A Profile-driven Dynamic Risk Assessment Framework for Connected and Autonomous Vehicles

Anhtuan Le, Carsten Maple, Tim Watson

Cyber Security Centre, WMG, University of Warwick, Coventry, UK, [a.le.1, cm, tw]@warwick.ac.uk

Keywords: profile-driven, dynamic risk assessment, connected and autonomous vehicle, cyber security, safety

Abstract

The Internet of Things has already demonstrated clear benefits when applied in many areas. In connected and autonomous vehicles (CAV), IoT data can help the autonomous systems make better decisions for safer and more secure transportation. For example, different IoT data sources can extend CAV's risk awareness, while the incoming data can update these risks in real-time for faster reactions that may mitigate possible damages. However, the current state of the art CAV research has not addressed this matter well enough. This paper proposes a profile-driven approach to manage IoT data in the context of CAV systems through a dynamic risk management framework. Unlike the current inflexible risk assessment strategies, the framework encourages more flexible investigation of risks through different risk profiles, each representing risk knowledge through a set of risk input considerations, assessment methods and optimal reaction strategies. As the risks change frequently with time and location, there will be no single profile that can cover all the risks that CAVs face on the road. The uses of different risk profiles, therefore can help interested parties to better understand the risks and adapt to various situations appropriately. Our framework includes the effective management of IoT data sources to enable the run-time risk assessment. We also describe a case study of using the proposed framework to manage the risks for the POD being developed in the Innovate UK-funded CAPRI project.

1 Introduction

The Internet of Things (IoT) is a major trend that is set to shape the development of the second digital revolution by connecting "everything" to the Internet. With the capability of gathering useful data from different sources, IoT has been having strong implications in a wide range of areas such as the smart home, the smart city, industrial systems, agriculture, health, and so on. In particular, it has become a key enabler for the development of intelligent transport systems (ITS) [1, 2]. IoT devices are being embedded in a wide range of transportation components such as in-vehicle networks, road-side infrastructures, environment and in vehicle-to-vehicle (V2V) communication. Data gathered from these sources will form the big picture of the internal state of a vehicle, as well as its connections and interactions with surroundings, which enable drivers to make smarter decisions for safer and more secure driving.

Driving decision-support enabled by understanding the vehicle's internal and external environments is the central objective of connected and autonomous vehicles (CAVs). The Society of Automotive Engineers has defined levels of autonomy from 0 to 5 [3]. At the highest level, the vehicle is expected to take the place of the driver to make all the driving decisions. CAV technology can solve many long-term transportation issues such as reducing the traffic congestions that have become more and more popular due to the fast-growing urbanisation; providing safer transportation by preventing accidents; and improving traffic signal controls and fleet managements [3]. These benefits motivate the investments from industry, academia, and governments, which expect to boost the CAV market to 131.9 billion USD in 2019 [3].

A lot of attempts have been made to improve the driving decision-support using transportation data. Several offline road accident databases (e.g. [4]) are available to analyse factors that affect road safety. Soon, IoT will outperform these databases as they can both record a greater deal of important information (e.g. in-car information gathered through sensors, surrounding data coming from road operators and other vehicles, etc.) and provide them in a timely fashion to reflect the most recent driving situation. IoT data can bring many benefits such as improving the risk assessment from multiple perspectives and detecting the run-time dangers to mitigate potential damages [2]. However, applying IoT data effectively for such benefits is not well-addressed yet in the literature. For example, current safety and security standards and practices mainly classify the static risks based on the vehicle's assets, therefore without considering other IoT data sources. These risk assessments are also not updated frequently, so they will not be able to adapt quickly to newly discovered risks. Recently several attempts have been made to analyse the road safety in real-time based on multiple data sources, however, there is still a lack of a flexible theoretical risk management framework to apply to wider situations. A common challenge that such attempts face is the management of IoT data, which are huge, unreliable and incomplete [5].

