Connected and autonomous vehicles: A cyber-risk classification framework

Article · November 2018

DOI: 10.1016/j.tra.2018.06.033

CITATIONS
4

READS
208

4 authors:

Barry Sheehan
University of Limerick
11 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Finbarr Murphy
University of Limerick
59 PUBLICATIONS **193** CITATIONS
SEE PROFILE

Martin Mullins
University of Limerick
60 PUBLICATIONS **177** CITATIONS
SEE PROFILE

Cian Ryan
Dublin City University
5 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Transportation Research Part A xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Transportation Research Part A

journal homepage: www.elsevier.com/locate/tra

Connected and autonomous vehicles: A cyber-risk classification framework

Barry Sheehan*, Finbarr Murphy, Martin Mullins, Cian Ryan

University of Limerick, Ireland

ARTICLE INFO

Keywords:
Connected and autonomous vehicles
Intelligent transport systems
Cyber-risk
Cyber liability
Risk assessment
Auto insurance
Bayesian networks

ABSTRACT

The proliferation of technologies embedded in connected and autonomous vehicles (CAVs) increases the potential of cyber-attacks. The communication systems between vehicles and infrastructure present remote attack access for malicious hackers to exploit system vulnerabilities. Increased connectivity combined with autonomous driving functions pose a considerable threat to the vast socioeconomic benefits promised by CAVs. However, the absence of historical information on cyber-attacks mean that traditional risk assessment methods are rendered ineffective. This paper proposes a proactive CAV cyber-risk classification model which overcomes this issue by incorporating known software vulnerabilities contained within the US National Vulnerability Database into model building and testing phases. This method uses a Bayesian Network (BN) model, premised on the variables and causal relationships derived from the Common Vulnerability Scoring Scheme (CVSS), to represent the probabilistic structure and parameterisation of CAV cyber-risk. The resulting BN model is validated with an out-of-sample test demonstrating nearly 100% prediction accuracy of the quantitative risk score and qualitative risk level. The model is then applied to the use-case of GPS systems of a CAV with and without cryptographic authentication. In the use case, we demonstrate how the model can be used to predict the effect of risk reduction measures.

1. Introduction

The multiplicity of enabling technologies embedded within connected and autonomous vehicles (CAVs) promises prevention and mitigation of accidents, reduction in greenhouse gas emissions and more efficient utility of energy and infrastructure (Hult et al., 2016). With this, the in-vehicle communication network supports an increasing wealth of electronic control units (ECUs), sensors, actuators and interfaces. A primary goal of driver-less vehicles is the reduction of road fatalities predominately caused by human error. However, it is again humans who pose the greatest threat to CAVs. The creators of the enabling technologies may unwittingly

Abbreviations: CAV, Connected and Autonomous Vehicle; BN, Bayesian Network; ECU, Electronic Control Units; NVD, National Vulnerability Database; CVSS, Common Vulnerability Scoring Scheme; OEM, Original Equipment Manufacturer; ASIL, Automotive Safety Integrity Level; GPS, Global Positioning System; TPMS, Tyre Pressure Monitoring Systems; CAN, Controller Area Network; OTA, Over-the-air; EM, Expectation-Maximisation; ML, Maximum Likelihood; ISO, International Organisation of Standardization; SAE, Society of Automotive Engineers; PCI, Payment Card Industry; Mod, Modified; Req, Requirement; Env, Environmental; Temp, Temporal; Adj, Adjacent; Ctrl, Control; Meas, Measurement; Infra, Infrastructure; V2V, Vehicle to Vehicle; V2I, Vehicle to Infrastructure; V2X, Vehicle to Everything; Cmplx, Complexity; Avail, Availability; Conf, Confidentiality; N, None; L, Low; M, Medium; H, High; C, Critical; Vers, Version; P, Probability

* Corresponding author.
E-mail address: Barry.Sheehan@ul.ie (B. Sheehan).

https://doi.org/10.1016/j.tra.2018.06.033

create systems with defects or vulnerabilities[1] that allow malicious hackers the opportunity to exploit these vulnerabilities. CAV cyber-risk is of particular concern to insurers, regulators and policing authorities and an appropriate method to risk assessment is required. In this paper, we present a Bayesian network (BN) cyber-risk classification model and demonstrate its ability to rank the risk of a CAV GPS system vulnerability. This model can be used by insurers, vehicle manufacturers and suppliers to classify the risk of CAVs using known system vulnerabilities. It can also be used to forecast future vulnerabilities using scenario analysis. To our knowledge, this is the first application of a probabilistic risk assessment of CAVs cyber systems using a significant data set.

Cyber-risk is defined as the risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems (IRM, 2018). Cyber-risks are dynamic in nature due to persistent digital innovations, intensifying global connectivity and the increasing sophistication of hackers. The fast pace of technological innovations, the potential for correlated risk exposure and the lack of historical claims data makes cyber-risk a complex phenomenon for insurers to underwrite (SwissRe, 2017). Commercial cyber security vulnerabilities pose risks including business interruption, breach of privacy and financial losses. However, with CAVs, the stakes are raised with the amplified threat of the loss of human life.

As vehicles have become functionalised beyond their traditional purpose as a means of transport, the on-board software requirements have risen exponentially. A modern CAV may have approximately 100 million lines of code directing the effective operation of up to 70 ECUs (Charette, 2009) (Glancy, 2012) (Klinedinst and King, 2016). To put this into perspective, the Windows Vista operating system has only 40 million lines of code (Zimmermann et al., 2010), has 905 known vulnerabilities listed in the National Vulnerability Database (NVD), and was exploited in the widescale WannaCry and NotPeyta ransomware cyber-attacks in 2017 (Perlroth et al., 2017). At the same time, there are a growing number of car manufacturers and OEMs testing CAV prototypes on public roads. While this is a crucial activity for the self-learning capabilities of CAVs, it has not been without obstacles with two road fatalities where the vehicle has been at fault. These events underscore that while the driver-less technologies are still maturing, the race to automation and commercialisation must not neglect the importance of public safety, product resilience and comprehensive cyber security.

To understand the cyber-risk posed by cyber-physical systems (such as CAVs) Keller et al. (2017) suggest the asset should be considered as the sum of its hardware and software based sub-components. Moreover, the authors (Keller et al., 2017) propose that a comprehensive cyber security assessment must discover, understand, and address any vulnerabilities within each component. An established method for assessing system vulnerabilities is the Common Vulnerability Scoring System (CVSS), a standardised and application-neutral mechanism for detailing the characteristics of vulnerabilities and the possible severity of vulnerability exploitation (Scarfone and Mell, 2009). In 2011, the International Telecommunications Union (ITU, 2011) formally adopted CVSS version 2.0 as an international standard for scoring vulnerabilities. The U.S. National Institute of Standards and Technology (NIST, 2018) provide open-access to a large repository of known vulnerabilities called the National Vulnerability Database (NVD, 2018). This database aggregates and updates descriptions, references, product names and CVSS scoring information of software vulnerabilities provided by researchers, vendors and vulnerability coordinators since 2000. The NVD provides 16 known vulnerabilities associated with vehicles and are included in the Supplementary Material.

Our model is consistent with the Common Vulnerability Scoring System (CVSS) and uses listed vulnerabilities within the NVD to learn the relationship between variables and the strength of these relationships. The CVSS uses potential exploitability and impact to quantify risk of a known vulnerability. We propose these metrics to calculate CAV cyber vulnerabilities. Furthermore, we suggest that the prevailing standard for risk classification for automotive electrical and electronic systems, the Automotive Safety Integrity Level (ASIL), is flawed in relation to CAVs.

For a CAV cyber-risk classification framework to be effective, it needs to be one that can adapt to the dynamically changing nature of the risk, evolving when new threats emerge. Traditional reactive (or historical data driven) models are generally incapable of predicting in environments of low volume and varied data. The Bayesian network (BN) model developed in this paper uses the NVD to learn the graphical structure and train the parameters. Since the technology that enables connectivity and autonomy in vehicles is still evolving, there is little empirical evidence of cyber-attacks on CAVs. However, an analysis of the evolution of software vulnerabilities and adapting this information to the CAV paradigm empowers proactive risk analysis and assessment for vehicle manufacturers, OEMs, suppliers and insurance companies. Our BN captures system vulnerabilities to cyber-threats, considering the exploitability and potential impact of cyber-incidents. The subsequent comprehensive aggregation of all system vulnerabilities may be used to determine an overall CAV risk score. The BN graphical framework can also be used as an effective visual mechanism to communicate advice to non-expert stakeholders regarding how to maintain and/or improve their cyber-risk rating.

