Jammer Detection in Vehicular V2X Networks

Ali Krayani, Nobel J. William, Lucio Marcenaro, and Carlo Regazzoni
DITEN, University of Genova, Italy
CNIT - Consorzio nazionale interuniversitario per le telecomunicazioni
email addresses: {ali.krayani, nobel.johnwilliam}@edu.unige.it, {lucio.marcenaro, carlo.regazzoni}@unige.it

(Invited Paper)

***Abstract*—Vehicle-to-Everything (V2X) is an emergent technology for enhancing traffic efficiency, road safety and autonomous driving. Vehicles interconnected with their prevalent wireless environment are prone to various security threats that might affect traffic and life safety immensely. Jamming attacks, a legacy and dated problem, still persists much to the havoc of V2X communications. The following paper proposes a framework for jammer detection adapted to V2X communications scenario. A Generalized Dynamic Bayesian network is used to learn the V2X signal environment in a statistical manner. Subsequently, a Modified Markov Jump Particle filter (M-MJPF) is used for signal predictions where the innovations in the observed signal versus the predicted signal enable our framework to detect the jammer. Simulation results highlight the efficacy and accuracy of our approach in V2X jammer detection.**

***Index Terms*—V2X, jammer detection, Generalized Dynamic Bayesian Networks.**

I. Introduction

Recently, vehicular technology has gained significant traction in the automotive and telecommunication industries [1]. Its extensive application across Vehicular ad hoc networks (VANETs) and Internet of Vehicles (IoVs) make it a prominent component in intelligent transportation systems and smart cities [2], [3]. It fundamentally provides a scaffold that enhances road safety, efficient road traffic management and lends a versatile infotainment pipeline for people on the road.

The integration of wireless communications in the automotive industry has led to the emergence of the Vehicle-to-Everything (V2X) communications [1]. V2X technology unwraps a host of current and future use cases such as cooperative awareness and sensing, vehicle on demand, tele-operated driving and subsequently fully autonomous driving [4]. V2X provides low-latency and high-reliability communications in vehicular networks, including vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P) and vehicle-to-infrastructure (V2I) communication links [5]. Due to its particular features as dynamic changes in the network structure, short connection duration, high mobility of network node, etc., V2X requires essential improvements to the functionalities of the conventional networks [6]. Moreover, as V2X technology stack evolves to be cognitive and self-aware, demands for safety and security becomes paramount, as it introduces open wireless networks, front and center into highly critical autonomous systems.

An important major class of denial of service attack at the physical (PHY) layer is the jamming attacks. Jammers often occupy the radio channel to detriment of its users by transmitting spurious radio signals. Jammers might mimic authorized equipment such as the Road Side Unit (RSU) by sending wrong information to vehicles in the vicinity leading to traffic jams or misleading vehicles to change driving behaviour [7]. Oscar *et al.* in [8] examines in detail the threats posed by jamming on VANETs. Attack vectors on vehicular networks are broadly classified into physical layer (Eavesdropping, GPS spoofing, Jamming), network layer attacks (Blackhole, Wormhole) and application layer attacks (Illusion, False Position) [9]. A Multi-Domain (Power and spectral) anti jamming scheme is proposed in [10]. Novel Jammer detection methodology using the dynamic Bayesian model framework is proposed in [11] to identify attacks at a symbol level over varying jammer power levels. Malebary *et al.* in [12], highlights different jamming models and their effectiveness in VANETs based on vehicle mobility patterns and jamming behaviour characteristics. Low power intermittent jamming detection using support vector machine (SVM) in [13] proposes to tackle different jammer strategies. Kumar *et al.* in [14] devises an anti jamming detection and mitigation scheme for localisation of the vehicles on the road. Moreover, a real time radio jamming detection scheme applying a data-mining method based on protocol design and past observation of channel events is demonstrated in [15].

Intentional, well designed attacks can often bring sophisticated networks to a standstill and thus, a serious detection and mitigation strategy to overcome this threat is vital. An important solution paradigm to mitigate many of the above attack scenarios is abnormality/ misbehaviour detection. A whitebox based approach for better explainabilty is an important step in designing advanced jamming detection schemes in tandem with enhanced resource allocation designs. This paper as in [11] proposes a jammer detection paradigm at the PHY layer applying a dynamic Bayesian framework adapted to meet the mobility based demands of the V2X scenario.

