# Machine Learning and Location Verification in Vehicular Networks

Ullah Ihsan[1], Robert Malaney[1] and Shihao Yan[2]

[1]School of Electrical Engineering & Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia

[2]School of Engineering, Macquarie University, Sydney, NSW 2109, Australia

*Abstract*—Location information will play a very important role in emerging wireless networks such as Intelligent Transportation Systems, 5G, and the Internet of Things. However, wrong location information can result in poor network outcomes. It is therefore critical to verify all location information before further utilization in any network operation. In recent years, a number of information-theoretic Location Verification Systems (LVSs) have been formulated in attempts to optimally verify the location information supplied by network users. Such LVSs, however, are somewhat limited since they rely on knowledge of a number of channel parameters for their operation. To overcome such limitations, in this work we introduce a Machine Learning based LVS (ML-LVS). This new form of LVS can adapt itself to changing environments without knowing the channel parameters. Here, for the first time, we use real-world data to show how our ML-LVS can outperform information-theoretic LVSs. We demonstrate this improved performance within the context of vehicular networks using Received Signal Strength (RSS) measurements at multiple verifying base stations. We also demonstrate the validity of the ML-LVS even in scenarios where a sophisticated adversary optimizes her attack location.

## I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) are a particular type of Intelligent Transportation System (ITS) which utilize communications to assist with various traffic problems. VANETs can function based on vehicle-to-vehicle communication and/or vehicle-to-Road Side Unit (RSU) communication [1]. RSUs are fixed base stations installed at certain locations with an aim to assist VANETs with their operations. An RSU (or a trusted vehicle whose location is *a priori* verified), can also function as a Processing Center (PC). The PC processes the communication data before issuing instructions to the vehicles under its coverage area.

Location information of vehicles is a key ingredient for VANETs. The vehicles usually obtain their location information through Global Navigation Satellite System (GNSS) and/or Global Positioning System (GPS), and report this information to the PC for use in subsequent network operations. A possibility exists where the supplied location information from the vehicle has errors in it. This may be due to some faulty hardware used in recording/forwarding the location information, or it may be due to a vehicle falsifying its location information (in order to have advantage over nearby vehicles or to simply disrupt the network). If the location information supplied by the vehicle is not verified, and the location error goes unnoticed, this may result in poor network outcomes such as traffic queues, traffic congestion, or poor

tolling. In extreme cases, a lack of position verification may lead to catastrophic situations such as vehicle collisions.

In recent years, a number of Location Verification Systems (LVSs) [2]–[11] have been devised to validate the vehicle's supplied location information. These LVSs in general make use of the numerous physical layer properties of the signal (transmitted by the vehicle and measured at the verifying base stations) to verify the vehicle's reported location information. The physical layer properties include Received Signal Strength (RSS), Time of Arrival (ToA) of the signal, and Angle of Arrival (AoA) of the signal. However, all LVSs have a serious limitation in their operation - they normally operate efficiently only for the channel conditions assumed at the time of their design [2]. That is, they normally only function well under the assumption that all *a priori* channel information provided to them remains accurate. Further, they are only able to efficiently address the threat-model scenarios they have been specifically designed for [12]. Such limitations make their real-world deployment suspect.

Machine Learning (ML) is an important technology which is now impacting many applications e.g., [13]–[19], and it is possible that inclusion of ML techniques may help resolve some of the LVS limitations mentioned above. Indeed, this has been shown to be the case in theoretical simulations of LVSs in the context of ToA schemes [20], and in theoretical simulations of 'in-region' location verification [21]. What remains to be determined is whether these advances hold up under conditions where real-world data is input to the ML-LVS. In this work, which represents the first experimental deployment of any ML-LVS, we answer this question in the affirmative. We summarize below our main contributions.

- We carry out for the first time an ML-LVS analysis based on real-world data, namely RSS measurements.
- We show that our ML-LVS outperforms an information-theoretic LVS when a malicious vehicle sets its claimed (untrue) location at some random location.
- We also show that unlike the information theoretic LVS, the ML-LVS still performs efficiently even when the malicious vehicle formally minimizes spoofing detection by optimizing its claimed (untrue) location.

The remainder of this paper is organized as follows. Section II details the system model. Section III presents the performance analysis using information theory and ML techniques. Section IV provides numerical results and future prospects, and Section V concludes the paper.