The proper functionality of the Global Positioning System (GPS) sensors are of critical importance to CAVs, providing self-localization with one-meter precision (Parkinson et al., 2017). The combination of information from LiDAR, radar and GPS permits self-localization and driving environment awareness and has been incorporated into most CAV prototypes, including Stanford's Junior (Montemerlo et al., 2008) and AnnieWAY (Geiger et al., 2012). However, the transmission of positioning data between satellites and GPS receivers are known to be susceptible to obstruction (Cui and Ge, 2003). Moreover, GPS signals are extremely weak signals broadcasted over wireless channels rendering them vulnerable to malicious remote interference (Jafarnia-Jahromi et al., 2012). Therefore, potential vulnerabilities associated with the GPS systems of a CAV are assessed using the BN model presented in this paper. Our case study application of the BN risk classification model demonstrates the viability of the approach.

[1] A vulnerability is defined as a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification (CVE, 2018).

The remainder of this paper is structured as follows: Section 1.1 provides an overview of the vulnerabilities associated with CAVs while Section 1.2 describes Bayesian networks and provides examples of their application within the cyber-risk domain. Section 2 details the implementation of the Bayesian network methodology utilising the NVD and CVSS. It also provides a description of the validation and case study methods. Section 3 presents the results of an out-of-sample validation test of the BN model and provides the results of the case study application of the model to the GPS systems of a CAV. Sections 4 discusses the principal contributions of this paper and Section 5 offers concluding remarks.

1.1. Connected and autonomous vehicle vulnerabilities

As vehicles become more connected to their external environment, the number of attack surfaces and risk of vulnerabilities being exploited escalates. A growing research literature has identified CAV vulnerabilities and analysed the potential impact of successful vulnerability exploitation while suggesting some mitigation measures (Petit and Shladover, 2015; Hong, 2016; Klinedinst and King, 2016; Lu et al., 2014; Studnia et al., 2013). The existing literature documents several successful cyber-attacks including those on security keys used by the ECUs, tyre pressure monitoring systems (TPMSs), wireless key fobs and more (Parkinson et al., 2017) (Zhang et al., 2014). Miller and Valasek (2015) operated a remote attack against a Jeep Cherokee by introducing malicious data into the Controller Area Network (CAN) bus that resulted in physical control of some elements of the vehicle including the braking system.

Zhang et al. (2014) present the challenges of defending connected vehicles against malware attacks. The authors (Zhang et al., 2014) suggest that the most severe security threats are yet to be realised as intelligent vehicles are increasingly able to connect to the Internet, enable Wi-Fi hotspots, communicate with other vehicles (V2V) and the external infrastructure (V2I) and patch over-the-air (OTA) ECU firmware updates. Parkinson et al. (2017) review a large volume of available literature identifying cyber vulnerabilities and mitigation methods for CAVs and highlight several knowledge gaps to prioritise future research within the CAV cyber security space. Moreover, Parkinson et al. (2017) find that the majority of known research is reactive in nature and that vulnerabilities are typically uncovered by researchers, hobbyists and white-hat hackers. Other reviews on the vulnerabilities of connected vehicles include Hong (2016), Klinedinst and King (2016), and Studnia et al. (2013).

Fig. 1 illustrates some fundamental cyber-attack types, vectors (or modes) and surfaces summarised by Parkinson et al. (2017), Zhang et al. (2014) and Petit and Shladover (2015). In the absence of connectivity, hackers require physical access to the vehicle to exploit system vulnerabilities. A successful attack of this kind would be confined to a singular vehicle only. However, with CAVs, the connection mechanisms which supports the communication between vehicles and infrastructure, also enables cyber-attacks to be carried out over wireless networks (Zhang et al., 2014). Hence, CAVs can be more easily compromised and weaponised to infect other vehicles. These connection mechanisms include vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-x (V2X), where x denotes any internet-enabled device (Lu et al., 2014). Studnia et al. (2013) identify cryptography, statistical anomaly detection systems and ECU software integrity solutions as the key security methods to protect CAVs against cyber-attacks.

1.2. Bayesian networks

BNs are probabilistic models of causes and effects, graphically expressing causal relationships (i.e. conditional probabilities) between different variables (Fenton and Neil, 2012). The chain of influences between variables can be illustrated graphically by linking nodes (i.e. variables) by one-way directed links that determine the nature of the causal dependencies (Nielsen and Jensen,

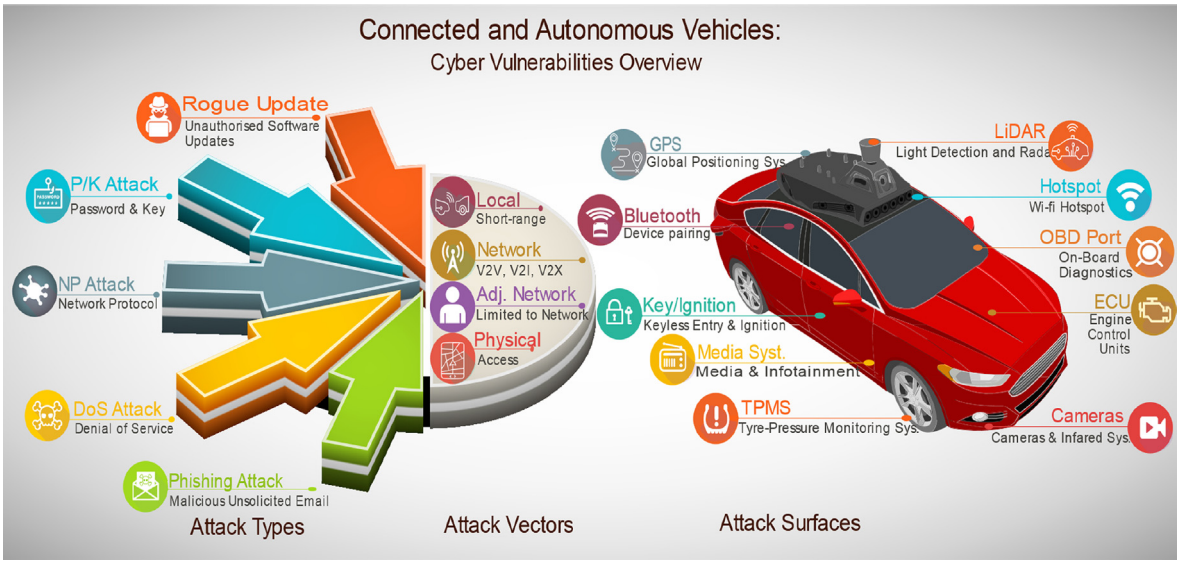

Fig. 1. Overview of cyber-attack types, attack vectors (or modes) and CAV attack surfaces.

2009). Each individual node has a finite set of mutually exclusive states, with each state described by a probabilistic expression determined by empirical relationships, mechanistic descriptions or expert judgement.

BN probabilistic models are suited to cyber-risk assessment through their ability to append subjective expert adjudication to heterogeneous datasets that often contain missing, or conflicting, information (Singh, 1997). Bayes' Theorem supports the probabilistic quantification of risk within the BN, and hence, enables this probabilistic updating capability. This makes the model particularly suited to problems with limited data through its ability to adapt its prior, or expert, belief (i.e. update its conditional probabilities) as new information becomes available. In this research, the structure of the BN model is first derived using expert judgement. This structure and the conditional dependencies between nodes are then updated by means of machine learning methods availing of a large dataset of known software vulnerabilities. The BN model is then applied to a CAV GPS system for cyber-risk classification. The variables input as evidence for this case-study are obtained using a combination of expert judgement and evidence from academic literature.

Another strength of BNs lie in their ability to facilitate bidirectional reasoning processes. While the one-way directed links in the BN graphical structure represent causal relationships, the flow of information moves in both directions. This allows BNs to be used for both prediction and abduction (Fenton and Neil, 2012) (Houmb et al., 2010). For example, if a software vendor is notified of a potential high-risk vulnerability within their product, the backward propagation (i.e., abduction) function of a BN can be used to prioritise how a lower risk level can be achieved (e.g. by implementing a workaround firmware update, or enhancing cryptography measures).

There are a growing number of BN applications for risk assessment across a diverse range of disciplines such as finance, medical diagnosis, safety and law (Fenton and Neil, 2012). A search of the literature indicates that BNs have not yet been applied to cyber-risk classification for CAVs. BNs have, however, been applied to other cyber security domains. Mukhopadhyay et al. (2013) develop a Copula-aided Bayesian Belief Network (CBBN) to determine the cyber-risk of digital business transactions and, hence, price e-insurance products. Qin and Lee (2004) use a BN model to identify cyber security attack plans, evaluate the likelihood of potential attack steps and forecast future attacks. Other applications of BNs include a usage based insurance risk estimation solution (Sheehan et al., 2017), traffic accident analysis (de Oña et al., 2011; de Oña et al., 2013), and accident injury severity estimation (Simoncic, 2004).