II. System Model and Problem Formulation

Consider a vehicular network consisting of N connected vehicles that are exchanging positional information with the base station (BS), while a malicious vehicle jammer transmits jamming signals with the intention of disrupting the legitimate V2I communications. The total available bandwidth is divided into N physical resource blocks (PRBs) and the set of V2I communication links between the vehicles and the BS is denoted as $\mathcal{N} = \{f_1, f_2, \ldots, f_N\}$ where each V2I link uses

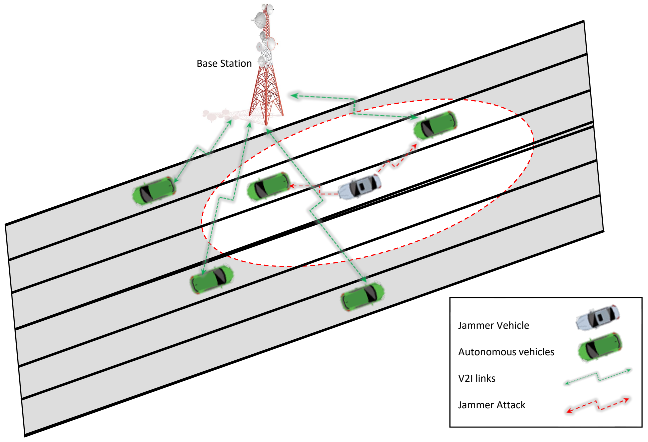


Fig. 1. Illustration of the System model.

a single PRB. The channel gain g_{nb,f_n} from the nth V2I link to the BS over the nth PRB is $g_{nb,f_n} = \alpha_{nb,f_n} h_{nb,f_n}$, where α_{nb,f_n} captures the large-scale fading effects as path-loss and shadowing and h_{nb,f_n} is the small-scale fading component which is distributed according to $\mathcal{N}(0,1)$. Denote $\mathcal{H}_0$ and $\mathcal{H}_1$ as the hypotheses of the absence and presence of the jammer, respectively. The received signal by the BS over the nth V2I link is given as: $r_{t,f_n} = g_{nb,f_n} x_{t,f_n} + v_{t,f_n}$ and $r_{t,f_n} = g_{nb,f_n} x_{t,f_n} + g_{jb,f_n} x^j_{t,f_n} + v_{t,f_n}$ at hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, where x_{t,f_n} is the legitimate transmitted signal, g_{jb,f_n} is the channel gain between jammer and the BS, x^j_{t,f_n} is the jamming signal, and v_{t,f_n} is the random noise. The BS receives multiple signals over N V2I links and aims to learn multiple dynamic models explaining the normal situation under $\mathcal{H}_0$. During testing, BS performs multiple predictions x^*_{t,f_n} conditioned on the learned models, and the jammer can be detected by comparing between predictions and current observations. If predictions do not match observations, the BS accepts $\mathcal{H}_1$. Otherwise, it accepts $\mathcal{H}_0$.

III. Proposed Jammer Detection Method

A. RF representation

We assume that the BS cast the dynamics of the physical signals received from connected vehicles at multiple levels using a Generalized state-space model. The BS aims to make inferences about hidden states generating sensory signals, given only sensory observations. We assume that the N vehicles are transmitting positional information to the BS over N PRBs. Thus, the BS receives N sensory observations ($\tilde{\mathrm{Z}}_{\mathrm{t}}$) each time instant t, which can be expressed as:

$$\tilde{\mathrm{Z}}_{\mathrm{t}} = \{\tilde{\mathrm{Z}}_{\mathrm{t,f_1}}, \tilde{\mathrm{Z}}_{\mathrm{t,f_2}}, \ldots, \tilde{\mathrm{Z}}_{\mathrm{t,f_N}}\}. \tag{1}$$