## II. SYSTEM MODEL

We consider the following system model in our work:

1) The true location of a legitimate or malicious vehicle is denoted by $\mathbf{x}_t = [x_t, y_t]$.
2) We refer to the reported location from a legitimate or malicious vehicle as the *claimed location*, which is denoted by $\mathbf{x}_c = [x_c, y_c]$. The claimed location for a legitimate vehicle is exactly the same as its true location. On the other hand, a malicious vehicle spoofs its location, *i.e.*, its claimed which is not the same as its true location.
3) For a malicious vehicle $||\mathbf{x}_c - \mathbf{x}_t|| \geq r$, where $r$ is an *a priori* distance representing the minimum distance between its claimed and true locations.
4) The framework consists of $N$ RSUs as verifying base stations, with publicly known true locations. All RSUs are in the transmission range of the vehicles (whose claimed locations have to be verified). The true location of the *i*-th RSU is $\mathbf{x}_i = [x_i, y_i]$ where $i = 1, 2, ..., N$.
5) We choose one of the RSUs as PC. The PC accumulates its own RSS measurements with the measurements collected by other RSUs for further processing. The PC decides on the integrity of a vehicle's claimed location.
6) Under the null hypothesis $\mathcal{H}_o$, the vehicle is legitimate, *i.e.*, we have

$$\mathcal{H}_o : \mathbf{x}_c = \mathbf{x}_t. \tag{1}$$

7) Under the alternative hypothesis $\mathcal{H}_1$, the vehicle is malicious, *i.e.*, we have

$$\mathcal{H}_1 : \mathbf{x}_c \neq \mathbf{x}_t. \tag{2}$$

Based on a log-normal pathloss model, under $\mathcal{H}_o$, the RSS (all RSS in dBm) measured by the *i*-th RSU from a legitimate vehicle, $y_i$, is given by

$$y_i = u_i + w_i, \qquad i = 1, 2, \ldots, N, \tag{3}$$

where $w_i$ is a zero mean normal random variable with variance $\sigma_T^2$ representing the channel noise, and $u_i$ is the mean RSS at *i*-th RSU. This latter quantity is given by

$$u_i = p_{d_o} - 10\,\gamma\,\log_{10}\left(\frac{d_i^c}{d_o}\right), \tag{4}$$

where $p_{d_o}$ is a reference RSS at a reference distance $d_o$, $\gamma$ is the path loss exponent, and $d_i^c$ is the distance of a legitimate vehicle's true location to the *i*-th RSU, given by

$$d_i^c = \sqrt{(x_c - x_i)^2 + (y_c - y_i)^2}.$$

The measurements made by the $N$ RSUs are independent of each other. Under $\mathcal{H}_o$, they collectively form a vector $\mathbf{y} = [y_1, y_2, \ldots, y_N]^T$. Based on (3) the vector $\mathbf{y}$ follows a multi-variate normal distribution given as

$$f(\mathbf{y}|\mathcal{H}_o) \sim \mathcal{N}(\mathbf{u}, \Sigma), \tag{5}$$

where $\mathbf{u} = [u_1, u_2, \ldots, u_N]^T$ is the mean RSS vector under $\mathcal{H}_o$, and $\Sigma = \sigma_T^2 \mathbf{I}_N$ is the covariance matrix with $\mathbf{I}$ as the identity matrix.

Under $\mathcal{H}_1$, a malicious vehicle spoofs its claimed location. It reports its claimed location to be at a minimum distance $r$ away from his true location. As an example scenario - we can think of the malicious vehicle pretending to be on the road while it actually is placed off in a nearby street. The RSS value measured by the *i*-th RSU from a malicious vehicle, $y_i$, is given by

$$y_i = v_i + w_i, \qquad i = 1, 2, \ldots, N, \tag{6}$$

where $v_i$ is given by

$$v_i = p_{d_o} - 10\,\gamma\,\log_{10}\left(\frac{d_i^t}{d_o}\right), \tag{7}$$

and $d_i^t$ is the distance of its true location to the *i*-th RSU, given by

$$d_i^t = \sqrt{(x_t - x_i)^2 + (y_t - y_i)^2}.$$

The measurements made by $N$ RSUs are independent of each other. Under $\mathcal{H}_1$, they collectively form a vector $\mathbf{y} = [y_1, y_2, \ldots, y_N]^T$. From (6), vector $\mathbf{y}$ follows a multi-variate normal distribution given as

$$f(\mathbf{y}|\mathcal{H}_1) \sim \mathcal{N}(\mathbf{v}, \Sigma), \tag{8}$$

where $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$ is the mean RSS vector under $\mathcal{H}_1$.

