critical attacks such as radar spoofing, tampering, and jamming (attack 1, 2, 3) and GPS spoofing (attack 12); these

attacks require higher attacker capabilities, therefore will be less feasible. Note that this does not mean the CAV is risk-free from those attacks, however, once any of them are launched, it can be detected and reported to ITS to update the attacker capabilities for future analysis. On the other hand, the spoofing attack on LIDAR and other attacks on camera will not be considered because it targets non-critical components in current operation.

Similarly, in (DEY), we found that the threat agent in (DEY) also aims to spoof the nearby object, or ultimately to slow down the vehicle, however attacks on the ultrasonic sensors require much higher capability of attackers, in which the capability vector is [10 6 7 0 7]. With such a high capability, the threat agents can be able to launch a number of attacks such as radar spoofing and jamming (attack 1,3), camera spoofing, tampering, and DoS (attack 7, 8, 9), and GPS jamming and spoofing (attack 12, 13). However, only attacks which target critical components (i.e. GPS and radar) will be added to the critical attack list.

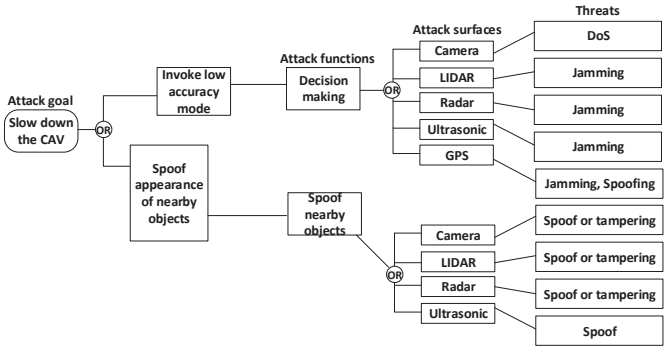

Figure 5. Example of an attack tree regarding the physical sensors

Table 1. Assessing system withstands for cyber-physical attacks on CAV – scales follow the scales in [5], assessments are based on [21-24]. ET = elapsed time; EX = expertise; K = knowledge; W = windows of opportunities; EQ = equipment.

ID	Threat name	System withstand				
		ET	EX	K	W	EQ
1	*Spoofing radar*	10	6	7	0	7
2	*Tampering radar*	17	6	7	0	7
3	*Jamming radar*	10	6	7	0	7
4	*Spoofing LIDAR*	1	3	0	0	4
5	*Tampering LIDAR*	10	3	7	0	7
6	*Jamming LIDAR*	1	3	0	0	4
7	*Spoofing Camera*	0	0	0	1	0
8	*Tampering Camera*	0	0	0	1	0
9	*DoS Camera*	0	0	0	1	0
10	*Spoofing ultrasonic*	10	6	7	0	7
11	*Jamming ultrasonic*	10	3	3	0	4
12	*Spoofing GPS*	4	3	3	0	4
13	*Jamming GPS*	1	3	0	0	1

Table 2. Dynamic risk assessment for CAV platooning

Road	Risk Assessment
(XA)	Very low security risk
(ABCD)	*GPS jamming*: High risk (high likelihood and high safety impact according to [20])
(DEY)	*GPS jamming and spoofing*: high risk *Radar jamming and spoofing*: high risk

The dynamic risk assessment results are summarised in Table 2 above.

5.3. Mitigation Strategy Consideration

Assume that the two best mitigations when the jamming attacks are launched are: *m1* - switch to the trajectory prediction to predict and update the GPS location while continuing to run as normal, and *m2* - slow down and stop the car. We will evaluate the three following mitigation strategies: the first two utilise static mitigations and the last one utilises the dynamic mitigations approach.

- Strategy S1–non-stop: uses *m1* during the trip
- Strategy S2–stop: uses *m2* during the trip
- Strategy S3–dynamic: use either *m1* or *m2* depending on the awareness of the security risks and road conditions

The risk assessments when implementing these three strategies are shown in Figure 6 below.