We assume that each sensory signal is a linear combination of a direct cause $\tilde{\mathrm{X}}_{\mathrm{t,f_n}}$ which is subject to random noise as follows:

$$\tilde{\mathrm{Z}}_{\mathrm{t,f_n}} = \mathrm{H}\tilde{\mathrm{X}}_{\mathrm{t,f_n}} + v_{t,f_n}, \tag{2}$$

where $\tilde{\mathrm{Z}}_{\mathrm{t,f_n}} \in \mathbb{R}^{2d}$ is a Generalized vector consisting the In-phase (I) and Quadrature (Q) features as well as the corresponding temporal derivatives (i.e., $\dot{I}$, $\dot{Q}$), $\mathrm{H} \in \mathbb{R}^{2d,2d}$ is the observation matrix that maps hidden states to observations, d is the space dimensionality that depends on the number of subcarriers in each PRB and f_n is the n-th PRB where $f_n \in \mathrm{N}$. The dynamic evolution of the hidden states $\tilde{\mathrm{X}}_{\mathrm{t,f_n}}$ can be explained by the following dynamic model:

$$\tilde{\mathrm{X}}_{\mathrm{t,f_n}} = \mathrm{A}\tilde{\mathrm{X}}_{\mathrm{t-1,f_n}} + \mathrm{B}\mathrm{U}_{\tilde{\mathrm{S}}_{t,f_n}} + w_{t,f_n}, \tag{3}$$

where $\mathrm{A} \in \mathbb{R}^{2d,2d}$ and $\mathrm{B} \in \mathbb{R}^{2d,2d}$ are the dynamic and control matrices, respectively. $\mathrm{U}_{\tilde{S}_{t,f_n}}$ is the control vector that depends on $\tilde{\mathrm{S}}_{t,f_n}$ and w_{t,f_n} is the process noise. $\tilde{\mathrm{S}}_{t,f_n}$ are discrete random variables which we refer to Generalized superstates realizing the direct cause of the continuous variables ($\tilde{\mathrm{X}}_{\mathrm{t,f_n}}$) and the in-direct cause to observations ($\tilde{\mathrm{Z}}_{\mathrm{t,f_n}}$). Those states evolve according to the following:

$$\tilde{\mathrm{S}}_{t,f_n} = \tilde{\mathrm{S}}_{\mathrm{t-1,f_n}} + w_{t,f_n}, \tag{4}$$

where $\mathrm{f}(.)$ is a non-linear function describing the dynamic transitions of the signal among the discrete variables at a specific f_n. The hierarchical stochastic processes defined in (2), (3) and (4) are structured in a Generalized Dynamic Bayesian Network (GDBN) as depicted in Fig.1. GDBN can model dynamic processes explaining the signal's temporal evolution at multiple levels and provides a graphical structure representing hidden and observed states as random variables encoding conditional dependencies [16].

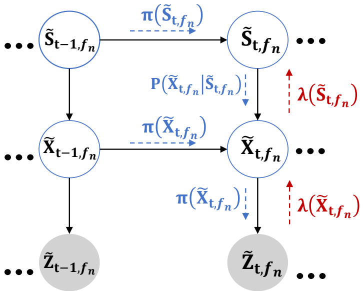

$\tilde{\mathrm{S}}_{\mathrm{t-1},f_n}$
$\pi(\tilde{\mathrm{S}}_{\mathrm{t},f_n})$
$\tilde{\mathrm{S}}_{\mathrm{t},f_n}$
$\mathrm{P}(\tilde{\mathrm{X}}_{\mathrm{t},f_n}|\tilde{\mathrm{S}}_{\mathrm{t},f_n})$
$\lambda(\tilde{\mathrm{S}}_{\mathrm{t},f_n})$
$\tilde{\mathrm{X}}_{\mathrm{t-1},f_n}$
$\pi(\tilde{\mathrm{X}}_{\mathrm{t},f_n})$
$\tilde{\mathrm{X}}_{\mathrm{t},f_n}$
$\pi(\tilde{\mathrm{X}}_{\mathrm{t},f_n})$
$\lambda(\tilde{\mathrm{X}}_{\mathrm{t},f_n})$
$\tilde{\mathrm{Z}}_{\mathrm{t-1},f_n}$
$\tilde{\mathrm{Z}}_{\mathrm{t},f_n}$

Fig. 2. Proposed GDBN.