## III. PERFORMANCE ANALYSIS

The outcome of an LVS is a binary result i.e. legitimate or malicious. This is different from a localization system where the output is an estimated location. We measure the performance of our LVS using two methodologies; through information theoretic analysis similar to [22] and, through the newly designed ML-LVS method which makes use of machine-learning techniques. In both the cases, a Bayes average cost function is chosen as the performance metric for LVS in terms of 'Total Error'. The Total Error is given by

$$\xi = p(\mathcal{H}_o)\alpha + p(\mathcal{H}_1)(1 - \beta), \tag{9}$$

where $p(\mathcal{H}_o)$ and $p(\mathcal{H}_1)$ are the *a priori* probabilities of occurrences of $\mathcal{H}_o$ (i.e. legitimate vehicle) and $\mathcal{H}_1$ (i.e. malicious vehicle), respectively. In this work, we assume the legitimate and the malicious vehicles in equal proportions so both $p(\mathcal{H}_o)$ and $p(\mathcal{H}_1)$ are equal to 0.5. $\alpha$ represents the False Positive Rate (the rate of legitimate vehicles being detected incorrectly) and $\beta$ represents the Detection Rate (the rate of malicious vehicles being detected correctly). Equation (9) therefore takes the form

$$\xi = 0.5\alpha + 0.5\,(1 - \beta). \tag{10}$$

## A. Information-theoretic LVS

We will refer to the information-theoretic analysis as the Likelihood Ratio Test (LRT) method from now on. The LRT method requires some parameters and channel information to be available in advance. This information includes the pathloss exponent $\gamma$, the mean RSS vectors as highlighted in the system model, and the LRT decision threshold $\ell$, It has been proven elsewhere that the LRT method achieves the optimum detection results for a given false positive rate [23]. This leads to the conclusion that the LRT minimizes the Total Error and maximizes the mutual information between input and output of the LVS [24]. We follow decision rule given below for the LRT method

$$\Lambda\left(\mathbf{y}\right) \triangleq \frac{p(\mathbf{y}|\mathcal{H}_1)}{p(\mathbf{y}|\mathcal{H}_o)} \mathop{\gtrless}\limits_{\mathcal{D}_0}^{\mathcal{D}_1} \ell, \tag{11}$$

where $\Lambda\left(\mathbf{y}\right)$ is the likelihood ratio, and $\mathcal{D}_1$ and $\mathcal{D}_0$ are the binary decision values (*i.e.*, whether the vehicle is legitimate or malicious), while $p(\mathbf{y}|\mathcal{H}_o)$, and $p(\mathbf{y}|\mathcal{H}_1)$ are given by

$$p(\mathbf{y}|\mathcal{H}_o) = \frac{1}{\sqrt[k]{2\pi}\sqrt{|\Sigma|}} e^{-\frac{1}{2}(\mathbf{y}-\mathbf{u})\Sigma^{-1}(\mathbf{y}-\mathbf{u})}, \tag{12}$$

$$p(\mathbf{y}|\mathcal{H}_1) = \frac{1}{\sqrt[k]{2\pi}\sqrt{|\Sigma|}} e^{-\frac{1}{2}(\mathbf{y}-\mathbf{v})\Sigma^{-1}(\mathbf{y}-\mathbf{v})}, \tag{13}$$

where $|\Sigma|$ is determinant of $\Sigma$. The decision rule given in (11) can be reformulated as

$$\Lambda\left(\mathbf{y}\right) \triangleq \frac{e^{-\frac{1}{2}(\mathbf{y}-\mathbf{v})\Sigma^{-1}(\mathbf{y}-\mathbf{v})}}{e^{-\frac{1}{2}(\mathbf{y}-\mathbf{u})\Sigma^{-1}(\mathbf{y}-\mathbf{u})}} \mathop{\gtrless}\limits_{\mathcal{D}_0}^{\mathcal{D}_1} \ell. \tag{14}$$