This paper tackles the issues of managing IoT data in assessing CAV risks by proposing a profile-driven risk management framework. Overall, our approach drives the IoT data into several predefined risk profiles that are most relevant to users' scenarios. IoT data are first used to train the preferred risk assessment model in each profile. After the training period, the coming data will be employed as the inputs of the model to derive the risk assessment output. In more details, the framework consists of two phases: the design and operation phases. In the design phase, a reference library of risk profiles is developed based on the best standards, practices, and literature. Each profile clarifies the risk interests, available data sources to monitor, options of assessment methods, and recommendations of situations in which this profile should be employed. When using the framework, upon the needs and views of the operators, several profiles will be chosen with configurations of relevant data sources and assessment methods. In the operation phases, the data are first used to train the risk assessment model of each chosen profile. Data sources are also filtered and cleaned for more reliable evaluations. After the training, the resulting data will be used as inputs for the assessment models to obtain the run-time risk output. The training procedure will be repeated when condition-to-update are satisfied, for example, when there are more than a certain amount of new incoming data, or when there are changes in the initial assumptions of the model. The re-training cycle aims at updating the model for more accurate assessments.

The benefits of this approach can be multi-fold:

- The decision-making is supported by more relevant data sources. The assessment will therefore be more accurate, while the training process will become faster and more flexible, due to the reduction of data and features to monitor.
- The risk profiles represent risks from different aspects of interest to users, and hence can provide more information and improve the decisions' quality.
- Users receive the output faster and understand the assessment more precisely, which means they are more aware of the situational risks and can react better to mitigate the damages.

This paper is structured as follows. Section 2 introduces the background and review the related work that consider the application of IoT in CAV risk management. Section 3 discusses the requirements and challenges for the dynamic risk assessment framework. Section 4 presents the proposed solution, while Section 5 introduces a relevant case study of the POD. Section 6 concludes the paper and considers the future work.

2 Background and Related Work

Risk management is the process of identifying the most likely and dangerous risks in order to mitigate them in advance [6]. When the level of CAV autonomy evolves, there will be more and more new safety and security risks coming together with the modern technologies they employ. Risk management therefore has become crucial to ensure the public acceptances of CAV.

Despite the importance of CAV risk management, standard and practice development is only at the initial stage. Prominent guidelines are the ISO 26262 [7] which considers the functional safety of on-board electrical and electronic systems [8]; the J3061 [9] and the NHTSA [10, 11] guidebooks that focuses on the security of cyber-physical vehicle systems. A common theme in such guidelines is the use of four main phases: asset identification to understand the objects to protect, threat modelling which focuses on the adversaries' capabilities, risk analysis to justify the potential risks, and finally the mitigation plan for risk detection and reaction [12]. This theme is inflexible and limited in dealing with the dynamic risk environment of CAVs. Moreover, it does not consider the involvement of other available data sources in improving the understanding of the security and safety of such systems.

Evaluating the risks continuously and readily getting the best reactions are vital for CAVs, given that the risks they face on roads changes frequently and rapidly. Cheng *et al.* [13] assessed the risks at run-time by gathering data from sources such as the in-vehicle sensors, the vehicle state and the driver's behaviours. Authors in [14] used object tracking and classification, traffic management communication, and driver intention to assess the risk dynamically for vehicles at intersections. A real-life project developed by the Tennessee Highway Patrol officers used a software model called "Crash Reduction Analysing Statistical History" (C.R.A.S.H) to predict the accidents in an area of five by six squared miles for four-hour periods each day. The prediction results were sent to help drivers to make better on-road decisions. The model took into consideration a wide range of impact factors such as sporting events, weather patterns, alcohol selling points (assumed that some drivers nearby will be affected by alcohol or drugs), accident history and so on. The software was claimed to have an accuracy rate of 72% and reduce the Tennessee traffic fatalities of 5.5% [15].

A common issue with the current CAV risk assessment approaches is that they may miss some unknown factors which lead to unforeseen risks. For example, many models missed the traffic changes in the peak hours, or road condition updates. Such unknown risk factors may significantly affect the fixed model of the current approaches. Other issues that were not addressed are the data selection for training the model and decision on when the model needs to be updated, especially when the upcoming data reflect changes that are not covered in the current model.