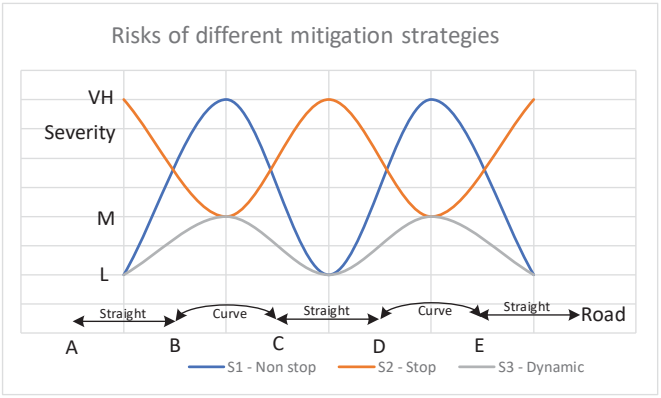

Figure 6. Comparisons of static and dynamic mitigation strategies when attacks are launched

The explanations are as follows.

For S1–non-stop, when the platoon runs in the straight lanes from A to B or from C to D, the errors of the trajectory prediction is small due to simple trajectory (a straight line). If a GPS jamming attack is detected, the CAV will switch to the local positioning therefore the likelihood and risk of crash is low. However, when the platoon runs in the curved lanes such as the road from B to C or from D to E, errors can become more critical, raising the risk of accident when the vehicle goes out of lane and hits a vehicle from the opposite lane. Therefore, the risk of a crash in these parts are high.

For S2–stop, when the platoon runs in the curved lanes such as the road from B to C or D to E, the platoon tends to slow down in the curve, therefore the risk of being crashed into by the rear

vehicle can be considered medium. However, when a jamming attack occurs in straight lanes such as the road from A to B or C to D, according to [20], there is a high chance of a crash caused by the rear vehicle because the reactions of the brake are not fast enough. Therefore, the crash risks in these cases are high.

For S3–dynamic, at first, the CAV applies *m1* in the straight lane AB. Before getting to B, the CAV will be informed of the curve lane ahead by RSU-2. Given that it is aware of the unreliability of the trajectory predictions when in curved lanes, and that it has knowledge that the jamming attack risk is high, the system will re-evaluate the mitigation strategy. The result is that *m2* is the best mitigation to choose, therefore it can switch to *m2*. Similarly, when moving to another straight lane CD, the changes of road conditions will invoke the mitigation re-evaluation so the CAV can always select the mitigation with minimal risk.

5.4. Discussions

In this section we discuss in what extent our approach is feasible with the requirements stated in Section 3.

Addressing the critical threats: the case study shows that our approach can quickly spot high-risk threats, which are having high likelihood and targeting the essential components. However, our approach relies on a knowledge-based system, which is subjective and requires maintenance to update with relevant knowledge. We have also employed a simplified approach to predict relevant attacks based on assumptions of the threat agent goals and capability. The precision of the attack predictions can be improved through more sophisticated methods (e.g. see [25]), but will also require more detail regarding the environments with more computational trade-off. Besides this, the critical threats that we specify may be more useful for short-term rather than long-term analysis, where some non-critical threats can be the first step to launch more severe attacks.

Capturing the risk changes: our approach can capture dynamic risks through monitoring the changes in the environment context, the CAVs' state, and the interest of stakeholders. The CAVs are quickly aware of the risk changes, the dynamic risk management can be lightweight, while the changes can be reflected in the mitigation strategies.

Coordinating between the CAVs and infrastructures: we identify the essential information to communicate between the CAVs and the infrastructures, which include the record of attacks, potential threat agents, their typical goals, attack methods, and road conditions which may affect the CAV functionalities. Moreover, the infrastructures, which have global views in traffic and security incidents along the roads, can manage the risks through sending certain requirements to improve the security of the CAVs (e.g. require more focus on specific attack surface). On the other hand, the CAVs can also report to the infrastructure any attacks that they detect during the trip for the benefit of other CAVs. Some important issues that still need to be considered are the quality (e.g. when the infrastructure has significant traffic due to a high number of communications) and the reliability (e.g. spoofing) of the communication.

Managing and controlling risks at different levels, from different aspects: different stakeholders can influence the risk control by including their risk interest for the CAV to monitor. For example, if passengers require protection their privacy then the system will monitor the extra risks from the CAV components that can be vulnerable for privacy leakage (the reasoning will be based on the knowledge-based system).