B. Training multiple GDBN models

The BS starts perceiving the spectrum supposing that observations over multiple PRBs are subject only to random noise. During this phase, it expects that the dynamic evolution of the signals at the continuous level evolve according to a static rules (i.e., $\mathrm{U}_{\tilde{S}_{t,f_n}}$ in (3) equals 0). Hence (3) can be rewritten as:

$$\tilde{\mathrm{X}}_{\mathrm{t,f_n}} = \mathrm{A}\tilde{\mathrm{X}}_{\mathrm{t-1,f_n}} + w_{t,f_n}. \tag{5}$$

Since the vehicles are connected and transmitting positional information to the BS, the latter notices deviations between what it is expecting to receive and what it is actually observing. Then, BS calculates the Generalized errors representing the difference between predictions and observations in the following way:

$$\tilde{\varepsilon}_{\tilde{X}_{t,f_n}} = \mathrm{H}^{-1}(\tilde{\mathrm{Z}}_{\mathrm{t,f_n}} - \mathrm{H}\tilde{\mathrm{X}}_{\mathrm{t,f_n}}). \tag{6}$$

Those errors are clustered in an unsupervised manner using the Growing Neural Gas (GNG) to learn the semantic level that capture the dynamics of the signals inside the spectrum. GNG outputs a set of clusters (i.e., the Generalized superstates defined in (4)) encoding errors with similar dynamic patterns, such that:

$$\mathbf{\tilde{S}_{f_n}} = \{\tilde{\mathrm{S}}_{1,\mathrm{f_n}}, \tilde{\mathrm{S}}_{2,\mathrm{f_n}}, \dots, \tilde{\mathrm{S}}_{\mathrm{M},\mathrm{f_n}}\}, \tag{7}$$

where M is the total number of clusters. Analysing the dynamic transitions among the learned clusters allows to estimate the transition probabilities $\pi_{ij} = \mathrm{P}(\tilde{\mathrm{S}}_{\mathrm{t},\mathrm{f_n}} = i | \tilde{\mathrm{S}}_{\mathrm{t-1},\mathrm{f_n}} = j)$ and learn the transition matrix, accordingly, which is defined as:

$$\mathbf{\Pi} = \begin{bmatrix} \pi_{11} & \pi_{12} & \cdots & \pi_{1M} \\ \pi_{21} & \pi_{22} & \cdots & \pi_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \pi_{M1} & \pi_{M2} & \cdots & \pi_{MM} \end{bmatrix}, \tag{8}$$

where $\mathbf{\Pi} \in \mathbb{R}^{M,M}$ $\sum_{i}^{\mathrm{M}} \pi_{ij} = 1$, such that, $i, j \in \mathrm{M}$. Each discrete variable $\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}} \in \mathbf{\tilde{S}_{f_n}}$ is assumed to follow a multivariate Gaussian distribution and associated with specific statistical proprieties as the mean vector $\tilde{\mu}_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}} = [\mu_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}}, \dot{\mu}_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}}]$ where $\mu_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}}$ stands for the average of all the data samples in terms of I/Q inside $\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}$ and $\dot{\mu}_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}}$ stands for the average over the corresponding derivatives, and the covariance matrix $\Sigma_{\tilde{\mathrm{S}}_{\mathrm{m},\mathrm{f_n}}}$.