A framework to manage the IoT dataflow on the CAV risk management lifecycle is needed to form better knowledge of risks from the gathered data. In [16], the authors suggested a knowledge-on-the-loop model to acquire risk knowledge by monitoring the system rationale flows continuously from design-time to post-deployment time and back. This framework supports the automated knowledge inference and

enrichment by using the Electronic Architecture and Software Technology – Architecture Description Language (EAST-ADL) to represent the knowledge; and the inference engine for automated reasoning and self-adaptation at post-deployment time.

For easy management, the risk data can be clustered and recorded into relevant profiles. The work in [17] uses the k-means cluster method to classify the situations in different road profiles. Such classifications were claimed to build a better dissemination strategy, which send the warning messages to all vehicle faster and more effectively. Authors in [18] also suggested the use of vehicle profiles, each represented by a history trust list and a friend list, to build a better trust management framework between vehicles.

3 Requirements and Challenges for Developing a Dynamic Risk Assessment Framework

CAVs operate on highly dynamic environments which contain frequent changes of threats, vulnerabilities, and technologies, while involving varied missions and functions. As a result, a dynamic risk management framework is essential to help the system adapt quickly to this unstable environment. Ideally, the framework should take advantages of the data coming from different IoT sources that can provide valuable risk information for a more accurate analysis. According to the NHTSA guideline [11], this framework also needs to be life-cycle based, and revisiting various tasks overtime depending on the changes of the information system and the environments. Moreover, the framework needs to keep monitoring the employed security controls over time to update the system's security state, while maintaining the initial security authorisation. The main challenges that this framework faces to satisfy these requirements are as follows.

3.1 Challenges from Managing the Gathered Big Data

Due to the large number of IoT sources and their sizes, the risk management framework will face the challenges of managing the big data gathered from such sources. Effective management should consider the characteristics of big data, which are different from traditional data. In fact, they are distinguished by the following factors: greater volume, variety (various types of data), velocity (produce, generate and analyse rapidly), value (low density but huge value), variability (inconsistency of data), and veracity (varied quality) [19]. The challenges in more details are:

- *Dealing with heterogeneous data:* data needs to be represented with the right metadata, which should be attached with provenance through the processing pipelines to trace any processing error happening along the dataflow [5].
- *Eliminating inconsistency and incompleteness:* the system must manage the data uncertainty, errors, and missing values to increase its data reliability. The volume and redundancy of big data can also be used in compensating missing data, verifying the conflicting cases, validating the trustworthy relationships, or finding the inherent clusters as well as relationships and models [5].
- *Reducing data scale for more efficient processing:* the large scale of gathered data leads to higher cost of storage and processing. On the other hand, for each risk assessment category, only a selected number of features and data are relevant. Therefore, the big data management needs to determine an effective way of selecting only the relevant data for the specified risk assessment interests. This will help to improve the data storage in a cost-effective manner.
- *Providing risk analysis in run-time:* the decision making in run-time may involve the complex queries on high volumes of data. To reduce the response time, data should be organised in an optimal way such as indexing or clustering in advance, based on careful specifications of the query needs.

3.2 Challenges from Managing the Risks at Different System Levels

Different system levels will have varied concerns and views on risk assessment. As a result, monitoring data and the assessment approaches for each level should be selected according to the corresponding concerns and views. Common CAV levels regarding risk managements are:

- *In vehicle level:* focuses on the safety and security risk assessment of the vehicle and other vehicles around.
- *Road sign level:* focuses on managing the safety and security of a local area, mainly by monitoring the traffic flow and other information sources that report specific properties of the situation along the road.
- *Area traffic management level:* the operator needs to understand how the local risks from one area can affect to the global risks of a larger area.
- *Producer level:* the producer need to assess the security and safety risk to improve the designs of their products.

