A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs

Sanaa Taha, *Student Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—A network mobility (NEMO)-based vehicular ad hoc network (VANET) is a new approach to integrate the NEMO protocol with VANETs. This integration supports communications between roadside units (RSUs) and vehicles and provides Internet access through public hotspots located inside public transportation systems, such as buses, trains, and shuttles. Passengers inside these public transportation systems enjoy full Internet access by using different mobile network nodes (MNNs), such as cell phones and personal digital assistants. However, due to the open nature of wireless network environments, physical-layer attackers can easily localize the MNNs by measuring their received signal strength (RSS) through positioning schemes such as the triangulation scheme. In this paper, we modify obfuscation, *i.e.,* concealment, and power variability ideas and propose a new physical-layer location privacy scheme, i.e., the fake point–cluster-based scheme, to prevent attackers from localizing users inside NEMO-based VANET hotspots. The proposed scheme involves fake-point- and cluster-based subschemes, and its goal is to confuse the attackers by increasing the estimation errors of their RSSs measurements and, hence, preserving MNNs' location privacy. Using correctness, accuracy, and certainty metrics, we show that the fake point–cluster-based scheme achieves higher MNN's location privacy when the number of network grid points in the hotspot decreases. In addition, our extensive simulations show that the fake point–cluster-based scheme achieves 23% and 37% decreases in the average sender's power and the MNN-AP route path length, respectively, compared with the fake-point subscheme.**

***Index Terms*—Network mobility (NEMO)-based VANET, NEMO security, physical-layer location privacy, physical-layer security, wireless position estimation attacks.**

I. Introduction

RECENTLY, both academia and industry have shown significant interest in the field of mobility management for vehicular networks achieving seamless communications for mobile nodes (MNs), *i.e.,* vehicles [2]. Mobility management protocols, such as Mobile IPv6 (MIPv6) and network mobility (NEMO) protocols, which are used to guarantee global Internet connectivity and mobile data services for MNs, have been proposed by many consortia and standards organizations, such as the Car-to-Car Communications Consortium [3] and the Internet Engineering Task Force. In addition, industry integrates these mobility management protocols with vehicular ad hoc networks (VANETs) [4] to support intelligent transportation system applications, including Internet access, real-time traffic information, video streaming, and infotainment.

In VANETs, a vehicle that is equipped with an on-board unit (OBU) communicates with other vehicles via a vehicle-to-vehicle (V2V) domain and communicates with a roadside unit (RSU) via a vehicle-to-infrastructure (V2I) domain. V2V and V2I communication domains are mainly for safety VANET applications, such as road accident notifications and weather warnings. In addition, nonsafety VANET applications, such as service infotainment and Internet access, have recently received a great deal of attention, particularly with the proliferation of public hotspots installed inside large vehicles (i.e., buses, trains, or planes).

Having the same goal of supporting global Internet connectivity, mobility management protocols [5] can be classified into host- and network-based mobility. In host-based mobility management protocols, such as MIPv6 [6], the MN manages its own mobility, whereas in network-based mobility protocols, such as Proxy MIPv6 [7], the mobility of an MN is managed by network entities, such as access routers, without involving the MN. In addition, the NEMO protocol [8] is an extension of the MIPv6 protocol to manage the mobility of moving networks as one unit. Therefore, NEMO is suitable for a scenario, such as that shown in Fig. 1, where a Wi-Fi hotspot is deployed in a large van (bus, train, or plane), and it is called a NEMO-based VANET [9]–[12]. In such networks, the OBU inside a vehicle also works as a mobile router (MR) to support a group of mobile network nodes (MNNs) located inside the vehicle with required communications.