C. Online prediction and perception

During the online testing process, the BS performs multiple predictions to anticipate the sensory signals it should receive over multiple PRBs by employing the Modified Markov Jump Particle Filter (M-MJPF) [17] on the learned GDBN models. Under the Bayesian filtering framework, M-MJPF provides a combination of predictive causal probabilistic inference by propagating predictive messages from hierarchically higher levels to lower levels (top-down) and diagnostic probabilistic inference by propagating diagnostic messages in the opposite direction from bottom to up. Predictive messages are based on prior knowledge encoded in the GDBN models learned during the training phase that carry both the predictions of superstates performed by the Particle Filter (PF) and predictions of continuous states performed by the Kalman Filter (KF). Such a combination provides probabilistic inference about the signals' dynamics inside the spectrum at multiple levels (discrete and continuous). Diagnostic messages carrying information form observations are used to evaluate how much the observed sensory signals match the predictions. PF relies on a proposal function extracted from (8) to sample a set of particles representing the predicted superstates. At each t, PF propagates L equally weighted particles associated with a certain superstates, such that $\{\tilde{\mathrm{S}}^{l}_{t,f_n}, \mathrm{W}_{t,l}\} \sim \{\pi(\tilde{\mathrm{S}}_{t,f_n}), \frac{1}{L}\}$. Then, a KF is used to predict $\tilde{\mathrm{X}}_{t,f_n}$ for each particle l using the dynamic model defined in (3) which can be expressed as $\mathrm{P}(\tilde{\mathrm{X}}_{t,f_n} | \tilde{\mathrm{X}}_{t-1,f_n}, \tilde{\mathrm{S}}^{l}_{t,f_n})$. In (3), the control vector explains the dynamic flow of the physical signal that depends on the previous state ($\tilde{\mathrm{X}}_{t-1,f_n}$) and the predicted superstate ($\tilde{\mathrm{S}}^{l}_{t,f_n}$), such that $\mathrm{U}_{\tilde{\mathrm{S}}_{t,f_n}} = \dot{\mu}_{\tilde{\mathrm{S}}^{l}_{t,f_n}}$. The predictive message is described by the posterior probability expressed as:

$$\begin{aligned} \pi(\tilde{\mathrm{X}}_{t,f_n}) &= \mathrm{P}(\tilde{\mathrm{X}}_{t,f_n}, \tilde{\mathrm{S}}^{l}_{t,f_n} | \tilde{\mathrm{Z}}_{t-1,f_n}) \\ &= \int \mathrm{P}(\tilde{\mathrm{X}}_{t,f_n} | \tilde{\mathrm{X}}_{t-1,f_n}, \tilde{\mathrm{S}}_{t,f_n}) \lambda(\tilde{\mathrm{X}}_{t-1,f_n}) d\tilde{\mathrm{X}}_{t-1,f_n}, \end{aligned} \tag{9}$$

where $\lambda(\tilde{\mathrm{X}}_{t-1,f_n}) = \mathrm{P}(\tilde{\mathrm{Z}}_{t-1,f_n} | \tilde{\mathrm{X}}_{t-1,f_n})$. After receiving the current sensory signals, posterior can be updated according to $\mathrm{P}(\tilde{\mathrm{X}}_{t,f_n}, \tilde{\mathrm{S}}^{l}_{t,f_n} | \tilde{\mathrm{Z}}_{t,f_n}) = \pi(\tilde{\mathrm{X}}_{t,f_n}) \lambda(\tilde{\mathrm{X}}_{t,f_n})$. Accordingly, the diagnostic message $\lambda(\tilde{\mathrm{S}}^{l}_{t,f_n}) = \lambda(\tilde{\mathrm{X}}_{t,f_n}) \mathrm{P}(\tilde{\mathrm{X}}_{t,f_n} | \tilde{\mathrm{S}}_{t,f_n})$ propagated from the observation level towards the top level (through the medium level) can be used to update the belief in the hidden superstates by updating the particles' weights according to $\mathrm{W}_{t,l} = \mathrm{W}_{t,l} \lambda(\tilde{\mathrm{S}}^{l}_{t,f_n})$.

D. Jammer detection

The predictive and diagnostic reasoning introduced in the previous section can be used to estimate a joint posterior at multiple levels. An additional process can be done to evaluate the similarity between the two messages arriving at a given node to estimate the abnormality indicator using a probabilistic distance. We employ the Bhattacharyya distance to calculate the difference between π and λ arriving at node $\tilde{\mathrm{X}}_{t,f_n}$ and defined as:

$$\Upsilon_{\tilde{X}_{t,f_n}} = -\ln\Bigg(\mathcal{BC}\big(\pi(\tilde{X}_{t,f_n}), \lambda(\tilde{X}_{t,f_n})\big)\Bigg) \tag{10}$$

where $\mathcal{BC}(.) {=} \int \sqrt{\pi(\tilde{X}_{t,f_n}) \lambda(\tilde{X}_{t,f_n})} d\tilde{X}_{t,f_n}$ is the Bhattacharyya coefficient. The abnormality indicator defined in (10) allows assessing how much the predictions match the observations and thus permits to detection of any jamming attack.