2. Methodology

A Bayesian Network (BN) model is proposed which utilizes the large collection of known software vulnerabilities stored in the NVD and the standardised CVSS scoring mechanisms to classify cyber-risk for CAV systems. The model is constructed using NVD data in the following steps. First, the graphical structure of the network is learned (i.e., determining the causal relationships). Next, the parameters are learned (i.e., the strength of the causal relationships via the conditional probability tables are determined) (Cheng et al., 2002). An out-of-sample validation test is then performed to examine the model accuracy is then applied. Finally, the model is then applied to a proposed CAV GPS system case study.

2.1. Data

Known software vulnerabilities listed within the NVD are used to create the BN. This data contains threat descriptions, product types, CVSS base attributes and a resultant base severity score for 104,210 software vulnerabilities from May 1990 to the present. The CVSS attributes are categorised into base, temp and environmental groups. The base metric group contains the intrinsic characteristics of a vulnerability that are constant over time and user environments (Mell et al., 2007). A base score is computed using a combination of qualitative exploitability and impact variables. The temporal group represents the changing of a vulnerability over time (i.e., at first there may be no remediation available, but over time an official fix becomes available). A temporal score updates the base score using the temporal variables if known. The environmental group provides context to the vulnerability and alters the score to highlight the features specific to the user's environment. For example, a successful breach into a CAVs steering functionality may have a higher impact than that into its windscreen wipers control module. The environmental score denotes the overall CVSS severity score, and updates the temporal score using context-specific variables. This CVSS severity score ranges between from 0 to 10. It quantifies the potential severity of a known vulnerability. In 2015, First (2018b) released version 3 of the CVSS. The updates included removing environmental group variables *Collateral Damage Potential* and *Target Distribution* and replacing them with mitigating factors in the event of a scope change. The *Authentication* base variable was also replaced by two variables; *Privileges Required* and *User Interaction*. The states within some of the attributes changed also (Hanford, 2013).

Both CVSS v2 and v3 vulnerability scores were extracted from the NVD. Of the 104,310 vulnerabilities, 6669 were deleted as they contained no useful information. 73,555 of the remaining cases only contained v2 group attributes, while 24,086 vulnerabilities were scored using both v2 and v3 scoring systems. For CVSS v2, the most probable state for each variable was: Access Vector = Network (70%), Access Complexity = Low (58%), Authentication = None (90%). Confidentiality/Integrity/Availability Impact were all equal to Partial at 47%, 51% and 43% respectively. Similarly, for CVSS v3 the most probable states for Attack Vector, Attack Complexity, Privileges Required and User Interaction were equal to Network (70.43%), Low (89%), None (72%) and None (59%) respectively. The only significant change in state observations were to Confidentiality/Integrity/Availability Impact, where the most probable state was equal to High determined by 59%, 51% and 63% of the total observations respectively. Further analysis of the NVD database is available in the Supplementary Material.

The NVD only records base metric attributes; therefore, 591 simulated vulnerabilities were created and scored using the CVSS v2

Table 1
Description of nodes describing the BN including (1) Variable name, (2) the Node ID (or acronym), (3) the CVSS version in which the variable is used, (4) the CVSS metric group, (5) list of possible states within which the variable can exist, and (6) list of parent nodes which have a causal influence on the variable (i.e., the child node). Parent nodes deduced from the CVSS equations are underlined in the ***Parent nodes*** **pa(X)** column. All parent nodes learned from the structural learning algorithm are not underlined besides RiskLevel and RiskScore which were derived using expert judgement.

Variable Desc.	Node ID	CVSS Vers.	Group	Possible states	Parent nodes pa(X)
Attack Vector	AV3	3	Base	Physical, Local, Adj. Network, Network	M_AV3
Attack Cmplx.	AC3	3	Base	L, H	M_AC3, PR3
Privileges Req.	PR3	3	Base	N, L, H	M_PR3
User Interaction	UI3	3	Base	None, Req.	M_UI, AV3, PR3
Scope	S3	3	Base	Unchanged, Changed	M_S3
Conf./Integrity/Avail. Impact	CI3, II3, AI3	3	Base	N, L, H	*CI3:* M_CI3, CR3, AI3 *II3:* M_II3, IR3, CI3, AI3 *AI3:* M_AI3, AR3
Conf./Integrity/Avail. Impact	CI2, II2, AI2	2	Base	N, Partial, Complete	*CI2:* II2, AI2, CR2 *II2:* IR2 *AI2:* II2, AR2
Base Score	BSc2, BSc3	2, 3	Base	[0 – 10]	*V3:* S3, ES3, IS3, BSev3 *V2:* ES2, IS2, BSev2
Base Severity	BSev2, BSev3	2, 3	Base	N, L, M, H, C	None
Access Vector	AV2	2	Base	Network, Adj. Network, Local	AC2
Access Cmplx.	AC2	2	Base	L, M, H	None
Authentication	Au2	2	Base	Multiple, Single, None	AV2
Exploit Code Maturity	ECM3	3	Temp.	Unproven, Proof of Concept, Functional, High	None
Remediation Level	RL2, RL3	2, 3	Temp.	Official Fix, Temporary Fix, Workaround, Unavailable	None
Report Confidence	RC2, RC3	2, 3	Temp.	*V3:* Unknown, Reasonable, Conf. *V2:* Unconf., Uncorroborated, Conf.	None
Exploitability	E2	2	Temp.	Unproven, Proof of Concept, Functional, High	None
Conf. Req.	CR2, CR3	2, 3	Env.	L, M, H	*V3:* None *V2:* IR2
Integrity Req.	IR2, IR3	2, 3	Env.	L, M, H	None
Avail. Req.	AR2, AR3	2, 3	Env.	L, M, H	None
Mod. Attack Vector	M_AV3	3	Env.	Network, Adj. Network, Local, Physical	None
Mod. Attack Cmplx.	M_AC3	3	Env.	L, H	None
Mod. Privileges Req.	M_PR3	3	Env.	N, L, H	None
Mod. User Interaction	M_UI3	3	Env.	None, Required	None
Mod. Scope	M_S3	3	Env.	Unchanged, Changed	None
Mod. Conf. Impact	M_CI3	3	Env.	L, M, H	CR3
Mod. Integrity Impact	M_II3	3	Env.	L, M, H	IR3
Mod. Avail. Impact	M_AI3	3	Env.	L, M, H	AR3
Collateral Damage Potential	CDP2	2	Env.	N, L, L-M, M-H, H	TD2
Target Distribution	TD2	2	Env.	N, L, M, H	None
Exploitability Score	ES2, ES3	2, 3	All	*V3:* [0–5] *V2:* [0–10]	*V3:* S3, AV3, AC3, UI3, PR3 *V2:* AC2, AV2, Au2
Impact Score	IS2, IS3	2, 3	All	*V3:* [0–5] *V2:* [0–10]	*V3:* S3, CI3, II3, AI3, ES3 *V2:* II2, CI2, AI2, CDP2, TD2
Temporal Score	TS2, TS3	2, 3	All	[0 – 10]	*V3:* ECM3, RL3, RC3 *V2:* E2, RL2, RC2
Env. Score	EnvS2, EnvS3	2, 3	All	[0 – 10]	*V3:* S3, BSc3, TS3 *V2:* BSc2, TS2, TD2, CDP2
Version	V	n/a	Risk	2, 3	None
Risk Score	RS	n/a	Risk	[0–10]	EnvS3, EnvS2, V
Risk Level	RLev	n/a	Risk	N, L, M, H, C	RS, V

and v3 online calculators (First, 2018a) to ensure that the model would learn the causal relationships between base, temporal and environmental metric groups. The simulated cases were created using Hugin 8.5 software tool. In total, 98,232 vulnerabilities were used to learn and test the BN. This dataset was randomly split into learning cases (90% of NVD and simulations each) and test cases for validation (10% of NVD and simulations) each. This data was used to learn and test the BN model using the learning algorithms provided in the Hugin 8.5 software (http://www.hugin.com/). The full NVD dataset, training data and test data are all available in the Supplementary Material.

Table 1 lists all the variables (nodes) used in the BN. The Risk Score and Risk Level nodes are the only instances that are user defined. These provide the overall risk score/level depending on the CVSS scoring version used to evaluate the vulnerability. Since CVSS v3 is the updated scoring mechanism, the overall Risk Score is assigned to the Environmental Score v3 if the vulnerability is scored using v3. The Risk Level uses the states defined in v3: None, Low, Medium, High, Critical.