However, preserving user location privacy in such a public mobile hotspot for a NEMO-based VANET is a challenge. Violating a mobile user's location privacy may lead, in some cases, to users being injured or losing their lives [13], [14]. More specific to the NEMO-based VANET hotspots, controlling information leakage at the physical layer is important to ensure the user's location privacy in wireless local area networks, even with applying confidentiality to the data-link layer [15]. Due to the open nature of the wireless environment,

Manuscript received February 11, 2013; revised April 24, 2013, May 3, 2013, and May 10, 2013; accepted May 26, 2013. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by the Bureau of Cultural and Educational Affairs of Egypt in Canada. The Associate Editor for this paper was G. Yan.

S. Taha is with the Department of Information Technology, Faculty of Computers and Information, Cairo University, Giza, Egypt (e-mail: staha@uwaterloo.ca).

X. Shen is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: xshen@uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2013.2265311

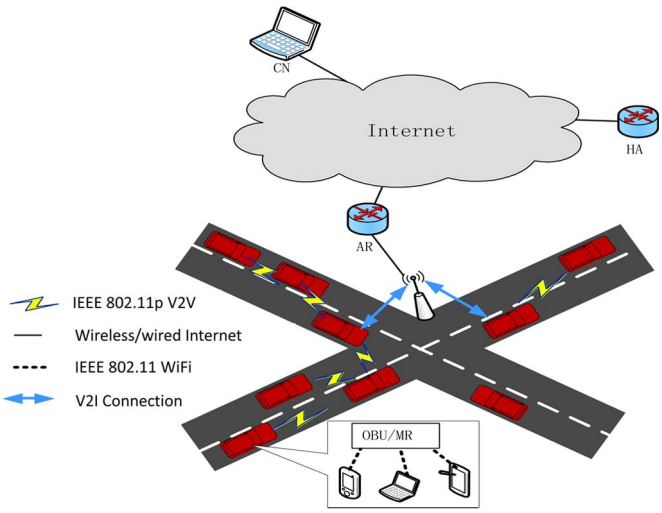

Fig. 1. NEMO-based VANET.

a physical-layer attacker can easily localize users by relating the strength of these users' signals and locations. Being supported with isotropic antennas, which emit signals in all directions, users' mobile devices in hotspots cannot hide their transmitted signals from physical-layer attackers. In addition, with the recent extensive studies that have been done to increase the accuracy of positioning systems used to localize mobile devices in location-based services (LBSs), physical-layer location privacy attacks become more difficult to mitigate as they exploit these high-accuracy positioning systems to localize the victims. Using cheap equipment, such as a received-signal-strength indicator (RSSI), the attacker can easily localize the sender by only acquiring its transmitted wireless signals even if an Internet Protocol (IP)-layer security scheme is implemented [16]. Furthermore, some existing physical-layer location privacy schemes are limited to power variability [17], which uses different power levels in transmitting packets; obfuscation [18], which confuses attackers by replacing real location information with fake location information; and the addition of noise [19], which decreases the accuracy of the sender's localization-to-noise ratio.

Those schemes are not appropriate for NEMO-based VANET hotspots. Power variability schemes have been proven as weak solutions, because attackers can easily reveal the original signals' power. In addition, existing obfuscation schemes disguise the exact user's location by returning to the attacker an expanded area in which the user is located. However, in NEMO-based VANET hotspots, location privacy attackers can get the exact users' locations, rather than an obfuscated area, with the help of the high-accuracy positioning schemes. Furthermore, adding noise to transmitted signals decreases the overall network performance.

In this paper, we evolve the ideas of obfuscation and power variability to propose a strong physical-layer location privacy scheme, i.e., the fake point–cluster-based scheme, which can be used in public hotspots for a NEMO-based VANET. To the best of our knowledge, the fake point–cluster-based scheme is the first to apply obfuscation, *i.e.,* concealing, to a user's location by an exact location rather than a wide area. Unlike existing obfuscation schemes, which are employed in the current LBS, our proposed scheme thwarts such a physical-layer location privacy attacker who tries to exploit the high-accuracy positioning schemes to define the sender's exact location. In addition, unlike current power variability schemes, our scheme changes the signal's power with respect to a specific reference point that we call a fake point; as a result, the impact of power variabilities is difficult to mitigate.