E. Simulation Results

In this section, simulation results are presented to validate the proposed jammer detection method. As in [18], we adopt the simulation setup for the freeway case introduced by the 3GPP TR 36.885 [19]. We consider $\mathrm{N} = 4$ connected vehicles exchanging positional signals with the BS over N V2I links. Each vehicle's initial position (including the jammer vehicle) is generated randomly over 5 lanes and each vehicle move along the lane following a linear motion and constant velocity as depicted in Fig. 3. The major simulation parameters are defined in Table I.

The BS receives 4 signals of the 4 V2I links each 50ms. Thus, the total time instants considered in the simulation are 600. The GDBN models are learned during the normal situation where the jammer is absent. During the online phase, the BS uses those models to predict what it should receive over each V2I link and detect the presence of the jammer in real time. We tested different scenarios (some examples are depicted in Fig. 4) where the jammer is targeting single or multiple PRBs and performs consecutive attacks in time domain. In order to evaluate the performance of the jammer detection method, we used a range of confidence thresholds

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Carrier Frequency	2GHz
Bandwidth	1.4 MHz
Cell radius	500 m
BS antenna height	25 m
BS antenna gain	8 dBi
BS receiver noise figure	5 dB
Vehicle antenna height	1.5 m
Vehicle antenna gain	3 dBi
Vehicle speed	40 km/h
V2I transmit power	23 dBm
Vehicle jammer transmit power	30 dBm
Noise power	-114 dBm
Simulation time	30 s
Path loss model	$128.1 + 37.6 \log d$
Shadowing distribution	Log-normal
Shadowing standard deviation	8 dB
Fast Fading	Rayleigh fading

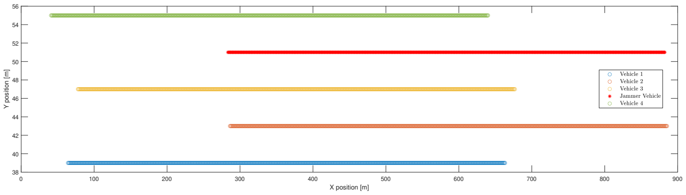
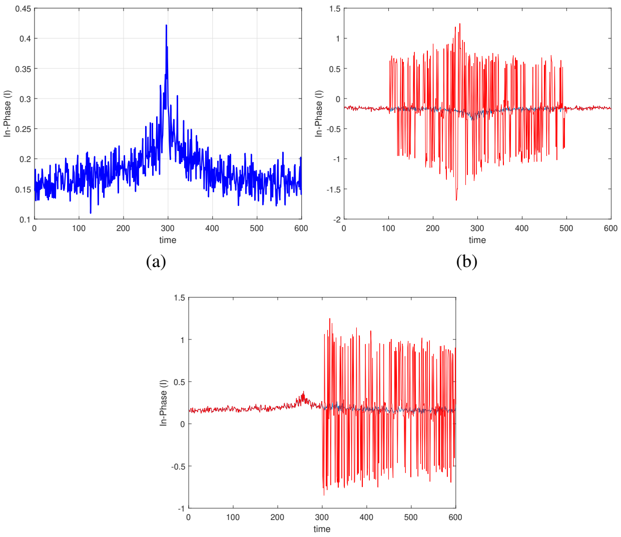


Fig. 3. The simulated environment includes 4 vehicles following a linear motion with constant velocity on different lanes in the presence of a jammer who intend to disturb the V2I communications.