3.3 Challenges from Understanding the Risks Deeper from Different Aspects

The gathered data can be used to obtain the risk assessment in different domains, such as:

- *System functional and technical safety requirements:* the system needs to monitor and analyse data related to the functional boundary and safe states to quickly detect potential hazards.
- *System security requirements:* the system needs to understand the security assets, attacks and consequences towards them. This will help to detect and react quickly with the security risks.
- *Situation awareness:* The collected information will be analysed to improve the situational awareness from different angles to achieve the global views, which later will lead to more accurate analysis.

4 Proposed Dynamic Risk Management Framework

In this section, we propose a dynamic risk assessment framework to manage the IoT data effectively for the evaluation of CAV risks. Instead of considering risks with a predefined set of threats and elements, our framework manages risks through profiles, each containing risk information of a specific aspect that relates to users' views and needs. A risk profile of an object reflects its current risk knowledge, which are formed through relevant collected data and assessment methods. The profile can be updated to reflect situation changes by analysing the monitoring data or advances in theoretical assessment methodologies. It also guides the reaction strategies for the risk assessment results, for example, suggesting best countermeasures (e.g. reconfiguring the protection, applying stricter encryption and security policies, etc.) for each type of results. Risk management authorities will collect and manage different risk profiles in a library and distribute the relevant profiles to users, either by broadcasting or on-request. In transportation, depending on risk awareness and needs, transporters can request relevant risk profiles to form their own risk assessment model. This model will consider only a limited number of IoT input sources filtered by the chosen profiles, hence it will assess the risk faster and provide more understandable results to users. Moreover, when accidents happen, road operators can broadcast similar profiles for other transporters to help them react faster and with an optimal strategy.

The framework consists of two main phases: the design phase and the operation phase, as can be seen in Fig. 1. The design phase involves analysing the related standards, practices, guidelines, and risk literature that form the risk knowledge represented by risk profiles. Each profile includes a specific set of metrics and features, and assessment models, differentiated by safety and security views and needs. Available and relevant IoT data will be selected to train the risk assessment models. After the training, the model is ready to derive assessment results when the new data arrive. In the operation phase, first CAVs will collect the risk profiles that are most relevant to their situations. They will also configure the data sources and assessment method in each profile. When CAVs are on the road, IoT data from pre-configured sources will be fed to the assessment model to answer the risk concerns in a way that is most meaningful for the users. Incident information will be also updated by road operators to help CAVs react better in run-time conditions. Inaccurate assessment result will be reported and reviewed to improve the risk understanding and optimise risk profiles. The reviews and updates will be done in cycle to adapt to the changes of the real world transportations.

The framework will develop the risk knowledge constantly through the risk profiles by the four steps shown in Fig. 1, which are elaborated further in the following paragraphs.

4.1 Risk Profile Justification

First, a comprehensive list of risk profiles is formed by reviewing the security practices, standards, and relevant risk literature. This list is re-reviewed frequently upon the literature update. As a result, the list is not fixed, but it can be either extended or eliminated. At high-level, each profile represents the risk knowledge of an aspect that users wish to use. At low-level, the profile contains a set of descriptions for requirements, metrics, assessment methods and recommendations of situations that are useful to employ.

In practice, users can select a set of profiles following their risk views and needs based on the guidelines from the profiles library. The justified set will identify the data sources that need to be monitored, and use these sources to derive on-road risk assessment results for users. CAV producers can extend users' profile choices by providing plug-n-play risk management modules, which are devices that collect information for assessing specific risks.

4.2 Risk Assessment Model Selection and Training

Knowledge of risk assessment models (e.g. form and meaning of results, pros and cons of methods) will be made available for users so they can choose the best suitable models for their purposes. For instance, some users may prefer a quantitative assessment model because it is easier to compare and rank different risks, while others think the qualitative models give more understandable results.

After the models are selected, IoT data will be filtered, pre-processed and used to train the model. To ensure adequate levels of accuracy, the models need to consider the size and quality of data. For example, data should be cross-checked for reliability, should be continuously updated for changing transport conditions, or in case of missing and unreliable data, the model should check from other available sources. At the end of this procedure, the model is ready to give assessment results up on incoming data.