We assume that the malicious vehicle optimizes its claimed location. That is, through an optimization strategy, it minimizes its probability of being detected by the LVS. We assume in this work that the malicious vehicle's optimum claimed location is constrained to be within the transmission range of the RSUs. To optimize its claimed location under such a constraint, the malicious vehicle minimizes the KL divergence between $f(\mathbf{y}|\mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_o)$ [25]. This divergence is as given below

$$D_{KL}(f(\mathbf{y}|\mathcal{H}_1)||f(\mathbf{y}|\mathcal{H}_0)) = \int_{-\infty}^{\infty} f(\mathbf{y}|\mathcal{H}_1) \ln \frac{f(\mathbf{y}|\mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} d\mathbf{y},$$
$$= \frac{1}{2}(\mathbf{v}-\mathbf{u})^T \Sigma^{-1}(\mathbf{v}-\mathbf{u}). \tag{15}$$

Then, the optimal claimed location $\mathbf{x}_c^*$ for the malicious vehicle can be obtained through

$$\mathbf{x}_c^* = \mathop{\mathrm{argmin}}\limits_{||\mathbf{x}_t-\mathbf{x}_c||\geq r} D_{KL}(f(\mathbf{y}|\mathcal{H}_1)||f(\mathbf{y}|\mathcal{H}_0)). \tag{16}$$

## B. ML-LVS

This section highlights the novel approach used to design a classification framework for the verification of a vehicle's claimed location through supervised ML techniques. Feed-forward neural networks are well known for their performance in classification problems. We use a multi-layer feed-forward neural network for the binary classification of a vehicle as either legitimate or malicious.

The framework considers $\mathbf{y}$ (the RSS observation vector measured in the field) and the vehicle's claimed location as inputs. Based on a series of trials with changing architectures for the ML-LVS, we decided upon a framework that has the raw inputs (RSS, claimed locations, and RSUs locations), a 10-neuron hidden layer, and a 1-neuron binary output layer. We also experimented with different transfer functions in various layers of the ML-LVS. The results shown in the next section adopted the hyperbolic tangent-sigmoid transfer function in the hidden layer and the linear transfer function in the output layer. The ML-LVS utilized the Levenberg-Marquardt as its backpropagation algorithm.

## IV. NUMERICAL RESULTS

RSS measurements from the vehicles were collected in a 150 X 150 meters area by 3 RSUs (an area that mimics a wide cross section of 2 highways). 3 devices were used as 3 RSUs to independently measure the RSS from the vehicles in the field at a frequency of 1 Hz simultaneously, *i.e.*, one RSS measurement per second per RSU. The origin of the area is set to the location of RSU-1 as shown in Fig. 1. Moving Wi-Fi modems with a single antenna and an attached GPS (used to record the vehicle's location at a frequency of 1 Hz) was used to mimic slow-moving vehicles. The GPS locations of these 'vehicles' are reported to the RSUs every second. The RSS measurements by individual RSUs and the vehicles' GPS locations were combined with the help of time stamps (available with both the measured RSS and the vehicles' GPS locations).

The pathloss exponent $\gamma$ is required for the LRT, and is determined directly from the field measurements via a linear fit of the measured RSS values against the logarithm of the distance to a RSU. $\mathbf{u}$ and $\mathbf{v}$ are calculated using (4) and (7) under the corresponding hypothesis. $\sigma_T$ is calculated using the mean RSS vector and the RSS measurements (made by each RSU).

The RSS measurements data is randomized and equally divided it into two halves with one half representing the legitimate vehicles and the other half representing the malicious vehicles. To launch a location-spoofing attack, the malicious vehicles spoof their locations by a minimum distance of $r$ meters away from their true locations. Random claimed locations for the malicious vehicles are simulated by taking into account the distance constraint $r$. Fig. 1 highlights true and simulated random claimed locations for a sample of the malicious vehicles.