2.2. BN structure and parameter learning

With sufficient data, machine learning techniques can be used to estimate the conditional probabilities (i.e., parameters) of a BN and to define the optimal configuration (i.e., structure) of the BN (Denœux, 2011, Alameddine et al., 2011). The prior structure of the BN is defined by deducing relationships from the CVSS scoring equations provided in their online documentation (First, 2018b). The BN structure is then optimized using the learning cases discussed in section 2.1 and the structural learning algorithm made available by the Hugin 8.5 software. For example, the CVSS v2 guide specifies the following equation to determine the *Base Score* (NIST, 2018):

$$Base\ \ Score = ((0.6 \times Impact\ \ Score) + (0.4 \times Exploitability\ \ Score) - 1.5) * f(Impact)$$

$$Where,\ \ f(Impact) = 0\ \ if\ \ Impact\ \ Score = 0,\ \ otherwise\ \ 1.176$$

It may be established from this that the *Impact Score* and *Exploitability Score* have a clear causal influence on the *Base Score*. This is represented graphically in the BN by a directed link from the *Impact Score* and *Exploitability Score* to the *Base Score*. The directed link from the *Base Severity* to the *Base Score* was determined as a result of the structure learning procedure. The prior structure, or parent nodes, deduced from the CVSS equations are underlined in Table 1. All parent nodes learned from the structural learning algorithm are not underlined.

Once the optimal graphical structure is learned, parameter estimation is performed using the Expectation-Maximisation (EM) algorithm. EM is appropriate for the calculation of maximum likelihood and maximum a posteriori estimates cases where missing data exists (Madsen et al., 2003). EM tries to find the optimal model parameters of the network given the observed evidence within the data. Non-informative prior probabilities were assigned to the nodes before the parameter learning process, hence the node parameters computed are the maximum likelihood (ML) estimates. These ML parameter estimates will become a priori beliefs when new NVD data becomes available, and the model will be refined to become the maximum a posterior BN.

The calculations are based on Bayes' Theorem, where the probability of a *hypothesis* given the *data* is expressed as:

$$P(hypothesis|data) = \frac{P(data|hypothesis) \times P(hypothesis)}{P(data)}$$

where $P(hypothesis)$ is the prior probability of the *hypothesis*, $P(hypothesis|data)$ is the probability of the *hypothesis* given the *data* (i.e., posterior probability), $P(data|hypothesis)$ is the probability of *data* given the *hypothesis* (i.e., likelihood) and $P(data)$ is the probability of the *data* (i.e., the evidence). An extended version of the Bayesian Network mathematical formulation, and structure and parameter learning algorithms are provided in Appendix 1.

2.3. BN validation test

As discussed in Section 2.1, there are 9794 cases withheld from the structure and parameter learning procedures to test the accuracy of the model. Missing variable data within the training and test cases accounted for 64% of the total database (i.e. each case has, on average, 64% of the variables with an unknown state). This is mainly due to temporal and environmental data not being reported to the NVD and v2 cases not including any v3 observations.

The out-of-sample test is performed for each case, where the risk score and risk level is predicted using the CVSS v2 and v3 parameters as input values. The predictions made by the BN model are assumed to be the state forecasted with the highest probability. These predictions are compared to the observed data, and the results are aggregated to determine the overall prediction accuracy for risk score and risk level.

2.4. Case study application

The BN cyber-risk classification model is applied to the Global Positioning Systems (GPS) for CAVs. Two well-known GPS threats are jamming and spoofing. GPS jamming is a simple and low-cost technique that uses radio frequency transmitters to prevent authentic signals being received by the GPS receiver. Devices to perform this attack are readily available at a cost of approximately US $20 (Petit and Shladover, 2015). Jamming enables car thieves to disable the antitheft tracker system from tracking the cars location once stolen. GPS spoofing refers to the procedure of broadcasting incorrect, but credible and valid, signals that deceive GPS receivers to provide false locations. Malicious exploitation of the GPS spoofing vulnerability could include guiding a CAV to an undesired location for theft, traffic disruption or crash initiation (Parkinson et al., 2017). Military-grade cryptographic authentication are proposed to be a suitable detection and mitigation technique against GPS spoofing and jamming attacks (Humphreys et al., 2008; O'Hanlon et al., 2013).

The description of GPS spoofing and jamming attacks by Petit and Shladover (2015) are used to derive CVSS version 2 states to use as input for the BN risk classification model. CVSS version 2 is used because it includes the Collateral Damage Potential variable, which is crucial for the robust description of CAV system risk.

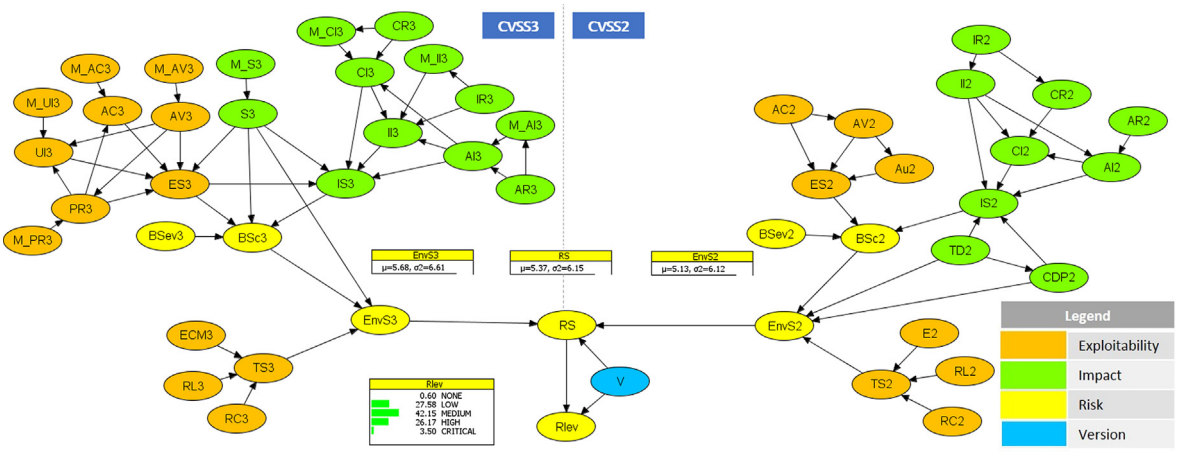

Fig. 2. Graphical structure and parameterization of the Bayesian network (BN) CAV cyber-risk classification model. Ellipses represent nodes and directed links indicate the conditional relationship between parent and child nodes. The bar chart for Rlev denotes the % state probabilities for the overall Risk Level. The rectangles above the EnvS2, EnvS3 and RS numerical nodes provide the mean and variance for Environmental Scores (v2 & v3) and Risk Score respectively. The nodes are colour categorised into orange for exploitability metrics, green for impact metrics, yellow for risk metrics and blue for CVSS version. CVSS Version 3 nodes are on the right hand side and CVSS Version 2 nodes are on the left hand side. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

3. Results

3.1. Bayesian network construction and validation results

The BN was developed with structure and parameter learning and is shown in Fig. 2. The illustration includes the marginal probabilities of the Risk Level (Rlev) node, and the mean and variance of the Environmental (EnvS2 & EnVS3) and Risk Score (RS) numerical nodes. The Risk Level node, which provides a qualitative classification of cyber-risk, specifies the following maximum likelihood state vulnerabilities: None (0.6%), Low (27.58%), Medium (42.15%), High (26.17%) and Critical (3.5%). Furthermore, based on all known vulnerabilities within the NVD at the time of writing, it is found that the average Environmental Score is higher for version 3 (5.68) than for version 2 (5.13). A sample of the resulting conditional probability tables are described in Appendix 2.

Table 2 provides a sample of 10 results from the out-of-sample validation test. The known Environmental Scores (v2 & v3), Risk Score and Risk Level of each case were withheld and all other parameters used by the BN as inputs (or evidence) to predict the Risk Score and Risk Level. The state with the highest probability is assumed to be the predicted state by the BN and is then compared to the actual state quantified using the online CVSS scoring tool. Comparison of the Risk Level predictions and actual values in Table 2 shows that it is predicted accurately in 9 out of 10 cases (the Risk Score is 100% accurate). For all 9794 test cases, the Risk Level is only predicted incorrectly for 2 cases (see Fig. 3) and the Risk Score is predicted accurately in all cases. Further technical details on the BN model construction and validation analysis can be found in the Supplementary Material.

3.2. GPS case study application results

The BN cyber-risk classification model is applied to the GPS system of a CAV. The CVSS input parameters were deduced from GPS jamming and spoofing descriptions provided by Petit and Shladover (2015) and Parkinson et al. (2017). Both GPS attack scenarios are evaluated with and without military-grade cryptography.

Table 3 displays the test cases applied to the BN model with the predicted Risk Scores and Risk Levels. The CVSS data was manually entered into the model as evidence and the Risk Score and Risk Level with the highest probability was observed. An example of manual evidence entry into the model and its resulting bidirectional flow of information is illustrated in Appendix 2. GPS spoofing with no risk mitigation is shown to exhibit the highest Risk Score (9.1). Moreover, the Risk Score is shown to reduce to 7.5 when cryptography risk mitigation is implemented. Similarly, the Risk Score is seen to reduce from 8.6 to 7.4 when cryptography is used to help mitigate GPS jamming attacks.