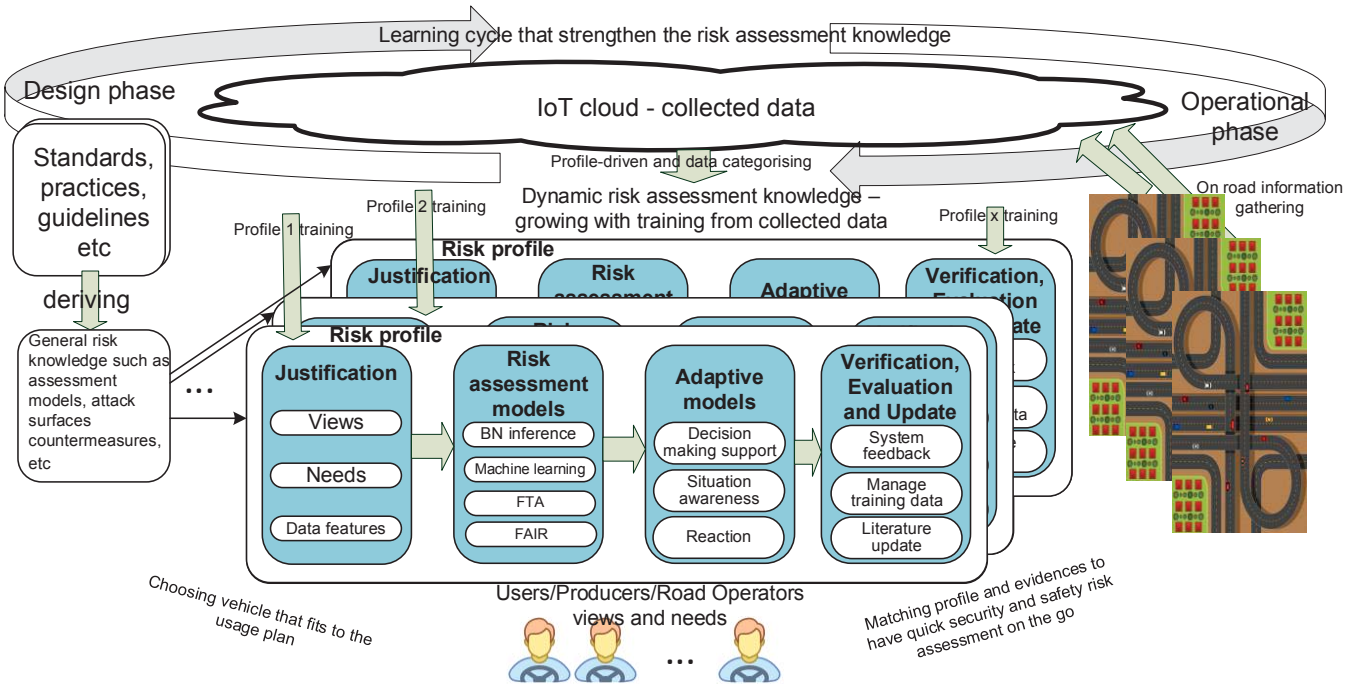

Figure 1: Profile-driven dynamic risk management framework

4.3 Adaptive and Run-time Security Monitoring

Users can obtain run-time risk assessment results when the upcoming IoT data are fed to the justified models. The results are presented in a form that is most understandable for users, while different risk profiles provide the views of system risks from different angles, therefore the framework can bring a deeper and more accurate risk awareness. In case abnormal risks are observed, users can follow suggestions on optimal reaction strategies provided in the profiles to adapt to the situation. In incident scenarios, the user reactions can be recorded for reviewing and learning to further improve the risk profiles.

4.4 Model Evaluation, Validation and Update

The selected risk profiles can be evaluated and validated based on the real-time operations of the system. For each type of situation, different risk profiles can be compared in terms of accuracy and efficiency to rank for recommendations. When a risk model provides inaccurate or unreliable assessment results, the relevant update IoT data will be used to re-train the models, subject to sufficient data size and data quality.