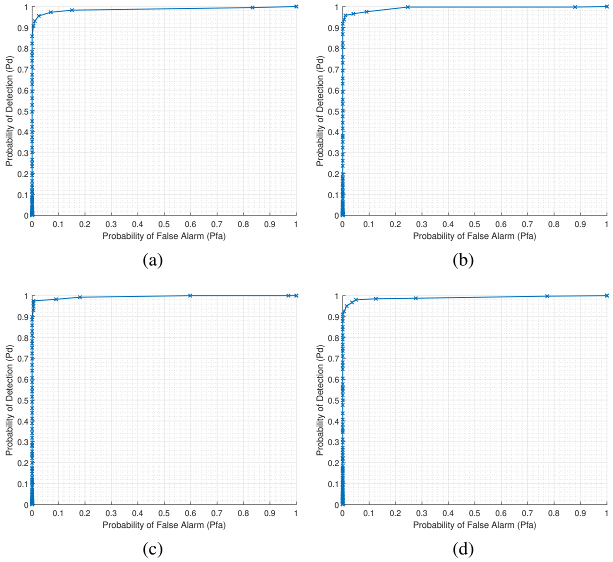
(a)

(b)

(c)

Fig. 4. Examples of three different situations: (a) normal signal over a certain V2I link, b) jammer attacking the V2I from $t = 100$ to $t = 500$, c) jammer attacking the V2I from $t = 300$ to $t = 600$.

to build the corresponding ROC curves. The ROC curves in Fig. 5, shows that the proposed method achieves high detection probability over multiple V2I links with low probability of false alarm. The ROC curves in Fig. 5 are related to the situation where the jammer is attacking all the links in the time interval from $t = 100$ to $t = 500$. While, Fig. 6 is related to a different situation where the jammer is attacking all the V2I links in the time interval from $t = 300$ to $t = 600$. It is to note that the proposed approach allows to detect and locate the jammer in both the time and the frequency domains. Thus, the BS can distinguish which of the V2I links are targeted by the jammer to change the resource allocation and learn an efficient anti-jamming strategy.



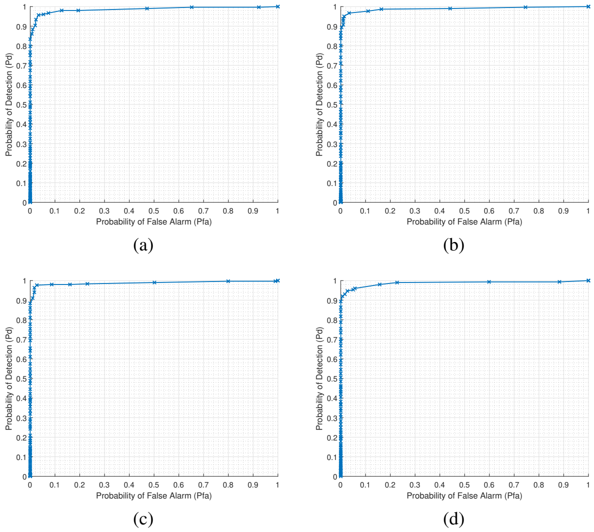
(a)

(b)

(c)

(d)

Fig. 5. In this scenario the jammer attacks all the V2I links from $t = 100$ to $t = 500$. The ROC curves of: (a) first V2I link, b) second V2I link, c) third V2I link, d) fourth V2I link.



(a)

(b)

(c)

(d)

Fig. 6. In this scenario the jammer attacks all the V2I links from $t = 300$ to $t = 600$. The ROC curves of: (a) first V2I link, b) second V2I link, c) third V2I link, d) fourth V2I link.

IV. CONCLUSION AND FUTURE WORK

This paper proposes a Generalized Dynamic Bayesian network (GDBN) based probabilistic switching model that learns a representation of the V2X radio environment and subsequently identifies jammer attacks on vehicular communications between BS and vehicles. Our work was rendered using simulated 4G signals under the duress of large scale and fast fading channel conditions. Furthermore, ROC performance curves were used as the evaluation metric to validate our model. It may be duly noted that the proposed method can detect jamming attacks under reasonable SNR levels. In the future, we aim to realise an urban scenario with higher vehicle distribution density to performance test our model and deal with jammers attacking with low power. We will further design anti-jamming strategies for enhanced physical layer security via self-aware functionalities.

References

[1] Khabaz Sehla, Thi Mai Trang Nguyen, Guy Pujolle, and Pedro Braconnot Velloso. Resource Allocation Modes in C-V2X: From LTE-V2X to 5G-V2X. *IEEE Internet of Things Journal*, pages 1–1, 2022.