4. Discussion

In this paper, we develop a Bayesian network for CAV cyber-risk classification. The model utilizes the CVSS software vulnerability risk-scoring framework to specify the initial structure, and optimises the configuration and conditional probabilities using the NVD repository. The BN achieves almost 100% prediction accuracy in a validation test for Risk Score and Risk Level using 9794 cases excluded from the preliminary learning steps. Regulatory bodies, manufacturers, suppliers and insurers can use this model to proactively assess the cyber-risk potential of new and existing CAV technologies.

Table 2
Sample (10 cases) results of out-of-sample validation test for BN with CVSS version 3 input data.[1] Cases denoted with * contain an incorrect prediction.

Test Data																
Case	Version	Attack Vector	Attack Cmplx.	Privileges Req.	User Interaction	Scope	Conf. Impact	Integrity Impact	Avail. Impact	Base Score	Base Severity	Exploit. Score	Impact Score	Exploit Code Maturity	Remediation Level	Report Confidence
1	3	LOCAL	L	N	REQ.	CHANGED	H	L	H	8.5	H	N/A	N/A	UNPROVEN	WORKAROUND	CONF.
2	3	ADJ_NETWORK	L	N	REQ.	UNCHANGED	L	N	N	3.5	L	N/A	N/A	PROOF OF CONCEPT	TEMPORARY FIX	CONF.
3	3	ADJ_NETWORK	L	N	REQ.	UNCHANGED	H	H	H	8	H	N/A	N/A	PROOF OF CONCEPT	UNAVAILABLE	N/A
4	3	ADJ_NETWORK	L	N	NONE	UNCHANGED	H	L	H	8.3	H	N/A	N/A	UNPROVEN	UNAVAILABLE	CONF.
5	3	NETWORK	L	N	REQ.	CHANGED	H	L	N	8.2	H	N/A	N/A	FUNCTIONAL	TEMPORARY FIX	REASONABLE
6*	3	LOCAL	L	N	NONE	UNCHANGED	L	L	N	5.1	M	N/A	N/A	UNPROVEN	WORKAROUND	CONF.
7	3	NETWORK	L	L	NONE	UNCHANGED	H	H	H	8.8	H	N/A	N/A	FUNCTIONAL	OFFICIAL FIX	REASONABLE
8	3	NETWORK	L	N	REQ.	CHANGED	H	H	N	9.3	C	N/A	N/A	FUNCTIONAL	WORKAROUND	UNKNOWN
9	3	NETWORK	L	L	NONE	UNCHANGED	H	H	H	8.8	H	N/A	N/A	N/A	UNAVAILABLE	REASONABLE
10	3	NETWORK	L	L	NONE	UNCHANGED	H	H	H	8.8	H	N/A	N/A	UNPROVEN	WORKAROUND	UNKNOWN

Case *(cont'd)*	Temp. Score	Test Data												Validation Data			
		Conf. Req.	Integrity Req.	Avail. Req.	Mod. Attack Vector	Mod. Attack Cmplx.	Mod. Privileges Req.	Mod. User Interaction	Mod. Scope	Mod. Conf. Impact	Mod. Integrity Impact	Mod. Avail. Impact	Env. Score	Risk Score Actual	Risk Score Prediction [*P. (State)*]	Risk Level Actual	Risk Level Prediction [*P. (State)*]
1	7.6	L	L	L	PHYSICAL	L	N	REQ.	CHANGED	L	H	H	N/A	4.4	0.59 (4.4)	M	0.73 (M)
2	3.3	L	L	M	PHYSICAL	H	L	REQ.	UNCHANGED	N/A	N	N	N/A	1	0.55 (1)	L	0.68 (L)
3	7.6	L	M	L	ADJ_NETWORK	L	L	REQ.	CHANGED	H	H	H	N/A	7.4	0.59 (7.4)	H	0.68 (H)
4	7.6	H	H	M	NETWORK	L	L	N/A	CHANGED	H	L	N	N/A	9.1	0.89 (9.1)	C	0.90 (C)
5	7.4	H	M	H	NETWORK	L	L	REQ.	CHANGED	H	N	L	N/A	8.2	0.75 (8.2)	H	0.81 (H)
6*	4.6	L	L	L	NETWORK	H	H	REQ.	CHANGED	N/A	L	H	N/A	3.8	0.05 (3.8)	L	0.32 (M)
7	7.8	L	M	M	NETWORK	L	N	NONE	CHANGED	H	L	N	N/A	6.8	0.90 (6.8)	M	0.93 (M)
8	8.1	L	L	M	PHYSICAL	H	L	REQ.	CHANGED	L	H	H	N/A	5.2	0.79 (5.2)	M	0.86 (M)
9	8.5	L	H	L	ADJ_NETWORK	H	H	REQ.	UNCHANGED	N	L	N	N/A	2.4	0.57 (2.4)	L	0.69 (L)
10	7.2	M	M	M	PHYSICAL	H	N	N/A	CHANGED	L	H	N	N/A	4.7	0.60 (4.7)	M	0.73 (M)

[1] Table 2 shows the Test Data (Base, Temporal, and Environmental) entered as evidence into the BN model used to predict values for Risk Score and Risk Level (Validation Data). The Environmental Scores (v2 & v3), Risk Score and Risk Level were excluded from the test data. The Risk Score and Risk Level state with the highest probability given the test data is assumed to be the predicted state and is then compared to the actual state quantified using the online CVSS scoring tool.

	Actual				
Predicted	NONE	LOW	MEDIUM	HIGH	CRITICAL
NONE	0	0	0	0	0
LOW	0	576	0	0	0
MEDIUM	0	2	4778	0	0
HIGH	0	0	0	4078	0
CRITICAL	0	0	0	0	360

Error rate: 0.02
Average Euclidian distance: 0.00044
Average Kullback–Leibler divergence: 0.00171

Fig. 3. Risk Level Confusion Matrix. Columns denote the count of actual observations within a specific Risk Level state and rows show the count of predictions of a specific Risk Level state.

The commercial race to fully connected and autonomous vehicles is hardly a sustainable one. Accidents resulting from CAV technology failure may result in public mistrust, reputational damage and large financial losses from product recalls. Regulatory bodies and insurance companies often play a large role in the enforcement of acceptable safety standards for new technologies. The regulatory body typically first establishes suitable safety standards and accreditation for the technology. The insurers will use then these standardised criteria, historical claims data and other information to attempt to forecast the risk of the technology. Considerable uncertainty about the future claims losses resulting from a new technology often results in insurance companies charging disproportionately large premia for coverage, or even explicitly declining to underwrite the risk.

There is an exiguous amount of cases within the existing academic literature or supervisory standards contending with cyber-risk assessment for CAVs. Henniger et al. (2009) use attack trees to analyse the security requirements of automotive on-board networks. The authors assessed potential cyber-attacks using severity, success probability and controllability permitting the ranking of attacks based on their relative risk. Controllability refers to the ability of the driver to influence the severity of the outcome. The International Organisation of Standardization (ISO) sets the automotive-specific functional safety standard for all automotive electrical and electronic systems with ISO 26262 (ISO, 2011). Similar to Henniger et al. (2009), the standard assigns a qualitative risk score, called the Automotive Safety Integrity Level (ASIL), based on the function of the probability of exposure, the accident severity and the ability of a driver to control the outcome if a critical event occurs. In the case of cyber security risk for CAV systems, we propose that the driver controllability factor is unsuitable for two reasons:

1. The Society of Automotive Engineers (SAE) J3016 definitions of driving autonomy assert that it is the systems[2] task to monitor the driving environment for threats within the three highest levels of automation (levels 3–5): conditional automation, high automation, and full automation (SAE, 2014). The driver's attention may, therefore, be distracted and ill-equipped to handle any emergency driving tasks.
2. For obvious reasons, the driver cannot be assumed to be an expert in software security nor have any special training to operate highly automated vehicles.

These assumptions are echoed by Petit and Shladover (2015) in their review of potential cyber-attacks specific to automated vehicles. Ward et al. (2013) also consider the suitability of the ISO 26262 to the cyber security of CAVs and conclude that the standards need extension and adaptation to encompass the atypical nature of potential cyber-threats.