5 Case Study: Dynamic Risk Management Framework for the PODs

In this section, we present a case study that applies the proposed framework to manage safety and security risks in our CAPRI (Connected & Autonomous POD on-Road Implementation) project, which is tasked with the development of the "pods-on-demand" (POD) type of services. Examples of the services include using the autonomous PODs to move passengers around fixed areas such as airports, shopping centres, or parks. Unlike the current PODs which operate by following white lines and evading obstacles [20], the PODs we are developing aim at better awareness of surrounding situations, hence become more flexible and adaptable in on-road decision making.

Security and safety risk management of such PODs is crucial in gaining public acceptance prior to their commercial release. The PODs are supposed to operate in public and uncontrolled environments so they will need detailed risk assessments and reaction processes to avoid unexpected situations. For the first phase, we developed a risk profile database as a knowledge platform to cover as many real-world risk situations as possible. We specify important assets and elements in operations and review relevant attacks on such objects. In particular, we focus on internal POD assets, cooperative communication from POD to POD, communication between PODs and fixed infrastructure such as road signs, and between PODs and the cloud-based traffic infrastructure management system. The communication architecture of the POD system is essentially an IoT-based system, where the data are constantly gathered from internal POD sensors, road infrastructure, and other sources that gather information such as weather and surrounding traffic. The operational data of PODs through time are stored in the cloud, which enables the learning and training needed for the risk analysis and prediction models.

We also review the relevant safety and security attacks that relate to the assets. For example, Petit *et al.* [21] reviews the potential attack surface of CAV associated with both the internal technology of the vehicles and their communication with external elements. Studies that discuss the vehicles' attack surface can be found, for example, in [22-29]. Petit *et al.* [30] also investigate the remote attacks on camera and Lidar system. Chen *et al.* [31] assess the contactless attacks

on vehicles' sensors that are used to guide the driving, such as millimetre-wave radars, ultrasonic sensors, forward-looking cameras by using off-the-shelf hardware. These attacks seriously affect the safety functions of such vehicles by blocking their vision and causing them to malfunction. Zhang *et al.* [32] considers the malware issue and its countermeasures. Amozahed *et al.* [33] assesses the effects of security attacks on the communication channel and sensors to create instability in the operation of a connected vehicle stream.

Overall risk assessment techniques can be classified mainly in three categories: quantitative, qualitative, and hybrid. The quantitative approach uses probability and statistics theory to assess the risk likelihood in numerical form, for example, using probabilistic models, such as Bayesian Networks, or machine learning models. These methods can provide a clear and concise estimation of the risks; however, they require certain amount of historical data which are normally difficult to collect. The qualitative approaches, on the other hand, rely on expert opinions for providing qualitative outputs in state form (i.e. High, Medium, Low). Specific examples include the FAIR framework [34], attack tree analysis [35], and Fault tree analysis [36]. Their main advantages are their reliability, as they involve expert reasoning, and understandability. However, the categorisation is vague and cannot be used to rank large numbers of threats. The hybrid models try to combine the advantages of quantitative and qualitative methods and reduce their drawbacks, for example, giving numerical assessment for risks in the same qualitative category [37]. Upon understanding different assessment approaches, we suggest the most suitable and efficient risk model for each profile.

We further obtain risk information for each profile from different security and safety standards, practices, guidelines, and work from other relevant projects, such as the E-Safety Vehicle Intrusion Protected Applications (EVITA) project [38], ETSI Threat, Vulnerability, and implementation Risk Analysis (TVRA) standard [39], Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [40], ISO26262 [7], NHTSA [10, 11], J3061 [35]. Recommendations of optimal strategies to deal with specific threats are also extracted from these sources to serve as guidelines in operations.