6. Conclusion and Future Work

This paper introduces a simplified approach to manage the dynamic cyber security risks in CAVs'. The system that has been developed proposes a knowledge-based system for reasoning the critical attack surfaces, as well as the relevant threat agents and attack goals which target the CAVs. We then propose a design to coordinate communication and information sharing between transportation infrastructure and the CAVs, to detect the changes in context. We have presented a module to manage the dynamic cyber security risks, including the consideration of planning optimal mitigations. We have also considered a case study of CAV in platooning, to emphasise the advantages of dynamic risk assessment over the existing static approaches.

We anticipate that some of our future work will be to develop more uses of the knowledge-based system on the security analysis, and to extend this research in simulation environment for further verification.

Acknowledgement

This work was funded by UK Research and Innovation through INNOVATE UK in project CAPRI (TS/P012264/1).

References

[1] T. Maughan, "No One's Driving: Autonomous Vehicles Will Reshape Cities, but is Anyone Taking Control of How?," *Architectural Design,* vol. 89, no. 1, pp. 92-99, 2019.

[2] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy,* vol. 2, no. 2, pp. 155-184, 2017.

[3] SAE, "J3061: Cybersecurity guidebook for cyber-physical vehicle systems," *Society for automotive engineers,* 2016.

[4] ENISA, "Cyber Security and Resilience of smart cars," *Technical report, The European Union Agency for Network and Information Security (ENISA).* 2016.

[5] A. Ruddle *et al.*, "Deliverable d2. 3: Security requirements for automotive on-board networks based on dark-side scenarios," *tech. rep., EVITA,* 2009.

[6] ETSI, "TS102 165-1: Telecommunications and internet converged services and protocols for advanced networking (tispan). Methods and protocols," 2011.

[7] M. M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, "A risk assessment framework for automotive embedded systems," in *Proceedings of the 2nd ACM*

International Workshop on Cyber-Physical System Security, 2016, pp. 3-14: ACM.

[8] *ISO 26262: Road vehicles-Functional safety*, 2011.

[9] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "Threat and risk assessment methodologies in the automotive domain," *Procedia computer science,* vol. 83, pp. 1288-1294, 2016.

[10] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 2016, pp. 47-58: ACM.

[11] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, 2009, pp. 641-646: IEEE.

[12] M. Howard and D. LeBlanc, *Writing Secure Code*. Microsoft Press, 2002.

[13] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "SARA: Security Automotive Risk Analysis Method," in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, 2018, pp. 3-14: ACM.

[14] A. Le, C. Maple, and T. Watson, "A profile-driven dynamic risk assessment framework for connected and autonomous vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1-8.

[15] G. Erdogan, A. Omerovic, M. K. Natvig, and I. C. Tardy, "Towards Transparent Real-Time Privacy Risk Assessment of Intelligent Transport Systems," in *International Workshop on Risk Assessment and Risk-driven Testing*, 2016, pp. 11-18: Springer.

[16] M. McGurrin, "Vehicle information exchange needs for mobility applications: version 3.0," U.S. Dept. Transp., Res. Innovative Technol. Admin., Washington, DC, Final Rep. FHWA-JPO-12-021 2013.

[17] B. S. Schoenfield, *Securing systems: Applied security architecture and threat models*. CRC Press, 2015.

[18] S. Behere and M. Törngren, "A functional reference architecture for autonomous driving," *Information and Software Technology,* vol. 73, pp. 136-150, 2016.

[19] T. A. Team. (2018). *Architecture Reference for Cooperative and Intelligent Transportation*. Available: . https: 982 //local.iteris.com/arc-it/index.html

[20] L. Cui, J. Hu, B. B. Park, and P. Bujanovic, "Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack," *Transportation Research Part C: Emerging Technologies,* vol. 97, pp. 1-22, 2018.

[21] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller, "Emerging attacks on VANET security based on GPS Time Spoofing," in *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015, pp. 344-352: IEEE.

[22] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe,* vol. 11, p. 2015, 2015.

[23] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *International Conference on Cryptographic Hardware and Embedded Systems*, 2017, pp. 445-467: Springer.

[24] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEFCON,* vol. 24, 2016.

[25] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 640-660, 2019.