We now present some numerical results based on our analysis from the LRT and ML-LVS. In Fig. 2, we assume that the malicious vehicles *randomly* forge their claimed locations at a minimum distance $r$ away from their true locations and within the transmission range of the RSUs. The Total Error is plotted against the number of training data used. For the LRT based LVS, we calculate the Total Error, the false positive rate, and the detection rate under different values of $r$ using (10) and (14). The Total Error for $r$ equal to 100m, 75m and 50m, is 0.05, 0.22, and 0.29, respectively (different colored-dashed arrows).
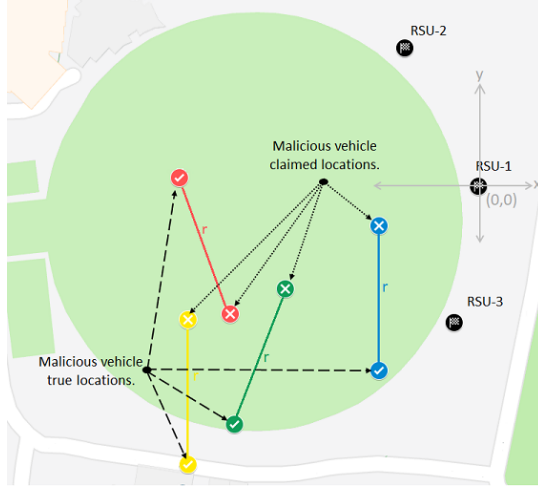
Fig. 1. Malicious vehicles fake their locations to launch a location-spoofing attack. They report their claimed locations $r$ meters away from their respective true locations. This figure only shows a sample of the malicious vehicles' true locations, their simulated random claimed locations at $r$ meters, and the true locations for the RSUs. The value of $r$ in this figure is 50 meters.

The data considered for the LRT based LVS in Fig. 2 is also considered for the ML-LVS. Unlike the LRT method where the LVS requires *a priori* information for the channel parameters, the ML-LVS only uses the measured RSS (at the RSUs) and the vehicles' reported claimed locations. This data which has genuine and malicious vehicles in equal proportions is randomized and divided into two data sets; a training set with 80% of the entire data, and a test set with the remaining 20% of the data. The training set also has data labels (genuine or malicious). These data labels indicate whether particular training sample represents a legitimate or malicious vehicle. Use of such data is required to set the weights and biases for the ML-LVS in the training phase. On the other hand, the data in the test set has no such labels which means that we have no *a priori* information if a particular sample belongs to a legitimate or a malicious vehicle. Once trained, the ML-LVS can be used to test the data in the test set for classification of the vehicles.

In the training phase in Fig. 2, we supply the ML-LVS with training samples from the training data at a rate of one random training sample per unit time and plot the Total Error for the test set after each unit time. The ML-LVS's backpropagation algorithm terminates the training phase once a threshold for any of its internally set parameters is met. We observe that in most cases the 'maximum validation failures' parameter of the backpropagation algorithm (the maximum number of sequential iterations in which the ML-LVS's performance fails to improve) is reached, and this terminates the training phase. We set this parameter to 6. This trained ML-LVS is then used to classify vehicles in the test set as either legitimate or malicious. This procedure is repeated for each value of the training data shown in Fig. 2. As shown in Fig. 2, as expected, the Total Error for the test set improves as the training continues. The final Total Error
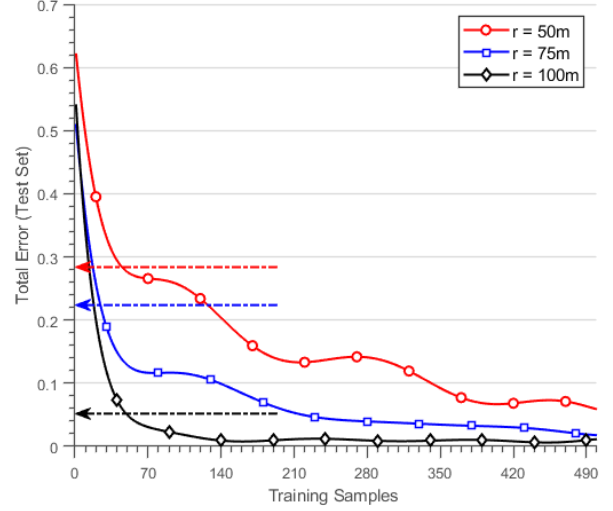