For the second phase, we justify several use cases to validate the framework in practice. Each use case involves specific assets and transporting entities, while assessing their relevant threats and attacks. We select the profiles from the first phase that fit the use case requirements. Both simulations and real-world trials were conducted to collect the training data for the corresponding assessment models. Accidental and attack scenarios are implemented to validate the system's capability to react to safety and security threats respectively. We also focus on how the different profiles related and give deeper understanding of the risks, which helps the PODs to make more optimal decisions.

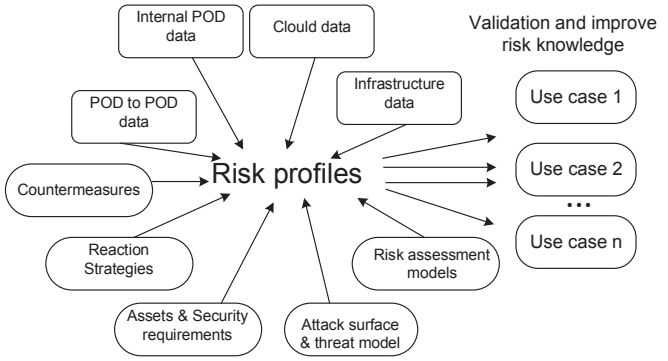

Figure 2: Applying the proposed framework in the CAPRI project

6 Conclusions and Future Work

This paper introduced a novel dynamic risk management framework to assess the risks from different views and system levels, based on risk knowledge represented through risk profiles. The framework provides a continuous cycle of selecting relevant risk profiles, training and updating assessment models, and managing the data sources effectively. The risk profiles can be adapted to varied stakeholders' needs, while capable of dealing with run-time requirement to support on-road decision making. The risk profile is also an effective concept in solving the challenges to make the most use of the IoT data. We also considered the practice of this framework by demonstrating a case study, which consider the risk assessment for the innovative autonomous PODs.

In the future, we aim at implementing the POD use cases to verify and validate the framework, and to improve the effectiveness of the dynamic profile selection, the IoT data management, and the reaction system. Another interesting aspect to explore is whether the system can predict the unknown threats, given that it has advances in updating and viewing the risks from different angles. An effective decision support tool for managing the CAV risks can also be developed based on the proposed framework.

Acknowledgements

This work was supported by the INNOVATE UK through the project CAPRI, contract number RESWM3525.

References

[1] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, "Situation awareness within the context of connected cars: A comprehensive review and recent trends," *Information Fusion,* vol. 29, pp. 68-83, 2016.

[2] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy,* vol. 2, no. 2, pp. 155-184, 2017/05/04, 2017.

[3] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE internet of things journal,* vol. 1, no. 4, pp. 289-299, 2014.