TABLE I
ABBREVIATION DEFINITIONS

d	distance
MNN	Mobile network node
MR	Mobile router
NEMO	Network mobility protocol
OBU	On-board unit
RP_i	Reference point i
RSS	Received signal strength
RSU	Road-side unit
VANET	Vehicula Ad Hoc network

The fake point–cluster-based scheme combines two independent subschemes, i.e., fake point and cluster based. The idea of the fake-point subscheme is that each sender selects and considers a random point inside the hotspot, which is called the fake point, when calculating the packet transmission power. Therefore, when many senders select the same fake point, the attacker's received signal strengths measured for different senders will be equalized, hence confusing the attacker. Thus, the sender's location privacy is protected as the attacker wrongly calculates the sender's location. In addition, the cluster-based subscheme prevents some of the attacker's monitoring devices from detecting the sender's signals, hence decreasing the accuracy of the attacker's positioning system. To analyze our location privacy scheme, we use three different metrics, namely, correctness, accuracy, and certainty. We observe that the probability of an attacker localizing a sender when the fake-point subscheme is employed decreases as the ratio of the number of attacker's monitoring devices to the number of the defined spatial grid points in the network increases. However, since the number of spatial grid points is always much larger than the number of an attacker's monitoring devices, the probability of localizing the sender by an attacker is quite large. Therefore, we combine the proposed cluster-based subscheme with the fake-point subscheme to decrease this probability. In addition, through extensive simulations, we show that our fake point–cluster-based scheme achieves 23% and 37% decreases in the average sender's power and the MNN-AP routing path length, respectively, over the fake-point subscheme because in the fake point–cluster-based scheme, the MNN selects a nearer fake point located in the neighbor cluster. Table I defines the abbreviations used in this paper.

The remainder of this paper is organized as follows. Section II discusses the NEMO-based VANET and wireless position estimation systems as the preliminaries. Section III reviews related work. The system model and the threat model are presented in Section IV. The proposed fake point–cluster-based scheme is introduced in Section V. The security analysis and the performance evaluation are introduced in Sections VI and VII, respectively. Finally, conclusions and future work are presented in Section VIII.