Evidence suggesting that human interactions with CAVs decrease as the autonomous capabilities increase can be seen from recent autonomous vehicle testing. The California Department of Motor Vehicles (DMV) lists 20 manufacturers permitted to test autonomous vehicles on their public roads in 2017. From these, 12 companies submitted the regulatory mandated annual disengagement reports for the testing periods December 2016 to November 2017 (California DMV, 2018). These reports include miles driven in autonomous mode per month, number of qualifying disengagements[3] and reasons for disengagements. Fig. 4 shows how the number of disengagements per 1000 miles are decreasing as manufacturers record more autonomous miles during the 2017 reporting period. This may be interpreted in two ways. First, the autonomous systems may be improving based on larger databases for model training. Second, test drivers increasingly trust the CAVs as the number of miles grow. The second explanation is also posited by Dixit et al. (2016) who found a positive correlation between reaction times[4] and autonomous miles driven. In 2017, Waymo noted the lowest qualifying disengagements per 1000 autonomous miles at 0.2, while recording the highest number (352,545) of autonomous miles

[2] System refers to driver assistance system, combination of driver assistance systems, or automated driving system.

[3] Disengagement, as defined by California DMV (2015), is deactivation of the autonomous mode when a failure of the autonomous technology is detected or when the safe operation of the vehicle requires that the autonomous vehicle test driver disengage the autonomous mode and take immediate manual control of the vehicle, or in the case of driverless vehicles, when the safety of the vehicle, the occupants of the vehicle, or the public requires that the autonomous technology be deactivated.

[4] Reaction time, as defined by California DMV (2015), is the period of time elapsed from when the autonomous vehicle test driver was alerted of the technology failure, and the driver assumed manual control of the vehicle.

Table 3
Description of GPS spoofing and jamming cyber-attacks with and without cryptography using the CVSS v2 variables and states.[1]

Input Data												
Case	Attack	Mitigation Technique	Version	Access Vector	Access Cmplx.	Authentication	Conf. Impact	Integrity Impact	Avail. Impact	Base Score	Base Severity	Exploitability
1	GPS Spoofing	None	2	NETWORK	L	N	N	COMPLETE	COMPLETE	9.4	H	PROOF OF CONCEPT
2	GPS Spoofing	Military-grade Cryptography	2	NETWORK	H	N	N	COMPLETE	COMPLETE	6.6	M	UNPROVEN
3	GPS Jamming	None	2	NETWORK	L	N	N	PARTIAL	COMPLETE	8.5	H	PROOF OF CONCEPT
4	GPS Jamming	Military-grade Cryptography	2	NETWORK	H	N	N	PARTIAL	COMPLETE	5.6	M	UNPROVEN

Case *(cont'd)*	Input Data										BN Model Output/ Predictions	
	Remediation Level	Report Confidence	Collatoral Damage Potential	Target Distribution.	Conf. Req.	Integrity Req.	Avail. Req.	Exploitability Score	Impact Score	Temporal Score	Risk Score	Risk Level
1	N/A	CONFIRMED	MED-HIGH	N/A	H	M	M	10	9.2	8.5	9.1	HIGH
2	N/A	CONFIRMED	MED-HIGH	N/A	H	M	M	3.9	9.2	5.9	7.5	HIGH
3	N/A	CONFIRMED	LOW	N/A	H	M	M	10	7.8	8.5	8.6	HIGH
4	N/A	CONFIRMED	LOW	N/A	H	M	M	3.9	7.8	5.6	7.4	HIGH

[1] Table 3 shows the Input Data (Base, Temporal, and Environmental) entered as evidence into the BN model used to predict values for Risk Score and Risk Level for four vulnerability scenarios involving the GPS system. The Risk Score and Risk Level state with the highest probability given the test data is assumed to be the predicted state.

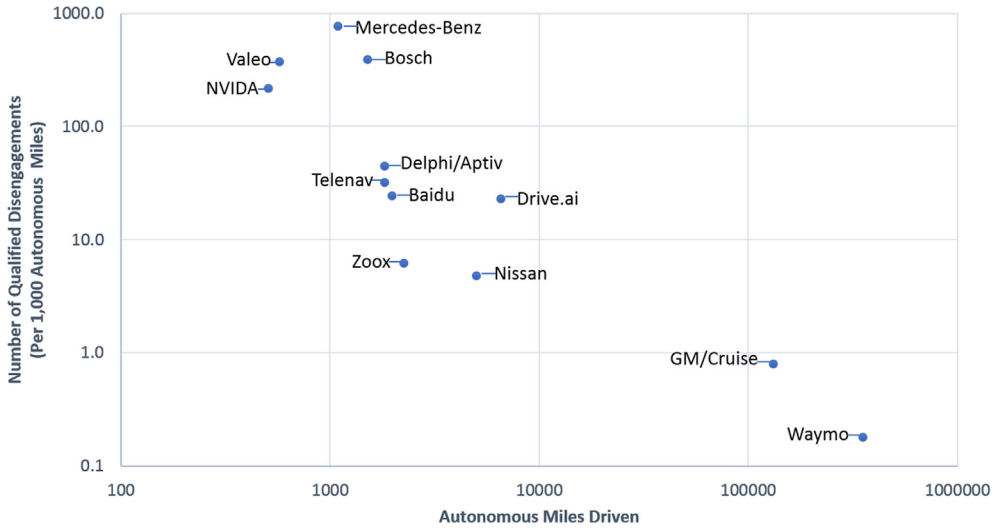

Fig. 4. Number of interventions per 1000 autonomous miles (log scale) by total driverless miles driven (log-scale) in California between 1st December 2016 (or earlier depending on initial issuance of testing permit) and 30th November 2017 (end of reporting period). Data source: California DMV (2018).

driven. This reinforces the unsuitability of the controllability factor within the ASIL risk scoring methodology for determining the risk of future CAVs systems.

The BN model developed in this paper excludes the driver controllability criteria for the purposes of cyber-risk assessment and uses probabilistic exploitability and impact metrics as risk proxies. It can be used by different stakeholders responsible for or concerned with the safe delivery of CAVs to our public roads. Vehicle manufacturers and suppliers can use the model to incorporate safety into the design of systems. For example, when the model is applied to a GPS case study, the BN classified the risk of a GPS spoofing cyber-attack as “Critical” when no cryptography mitigation techniques are applied. The BNs ability for scenario analysis is shown by highlighting the risk reduction when military-grade cryptography is utilized to prevent GPS spoofing. This can be extended to other CAV systems to promote the incorporation of cyber security into the design of CAV systems.

Regulatory bodies often lag behind when it comes to setting appropriate standards for emerging technologies. For CAVs, regulators are confronted with an unusual dilemma whereby risky testing of autonomous vehicles on public roads in the short-term is necessary to improve the safety and accuracy of the underlying automated driving systems in the medium- to long-term. The CVSS can be used to set threshold risk scores for known or scenario-based vulnerabilities. For example, in 2007 the CVSS v2 was incorporated into the Payment Card Industry Data Security Standard (PCI DSS) (First, 2018b). For compliance, all vendors processing payment cards must demonstrate that none of their computing systems have known vulnerabilities with a CVSS v2 score greater than or equal to 4. As the potential impact of vulnerabilities within CAVs is much greater than that of the PCI, the minimum system vulnerability demonstrable by manufacturers must be less than 4 (if any vulnerabilities are to be tolerated at all). The BN model can be used to aggregate both known and scenario-based vulnerabilities for regulators to stress test the cyber security of CAV systems.

The motor insurance industry are key stakeholders to the success of CAVs. Insurers are innovation enablers; they can bear the financial risk that underlies all state-of-the-art emerging technologies. With CAVs, however, technology faults or malicious exploitation by hackers not only present the threat of potentially catastrophic financial loss, but also major commercial reputational damage. Amendo et al. (2016) suggest that future autonomous vehicles linked to one manufacturer may be susceptible to catastrophic insurance loss since hacking a single vehicle may compromise an entire fleet. The volume and complexity of the sub-systems which comprise a CAV denote the difficulty ahead for insurers to forecast future claims with some degree of accuracy. Motor insurers will be required to adjust their actuarial pricing and underwriting systems as accident liability transfers from the human driver to the CAV technology (Sheehan et al., 2017). It has been projected that the adjustment to autonomous vehicles will generate at least $81 billion in new insurance revenues in the US between 2020 and 2025, with cyber-risk and product liability presenting the greatest opportunity generating $12 billion and $2.5 billion respectively in 2025 (Accenture, 2017). The model developed in this research provides insurers with a cyber-risk classification tool. The BN promotes proactive risk assessment as the motor insurance industry shifts to a technology-induced liability regime.

With 250 million connected cars predicted by 2020 (Meulen and Gartner, 2015), the potential for major product recall or liability claims triggered by cyber-attacks or software defects increases. For example, the Jeep Cherokee cyber-attack conducted by researchers Miller and Valasek (2015) initiated the recall of 1.4 million vehicles and at a cost of €761 m to the manufacturer, Chrysler (Sharman, 2015). This possibility of highly significant correlation of CAV cyber-attacks could prove a major obstacle for motor insurers in terms of risk-taking capacity and reserving. Therefore, only larger insurers and reinsurers may have the capacity to underwrite CAV cyber insurance in the future. The BN model developed in this paper can be used by insurers to classify the cyber-risk of the CAVs sub-systems and, hence, set underwriting criteria based on the aggregated Risk Score or Risk Level. These aggregated

scores can be used to compare the relative cyber-risk of different CAVs. Furthermore, insurers may use the BN to advise clients (manufacturers, OEMs, suppliers) on the effect of risk reduction techniques on their CAV components. This was demonstrated in the GPS application, where the Risk Score for a GPS spoofing attack is seen to reduce from 9.1 to 7.5 with the use of cryptography.