[4] UK. "UK road traffic accident data," https://data.gov.uk/dataset/road-traffic-accidents.
[5] H. Jagadish, J. Gehrke, A. Labrinidis, Y. Papakonstantinou, J. M. Patel, R. Ramakrishnan, and C. Shahabi, "Big data and its technical challenges," *Communications of the ACM,* vol. 57, no. 7, pp. 86-94, 2014.
[6] K. M. Martin, and R. H. ISG, "Towards an Autonomous Vehicle Enabled Society: Cyber Attacks and Countermeasures1."
[7] I. ISO, "26262: Road vehicles-Functional safety," *International Standard ISO/FDIS,* vol. 26262, 2011.
[8] C. Schmittner, and Z. Ma, "Towards a framework for alignment between automotive safety and security standards." pp. 133-143.
[9] SAE, "SAE International: J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," 2016.
[10] NHTSA, "National Highway Traffic Safety Administration: Cybersecurity best practices for modern vehicles," *Report No. DOT HS,* vol. 812, pp. 333, 2016.
[11] M. C, and H. K, "National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles," *Washington, DC: National Highway Traffic Safety Administration*, 2014.
[12] H. Abie, and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth." pp. 269-275.
[13] H. Cheng, N. Zheng, X. Zhang, J. Qin, and H. Van De Wetering, "Interactive road situation analysis for driver assistance and safety warning systems: Framework and algorithms," *IEEE Transactions on intelligent transportation systems,* vol. 8, no. 1, pp. 157-167, 2007.
[14] K. C. Fuerstenberg, and B. Roessler, "Results of the EC-Project INTERSAFE," *Advanced Microsystems for Automotive Applications 2008*, pp. 91-102: Springer, 2008.
[15] C. Subramanian. "The new way that tennessee is reducing auto fatalities," http://nationswell.com/tennessee-c-r-a-s-h-program-reduces-auto-fatalities/.
[16] D. Chen, K. Meinke, K. Östberg, F. Asplund, and C. Baumann, "A Knowledge-in-the-loop approach to integrated safety&security for cooperative system-of-systems." pp. 13-20.
[17] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "An adaptive system based on roadmap profiling to enhance warning message dissemination in VANETs," *IEEE/ACM Transactions on Networking (TON),* vol. 21, no. 3, pp. 883-895, 2013.
[18] X. Chen, and L. Wang, "A Cloud-Based Trust Management Framework for Vehicular Social Networks," *IEEE Access,* vol. 5, pp. 2967-2980, 2017.
[19] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context Aware Computing, Learning and Big Data in Internet of Things: A Survey," *IEEE Internet of Things Journal*, 2017.
[20] D. Smith, "Robocar versus the Pod: A commentary on the state of play in the race for autonomous vehicle commercialisation," *Construction Research and Innovation,* vol. 8, no. 2, pp. 60-65, 2017.
[21] J. Petit, and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 16, no. 2, pp. 546-556, 2015.
[22] A. Bertolino, F. Di Giandomenico, G. Lami, F. Lonetti, E. Marchetti, F. Martinelli, I. Matteucci, and P. Mori, "A tour of secure software engineering solutions for connected vehicles," *Software Quality Journal*, pp. 1-34, 2017.
[23] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions." p. 1.
[24] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces."
[25] M. Razzaque, A. Salehi, and S. M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: survey and the road ahead," *Wireless Networks and Security*, pp. 107-132, 2013.
[26] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks." pp. 1-12.
[27] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, "Security of autonomous systems employing embedded computing and sensors," *IEEE micro,* vol. 33, no. 1, pp. 80-86, 2013.
[28] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: a survey and future perspectives," *IEEE Communications Magazine,* vol. 54, no. 2, pp. 98-104, 2016.
[29] R. Coppola, and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys (CSUR),* vol. 49, no. 3, pp. 46, 2016.
[30] 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, pp. 2015, 2015.
[31] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON,* vol. 24, 2016.
[32] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 10-21, 2014.
[33] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle

streams and their impact on cooperative driving," *IEEE Communications Magazine,* vol. 53, no. 6, pp. 126-132, 2015.

[34] A. Shostack, *Threat modeling: Designing for security*: John Wiley & Sons, 2014.

[35] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using SAE J3061 for Automotive Security Requirement Engineering." pp. 157-170.

[36] K. Schmidt, P. Tröger, H.-M. Kroll, T. Bünger, F. Krueger, and C. Neuhaus, "Adapted development process for security in networked automotive systems," *SAE International Journal of Passenger Cars-Electronic and Electrical Systems,* vol. 7, no. 2014-01-0334, pp. 516-526, 2014.

[37] A. Le, Y. Chen, K. K. Chai, A. Vasenev, and L. Montoya, "Assessing loss event frequencies of smart grid cyber threats: Encoding flexibility into fair using bayesian network approach," *Smart Grid Inspired Future Technologies*, pp. 43-51: Springer, 2017.

[38] EVITA, "E-safety vehicle intrusion protected applications (EVITA)," http://www.evita-project.org/, 2016.

[39] J. E. Rossebo, S. Cadzow, and P. Sijben, "eTVRA, a threat, vulnerability and risk assessment method and tool for eEurope." pp. 925-933.

[40] C. J. Alberts, and A. Dorofee, *Managing information security risks: the OCTAVE approach*: Addison-Wesley Longman Publishing Co., Inc., 2002.