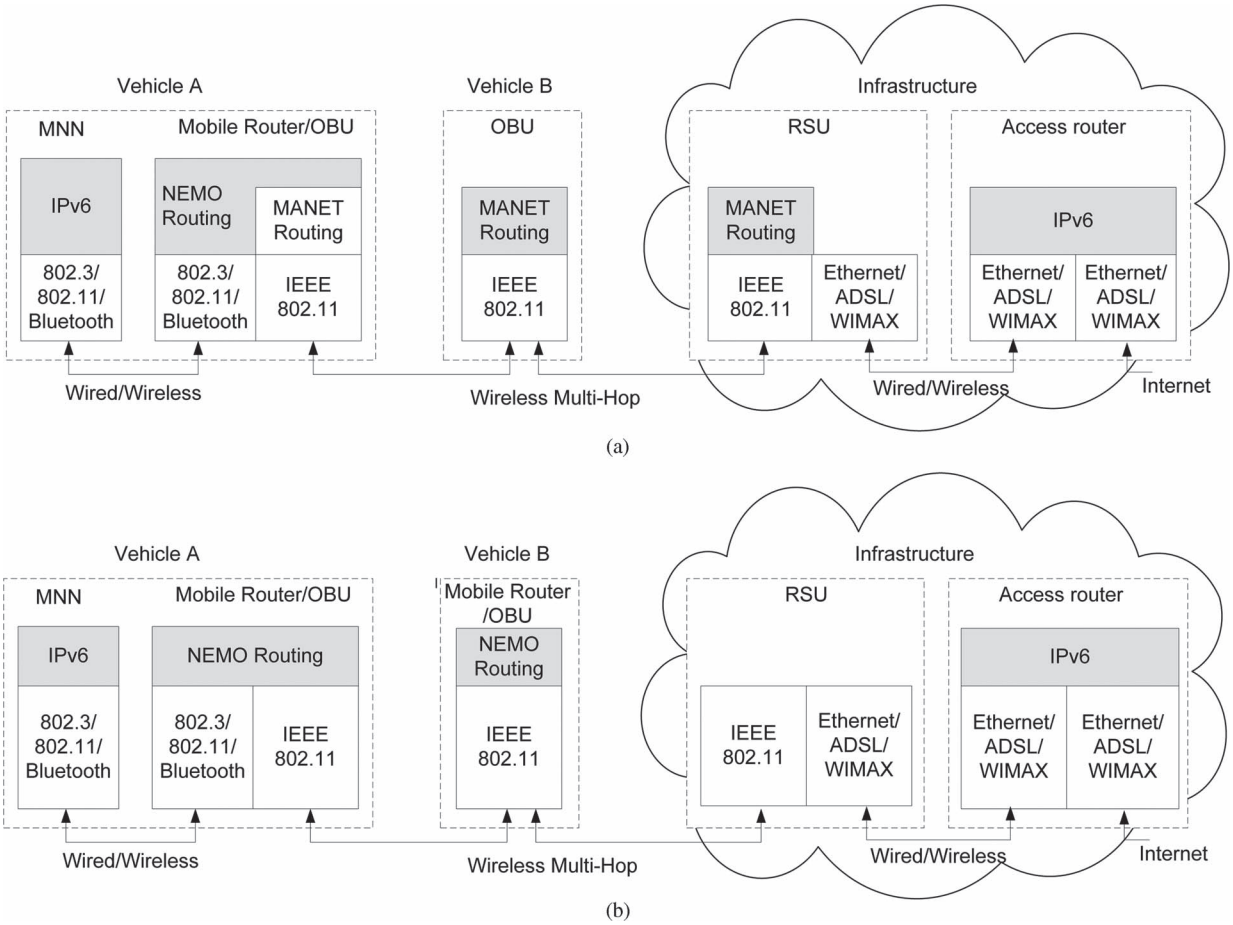

Fig. 2. NEMO-based VANET integration approaches. (a) MANET-centric approach. (b) NEMO-centric approach.

II. Preliminaries

A. NEMO-Based VANET

The NEMO Basic Support (NEMO BS) protocol [20] is the standard protocol to manage mobility in the entire moving network. As an extension of the mobile IP protocol [21], [22], NEMO BS employs mobile IP's basic functionalities, such as the home binding updates; however, these functionalities are performed by the MR rather than the MNNs, which only implement the basic IP protocol without being aware of the entire NEMO.

Supporting the network's MNNs with the required mobility, NEMO BS has some benefits over the MIP protocol, such as reducing signaling overhead and mobility costs. In NEMO BS, the MNNs do not need to implement any mobility protocols, and it is designed to support a single-hop mobile network where there is a direct communication between an MR and the Internet access router. Therefore, to support vehicle-to-vehicle-to-infrastructure (V2V2I), in which the vehicle communicates with the RSU through multihop access, the integration of NEMO with a VANET, namely, NEMO-based VANET, has two roles: 1) supporting session continuity and global Internet access via NEMO BS and 2) supporting multihop communication via V2V2I routing schemes such as georouting [23], [24].

To integrate NEMO BS with a VANET, two approaches have been defined [10], [25], i.e., mobile ad hoc network (MANET)-centric and NEMO-centric. The difference between the two approaches relates to the way of implementing the intermediate vehicles (Vehicle B in Fig. 2) that contribute in the V2V2I multihop communications. Fig. 2(a) shows the MANET-centric approach, in which the intermediate vehicle does not need to implement a NEMO BS protocol; rather, only a MANET routing protocol is employed, while the sender vehicle [Vehicle A in Fig. 2(a)] implements the NEMO protocol on top of the MANET routing protocol. The separation of the two protocols' implementations is the advantage of this approach, which, in turn, decreases the complexity of NEMO-based VANETs. On the other hand, Fig. 2(b) shows the NEMO-centric approach, in which multihop communications are created by implementing the NEMO BS on both the intermediate and sender vehicles. In addition to working as an MR, each OBU in the intermediate V2V2I communication path also works as a gateway for the moving-network's MR. The NEMO-centric approach is more appropriate for nested NEMO and hierarchical structured networks, whereas the MANET-centric approach is more suitable for our scenario, in which the ad hoc structure is implemented in the multihop communication.