5. Conclusion

This paper presents a methodological approach to classify CAVs based on their cyber-security posture. The proposed BN cyber-risk classification model is tested for accuracy and applied to CAV GPS systems. The advantage of this method is that it allows the use of expert opinion, appended with quantitative and qualitative information using belief updating inherent to its Bayesian nature. Expert judgement was utilized in the initial construction of the BNs graphical structure and in the case study application of the model. Quantitative and qualitative information from the NVD were used to refine the BN structure and parameters using machine learning methods. The model can be used to aggregate both known and potential vulnerabilities even when full details are not known. The current automotive-specific functional safety standard for automotive electrical and electronic systems (ISO 26262) was assessed in relation to its suitability for CAVs for cyber-risk and in general.

We propose the CVSS software vulnerability scoring mechanism as a suitable standardised framework for CAV cyber-risk assessment. We use the data from 88,438 known vulnerabilities scored using CVSS and contained within the NVD and can exploit this prior evidence to predict knowledge gaps or potential new cyber vulnerabilities. Hence, it can be used for cyber-risk scenario-analysis and used to reverse-engineer appropriate risk levels of new CAV enabling technologies. The BN model is dynamic by nature, and can adapt its parameters and/or structure as new information becomes available. Therefore, the BN can be updated daily with new vulnerabilities reported within the NVD enabling proactive and instantaneous cyber-risk assessment. Based on this research, we recommend that the following actions are taken by regulatory bodies and others who are responsible for the safe and sustainable development of CAVs:

- Maximum allowable (or threshold) CVSS scores should be established and audited by regulatory bodies for known and scenario-based vulnerabilities for CAVs (e.g., no CAV system should have a vulnerability with a CVSS score greater than 2).
- The US National Institute of Standards and Technology (NIST) should restore the collateral damage potential and target distribution variables to the CVSS scoring mechanism. These variables are crucial for CAV cyber-risk assessment due to their highly correlated nature and their potential to cause loss of life.

The ISO 26262 automotive-specific functional safety standard needs to update its qualitative risk score (ASIL) for cyber-risk and the forthcoming expansion of CAVs on our public roads. As the number of autonomous test miles increase, the suitability of including a “driver controllability” metric diminishes.

Acknowledgements

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 690772. See www.vi-das.eu.

Conflicts of interest

The authors declare no conflict of interest.

Appendix 1. Bayesian network mathematical formulation

A Bayesian network is defined mathematically by $\mathscr{N} = (G = (V, E), \mathscr{P})$ and contains an directed, acyclic graph (DAG) G consisting of variables (or nodes) V and edges (or directed links)E. The set of probability distributions is denoted by $\mathscr{P}$. Each node $X \in V$ is a random variable and for each there exists a conditional probability distribution $P(X|pa(X)) \in \mathscr{P}$, where $pa(X)$ represents the parent nodes of X (Madsen et al., 2003). The Bayesian network $\mathscr{N}$ characterises the joint probability distribution $P(V)$, which factorizes according to the structure G given the equation below (Madsen et al., 2003):

$$P(V) = \prod_{X \in V} P(X|\ pa(X))$$

The prior structure G of the BN in this research is defined by deducing clear relationships from the CVSS scoring equations provided in their online documentation (NIST, 2018) (First, 2018b). These relationships, or edges, were specified as constraints prior to learning. The BN structure G was then optimized using the learning cases discussed in Section 2.1 and the structural learning algorithm made available by the Hugin 8.5 software. The Necessary Path Condition (NPC) structure learning algorithm was utilised with 0.05 level of significance specified. This is a constraint-based approach which identifies the optimal DAG structure from a set of conditional dependence and independence relations (CIDRs) obtained from statistical tests for independence. For a more detailed description of the BN structure learning algorithms see Madsen et al. (2003) or Steck and Tresp (1999).

The non-informative prior probability distributions $\mathscr{P}$ are updated using the Expectation-Maximisation (EM) algorithm to calculate the Maximum Likelihood (ML) parameters Θ representing the given structure G. The EM algorithm estimates the parameters of

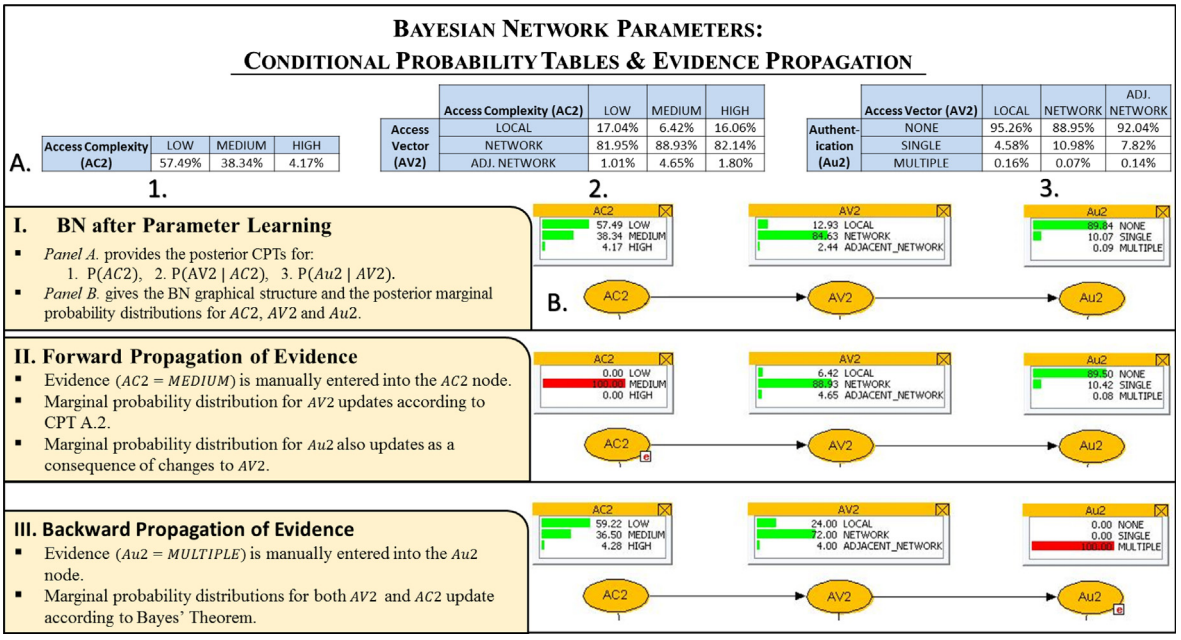

Fig. 5. Illustration of the CPT parameters of the learned BN and the bidirectional propagation of evidence functionality of the BN.

the BN by calculating the expected value of:

$$Q(\Theta^*|\ \Theta)=\mathbb{E}_{\Theta}\{\log P(X|\ \Theta^*)|D\}$$

where P is the density function of X, D is the learning data (or evidence), and Θ^* denotes the updated posterior parameters. The EM algorithm iterates by calculating the expected value of Q with respect to Θ (expectation step) and then maximising Q in Θ^* (maximisation step) until the stopping criteria is satisfied. For a more comprehensive description of the BN EM parameter learning algorithm see Madsen et al. (2003) or Lauritzen (1995).

Appendix 2. Bayesian network CPTs and evidence propagation illustration

See Fig. 5.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.tra.2018.06.033.