Fig. 2. A comparison study where an ML-LVS outperforms an LRT based LVS. The ML-LVS with no *a priori* channel information achieves a final Total Error (indicated by solid lines) of 0.01, 0.02, and 0.06, for $r$ equal to 100m, 75m, and 50m, respectively, for the data in the test set. On the other hand, the LRT based LVS with *a priori* channel information achieves a Total Error (indicated by dashed arrows) of 0.05, 0.22, and 0.29, for $r$ 100m, 75m, and 50m, respectively, for the data in the test set. Note, in these calculations, the malicious vehicles do not optimize their claimed locations.
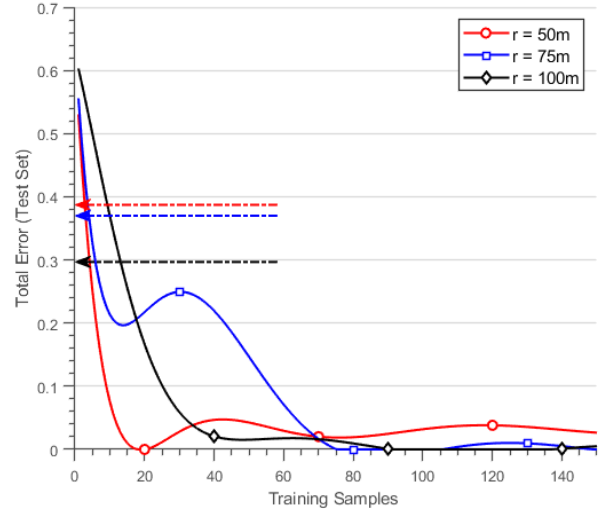


Fig. 3. A comparison study of the LRT based LVS with ML-LVS as in Fig. 2 except the malicious vehicles now optimize their claimed locations.

for the test set (after 500 training samples) using the ML-LVS for $r$ equal to 100m, 75m and 50m, is 0.01, 0.02, and 0.06, respectively. It is evident from Fig. 2 that the ML-LVS with no *a priori* channel information has much-improved performance relative to the LRT based LVS.

We now assume that the malicious vehicles can overhear the communication between the legitimate vehicles and the RSUs. The malicious vehicles use this information to best optimize their claimed locations ($\mathbf{x}_c = \mathbf{x}_c^*$) prior launching a location-spoofing attack. That is, they set their claimed

location using (15) so as to minimize their probability of being marked malicious by the LVS.

In Fig. 3 we compare the performances of the ML-LVS and the LRT based LVS. We see again that the ML-LVS still outperforms the LRT based LVS. However, we notice a rather counter-intuitive finding where, compared to Fig. 2, the Total Error for the ML-LVS improves much faster. This counter intuitive finding is as a result of the geometry of the RSUs in this specific experiment. This geometry leads to a clustering in the malicious vehicles' claimed location settings. In general (*i.e.* more general RSU geometries), if the malicious vehicles' optimize their claimed locations, the Total Error for the ML-LVS is expected to take longer to reach its asymptotic value.

In future work we plan to integrate Support Vector Machines (SVM) into the designed neural-network framework of our ML-LVS. We also plan to deploy this modified ML-LVS in more complex channel fading environments such as those possessing Rician fading channels. These additional studies are likely to provide for even more performance gains in ML-LVSs relative to LRT based LVSs.

## V. CONCLUSION

Information-theoretic LVS frameworks, due to their operating limitations, are not practical in many real-world scenarios. To address this gap, we have proposed the use of a ML approach to location verification. This new approach is particulary useful since unlike an information-theoretic LVS, a ML-LVS does not require *a priori* information on the channel parameters. Additionally, a ML-LVS can adapt itself to any changing channel conditions.

Using real-world RSS data, we have shown for the first time how a deployed ML-LVS outperforms state-of-the-art information-theoretic LVS. Further, we have shown how this result holds even when the adversary optimizes its attack location. Future work in this area will help us develop a fully robust state-of-the-art artificially intelligent LVS, an LVS which will be wholly practical in terms of its location verification performance in a wide range of future wireless networks beyond the networks we have studied here.

We believe the novel approach for enhancing the performance of real-world LVSs that we have developed here potentially forms the foundation for all future works in the important area of wireless location verification.

## VI. ACKNOWLEDGMENT

## REFERENCES

[1] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[2] S. Yan and R. Malaney, "Location verification systems in emerging wireless networks," *ZTE Comms.*, vol. 11, no. 3, pp. 03–10, Jul. 2013.

[3] D. Sheet, O. Kaiwartya *et al.*, "Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks," *IET Intelligent Transportation Systems*, vol. 11, no. 2, pp. 53–60, Mar. 2017.