[2] Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet of Things Journal*, 5(5):3701–3709, Oct 2018.

[3] Andreas Pressas, Zhengguo Sheng, Peter Fussey, and David Lund. Connected Vehicles in Smart Cities: Interworking from Inside Vehicles to Outside. In *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–3, June 2016.

[4] Mate Boban, Apostolos Kousaridas, Konstantinos Manolakis, Josef Eichinger, and Wen Xu. Connected roads of the future: Use cases, requirements, and design considerations for vehicle-to-everything communications. *IEEE vehicular technology magazine*, 13(3):110–123, 2018.

[5] Shanzhi Chen, Jinling Hu, Yan Shi, Li Zhao, and Wen Li. A Vision of C-V2X: Technologies, Field Testing, and Challenges With Chinese Development. *IEEE Internet of Things Journal*, 7(5):3872–3881, May 2020.

[6] A. Jantošová, J. Morgoš, I. Dolnák, and J. Litvik. A comparative study of the most perspective radio access technologies for vehicular V2X networks. In *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 243–247, Nov 2020.

[7] Shanzhi Chen, Qiang Li, Yong Wang, Hui Xu, and Xiaoyong Jia. C-V2X equipment identification management and authentication mechanism. *China Communications*, 18(8):297–306, Aug 2021.

[8] Oscar Punal, Carlos Pereira, Ana Aguiar, and James Gross. Experimental characterization and modeling of rf jamming attacks on vanets. *IEEE transactions on vehicular technology*, 64(2):524–540, 2014.

[9] Fatih Sakiz and Sevil Sen. A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov. *Ad Hoc Networks*, 61:33–50, 2017.

[10] Luliang Jia, Yuhua Xu, Youming Sun, Shuo Feng, Long Yu, and Alagan Anpalagan. A multi-domain anti-jamming defense scheme in heterogeneous wireless networks. *IEEE Access*, 6:40177–40188, 2018.

[11] Ali Krayani, Mohamad Baydoun, Lucio Marcenaro, Yue Gao, and Carlo S. Regazzoni. Smart Jammer Detection for Self-Aware Cognitive UAV Radios. In *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1–7, Aug 2020.

[12] Sharaf Malebary, Wenyuan Xu, and Chin-Tser Huang. Jamming mobility in 802.11p networks: Modeling, evaluation, and detection. In *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pages 1–7, 2016.

[13] Nalam Venkata Abhishek and Mohan Gurusamy. Jade: Low power jamming detection using machine learning in vehicular networks. *IEEE Wireless Communications Letters*, 10(10):2210–2214, 2021.

[14] Sunil Kumar, Karan Singh, Sushil Kumar, Omprakash Kaiwartya, Yue Cao, and Huan Zhou. Delimitated anti jammer scheme for internet of vehicle: Machine learning based security approach. *IEEE Access*, 7:113311–113323, 2019.

[15] Nikita Lyamin, Denis Kleyko, Quentin Delooz, and Alexey Vinel. Real-time jamming dos detection in safety-critical v2v c-its using data mining. *IEEE Communications Letters*, 23(3):442–445, 2019.

[16] Ali Krayani, Atm S. Alam, Marco Calipari, Lucio Marcenaro, Arumugam Nallanathan, and Carlo Regazzoni. Automatic Modulation Classification in Cognitive-IoT Radios using Generalized Dynamic Bayesian Networks. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pages 235–240, June 2021.

[17] Ali Krayani, Mohamad Baydoun, Lucio Marcenaro, Atm S. Alam, and Carlo Regazzoni. Self-learning bayesian generative models for jammer detection in cognitive-uav-radios. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pages 1–7, Dec 2020.

[18] Le Liang, Shijie Xie, Geoffrey Ye Li, Zhi Ding, and Xingxing Yu. Graph-Based Resource Sharing in Vehicular Communication. *IEEE Transactions on Wireless Communications*, 17(7):4579–4592, July 2018.

[19] 3GPP TR 36.885. Technical Specification Group Radio Access Network; Study on LTEBased V2X Services; (Release 14). V2.0.0, Jun., 2016.