References

Alameddine, I., Cha, Y., Reckhow, K.H., 2011. An evaluation of automated structure learning with Bayesian networks: an application to estuarine chlorophyll dynamics. Environ. Modell. Software 26, 163–172.
Amendo, C., Hamm, P., Kelly, J., Maerz, L., Brunette, K., Scrudato, M., Finley, G. & Greene, L., 2016. Autonomous Vehicles-Considerations for Personal and Commercial Lines Insurers. Munich Re.
California DMV, 2015. Title 13, Division 1, Chapter 1: Article 3.7 – Autonomous Vehicles, Section 227.18 Requirements for Autonomous Vehicle Test Drivers.
California DMV, 2018. Disengagement Reports [Online]. Available: https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/disengagement_report_2017 [Accessed 24 April, 2018 2018].
Charette, R.N., 2009. This car runs on code. IEEE Spectr. 46, 3.
Cheng, J., Greiner, R., Kelly, J., Bell, D., Liu, W., 2002. Learning Bayesian networks from data: an information-theory based approach. Artif. Intell. 137, 43–90.
Cui, Y., Ge, S.S., 2003. Autonomous vehicle positioning with GPS in urban canyon environments. IEEE trans. Robotics Automation 19, 15–25.
CVE, 2018. Common Vulnerabilities and Exposures [Online]. Available: https://cve.mitre.org/about/terminology.html [Accessed 27/04/2018 2018].
de Oña, J., López, G., Mujalli, R., Calvo, F.J., 2013. Analysis of traffic accidents on rural highways using Latent Class Clustering and Bayesian Networks. Accid. Anal. Prev. 51, 1–10.
de Oña, J., Mujalli, R.O., Calvo, F.J., 2011. Analysis of traffic accident injury severity on Spanish rural highways using Bayesian networks. Accid. Anal. Prev. 43, 402–411.
Denœux, T., 2011. Maximum likelihood estimation from fuzzy data using the EM algorithm. Fuzzy Sets Syst. 183, 72–91.
Dixit, V.V., Chand, S., Nair, D.J., 2016. Autonomous vehicles: disengagements, accidents and reaction times. PLoS One 11, e0168054.
Fenton, N., Neil, M., 2012. Risk Assessment and Decision Analysis with Bayesian Networks. CRC Press.
FIRST. 2018a. Calculator [Online]. Available: https://www.first.org/cvss/calculator/3.0 [Accessed 23/04/18 2018].
FIRST. 2018b. User guide [Online]. Available: https://www.first.org/cvss/user-guide [Accessed 23/04/18 2018].
Geiger, A., Lauer, M., Moosmann, F., Ranft, B., Rapp, H., Stiller, C., Ziegler, J., 2012. Team AnnieWAY's entry to the 2011 grand cooperative driving challenge. IEEE

Trans. Intell. Transp. Syst. 13, 1008–1017.
Glancy, D.J., 2012. Privacy in autonomous vehicles. Santa Clara Law Rev. 52, 1171.
Hanford, S., 2013. Common vulnerability scoring system, v3 development update. Technical report, Forum of Incident Response and Security Teams (FIRST).
Henniger, O., Apvrille, L., Fuchs, A., Roudier, Y., Ruddle, A., Weyl, B., 2009. Security requirements for automotive on-board networks. In: Intelligent Transport Systems Telecommunications, (ITST), 2009 9th International Conference on. IEEE, pp. 641–646.
Hong, J., 2016. Cyber security issues in connected vehicle of intelligent transport system. Ind. J. Sci. Technol. 9.
Houmb, S.H., Franqueira, V.N., Engum, E.A., 2010. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Softw. 83, 1622–1634.
Hult, R., Campos, G.R., Steinmetz, E., Hammarstrand, L., Falcone, P., Wymeersch, H., 2016. Coordination of cooperative autonomous vehicles: toward safer and more efficient road transportation. IEEE Signal Process Mag. 33, 74–84.
Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'hanlon, B.W., Kintner, Jr., P.M., 2008. Assessing the spoofing threat: development of a portable GPS civilian spoofer. Proceedings of the ION GNSS international technical meeting of the satellite division. p. 56.
IRM, 2018. Institute of Risk Management. Available: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/ [Accessed 10/05/2018 2018].
ISO, 2011. ISO 26262: Road vehicles-Functional safety. International Standard ISO/FDIS.
Jafarnia-jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G., 2012. GPS vulnerability to spoofing threats and a review of antispoofing techniques. Int. J. Navigation Observ.
Keller, T.M., Benjamin, J.S., Wright, V.L., Gold, B.H., 2017. Vulnerabilities Under the Surface. Idaho National Lab.(INL), Idaho Falls, ID (United States).
Klinedinst, D., King, C., 2016. On board diagnostics: risks and vulnerabilities of the connected vehicle. Software Eng. Inst.-Carnegie Mellon Univ. 10.
Lauritzen, S.L., 1995. The EM algorithm for graphical association models with missing data. Comput. Stat. Data Anal. 19, 191–201.
Lu, N., Cheng, N., Zhang, N., Shen, X., Mark, J.W., 2014. Connected vehicles: solutions and challenges. IEEE Internet Things J. 1, 289–299.
Madsen, A.L., Lang, M., Kjærulff, U.B., Jensen, F., 2003. In: Quantitative Approaches to Reasoning and Uncertainty. Springer, pp. 594–605.
Mell, P., Scarfone, K. & Romanosky, S., 2007. A complete guide to the common vulnerability scoring system version 2.0. Published by FIRST-Forum of Incident Response and Security Teams. p. 23.
Meulen, R.V.D., Gartner, J.R., 2015. Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities. Gartner, STAMFORD, Conn.
Miller, C., Valasek, C., 2015. Remote exploitation of an unaltered passenger vehicle. Black Hat USA.
Montemerlo, M., Becker, J., Bhat, S., Dahlkamp, H., Dolgov, D., Ettinger, S., Haehnel, D., Hilden, T., Hoffmann, G., Huhnke, B., 2008. Junior: the stanford entry in the urban challenge. J. Field Rob. 25, 569–597.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K., 2013. Cyber-risk decision models: to insure IT or not? Decis. Support Syst. 56, 11–26.
Nielsen, T.D., Jensen, F.V., 2009. Bayesian Networks and Decision Graphs. Springer Science & Business Media.
NIST, 2018. National Institute of Standards and Technology [Online]. Available: https://nvd.nist.gov/ [Accessed 22/04/2018 2018].
NVD, 2018. National Vulnerability Database [Online]. Available: https://nvd.nist.gov/vuln/data-feeds [Accessed 30/03/2018 2018].
O'Hanlon, B.W., Psiaki, M.L., Bhatti, J.A., Shepard, D.P., Humphreys, T.E., 2013. Real-time GPS spoofing detection via correlation of encrypted signals. Navigation 60, 267–278.
Parkinson, S., Ward, P., Wilson, K., Miller, J., 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. 18, 2898–2915.
Perlroth, N., Scott, M., Frenkel, S., 2017. Cyberattack Hits Ukraine Then Spreads Internationally. The New York Times.
Petit, J., Shladover, S.E., 2015. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 16, 546–556.
Qin, X., Lee, W., 2004. Attack plan recognition and prediction using causal networks. In: Computer Security Applications Conference, 2004. 20th Annual. IEEE, pp. 370–379.
SAE, 2014. International Surface Vehicle Information Report: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. J3016. Society of Automotive Engineers.
Scarfone, K., Mell, P., 2009. An analysis of CVSS version 2 vulnerability scoring. In: Empirical Software Engineering and Measurement, 2009. ESEM 2009. 3rd International Symposium on. IEEE, pp. 516–525.
Sharman, A., 2015. Recall costs drag Fiat Chrysler to third-quarter net loss. Available: https://www.ft.com/content/85a2f738-7d7a-11e5-98fb-5a6d4728f74e [Accessed 21/04/18].
Sheehan, B., Murphy, F., Ryan, C., Mullins, M., Liu, H.Y., 2017. Semi-autonomous vehicle motor insurance: a Bayesian Network risk transfer approach. Transport. Res. Part C: Emerging Technol. 82, 124–137.
Simoncic, M., 2004. A Bayesian network model of two-car accidents. J. Transport. Statist. 7, 13–25.
Singh, M., 1997. Learning Bayesian networks from incomplete data. In: Proceedings of the Fourteenth National Conference on Artificial Intelligence and Ninth Conference on Innovative Applications of Artificial Intelligence. AAAI Press, pp. 534–539.
Steck, H., Tresp, V., 1999. Bayesian belief networks for data mining. In: Proceedings of the 2. Workshop on Data Mining und Data Warehousing als Grundlage moderner entscheidungsunterstützender Systeme. Citeseer, pp. 145–154.
Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., Laarouchi, Y., 2013. Survey on security threats and protection mechanisms in embedded automotive networks. In: Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on. IEEE, pp. 1–12.
SWISSRE, 2017. Cyber: Getting to Grips with a Complex Risk. SwissRe.
Ward, D., Ibarra, I., Ruddle, A., 2013. Threat analysis and risk assessment in automotive cyber security. SAE Int. J. Passenger Cars-Electronic Electr. Syst. 6, 507–513.
ITU, 2011. X.1521: Common Vulnerability Scoring System. Geneva, Switzerland: International Telecommunications Union.
Zhang, T., Antunes, H., Aggarwal, S., 2014. Defending connected vehicles against malware: challenges and a solution framework. IEEE Internet Things J. 1, 10–21.
Zimmermann, T., Nagappan, N., Williams, L., 2010. Searching for a needle in a haystack: predicting security vulnerabilities for windows vista. In: Software Testing, Verification and Validation (ICST), 2010 Third International Conference on. IEEE, pp. 421–428.