[4] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Location verification systems for VANETs in Rician fading channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5652–5664, Jul. 2016.

[5] P. Monteiro, J. Rebelatto, and R. Souza, "Information-theoretic location verification system with directional antennas for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 1, pp. 93–103, Jan. 2016.

[6] S. Yan, I. Nevat, G. W. Peters, and R. Malaney, "Location verification systems under spatially correlated shadowing," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4132–4144, Jun. 2016.

[7] F. Malandrino, C. Casetti, C. Chiasserini, M. Fiore, R. Yokoyama, and C. Borgiattino, "A-VIP: Anonymous verification and inference of positions in vehicular networks," in *Proceedings of the IEEE INFOCOM*, Apr. 2013, pp. 105–109.

[8] W. Jaballah, M. Conti, M. Mosbah, and C. Palazzi, "Secure verification of location claims on a vehicular safety application," in *Proceedings of the International Conference on Computer Communication and Networks (ICCCN)*, Aug. 2013, pp. 1–7.

[9] I. Kim, B. Kim, and J. Song, "An efficient location verification scheme for static wireless sensor networks," *Sensors*, vol. 17, no. 2, p. 225, Jan. 2017.

[10] G. Caparra, M. Centenaro, N. Laurenti, and S. Tomasin, "Optimization of anchor nodes' usage for location verification systems," in *Proceedings of the International Conference on Localization and GNSS (ICL-GNSS)*, Jun. 2017, pp. 1–6.

[11] C. Vaas, M. Juuti, N. Asokan, and I. Martinovic, "Get in line: Ongoing co-presence verification of a vehicle formation based on driving trajectories," in *Proceedings of the European Symposium on Security and Privacy (Euro S&P)*, Apr. 2018, pp. 199–213.

[12] B. Yu, C. Xu, and B. Xiao, "Detecting sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[13] M. Abadi, A. Agarwal, P. Barham *et al.*, "Tensorflow: Large-scale machine learning on heterogeneous distributed systems," *arXiv:1603.04467*, Mar. 2016.

[14] J. Wan, D. Wang, S. Hoi *et al.*, "Deep learning for content-based image retrieval: A comprehensive study," in *The ACM International conference on Multimedia*, Nov. 2014, pp. 157–166.

[15] E. Rosten and T. Drummond, "Machine learning for high-speed corner detection," in *The European conference on Computer Vision*. Springer, Jul. 2006, pp. 430–443.

[16] G. Hinton, L. Deng *et al.*, "Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 82–97, Nov. 2012.

[17] S. Irtza, V. Sethu, E. Ambikairajah, and H. Li, "End-to-end hierarchical language identification system," *IEEE SigPort*, Apr. 2018.

[18] P. Matějka, O. Glembek, O. Novotný, O. Plchot, F. Grézl, L. Burget, and J. H. Cernocký, "Analysis of DNN approaches to speaker identification," in *The IEEE International conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2016, pp. 5100–5104.

[19] H. Zen, A. Senior, and M. Schuster, "Statistical parametric speech synthesis using deep neural networks," in *The IEEE International conference on Acoustics, Speech and Signal Processing (ICASSP)*, May. 2013, pp. 7962–7966.

[20] U. Ihsan, Z. Wang, R. Malaney, A. Dempster, and S. Yan, "Artificial intelligence and location verification in vehicular networks," *arXiv:1901.03001*, Jan. 2019.

[21] A. Brighente, F. Formaggio, M. Centenaro, G. M. Di Nunzio, and S. Tomasin, "Location-verification and network planning via machine learning approaches," *arXiv:1811.06729*, Nov. 2018.

[22] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Timing information in wireless communications and optimal location verification frameworks," in *Communications Theory Workshop (AusCTW)*, Feb. 2014, pp. 144–149.

[23] J. Neyman and E. S. Pearson, "IX. On the problem of the most efficient tests of statistical hypotheses," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 231, no. 694-706, pp. 289–337, Feb. 1933.

[24] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Optimal information-theoretic wireless location verification," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.

[25] S. Eguchi and J. Copas, "Interpreting Kullback–Leibler divergence with the Neyman–Pearson lemma," *Journal of Multivariate Analysis*, vol. 97, no. 9, pp. 2034–2040, Oct. 2006.