B. Wireless Position Estimation

Our threat model relates to a location privacy attacker who exploits positioning estimation systems [26] to reveal a

sender's physical location from the received signal strength (RSS). Therefore, here, the wireless positioning estimations are illustrated in more detail to more deeply understand the attacking strategy. Moreover, the two steps of the wireless position estimation process, i.e., distance measurement and location estimation, are described in detail.

The goal is to accurately estimate the mobile user's location inside a wireless network, such as Wi-Fi or a cellular network, when the user transmits signals. Starting with the distance measurement step, the mobile user's signal parameters are measured, and the distances to the sender are estimated at certain reference points distributed across the network. RSS, time of arrival, time difference of arrival, and angle of arrival are examples of the signal parameters. From the attacker's perspective and unlike other signal parameters, the RSS measurement is the best to use as it requires only inexpensive equipment, such as the RSSI [26]. Therefore, here, we focus on RSS-based estimation, in which each reference point at distance d from the mobile user measures the received signal power, i.e., $\bar{p}(d)$, as

$$\bar{P}(d) = P_0 - 10n\log(d/d_0) \tag{1}$$

where P_0 is the received signal power from a known location that is located at distance d_0 from the reference point, and n is the path loss exponent, which depends on the propagation model of the signal in the wireless environment. In addition to the path loss, the received power is also affected by both shadowing and fast fading (mutipath). In practice, with a long time interval of signal observation, the effect of the multipath on the propagated signal is excluded. Therefore, the received power is modeled to include the path loss modeled in (1) and the shadowing modeled as a zero-mean Gaussian random variable with variance σ^2 to consider the variability of the signal fading conditions. The RSS measurement can be modeled as

$$P(d) \sim N\left(\bar{P}(d), \sigma^2\right). \tag{2}$$

After measuring the RSS at reference point i located in (x_i, y_i), the estimated distance to the sender, i.e., $f_i(x, y)$, is measured as

$$f_i(x, y) = \sqrt{(x - x_i)^2 + (y - y_i)^2}. \tag{3}$$

In the second step, i.e., location estimation, two techniques for location estimation are defined: 1) mapping (fingerprinting) and 2) geometric and statistical. The mapping techniques rely on an off-line training phase in which a database of different RSS estimations and their correspondent senders' locations is created. Depending on the training phase, a mapping method is used to match a new measured RSS value to entities in the database. In our NEMO-based hotspot, we assume that attackers cannot perform the training phase. Alternatively, the geometric and statistical techniques can be used. In geometric techniques, the position of the MN can be estimated as the intersection of position circles obtained from RSS measurements that are estimated at different reference points. Since each RSS forms a circle, at least three reference points are needed to define the intersection point. In addition, using the statistical techniques, the location of the MN can be defined as

$$Z = f(x, y) + \eta \tag{4}$$

where $Z = [Z_1, Z_2, \ldots, Z_N]^T$, $f(x, y) = [f_1(x, y), f_2(x, y), \ldots, f_N(x, y)]^T$, and $\eta = (\eta_1, \eta_2, \ldots, \eta_N)^T$ are the parameters collected from each reference point i as

$$Z_i = f_i(x, y) + \eta_i, \qquad i = 1, 2, \ldots, N \tag{5}$$

where N is the number of reference points, $f_i(x, y)$ is the distance that reference point i estimates for the sender location (x, y) by using the measured RSS value as in (3), and η_i is the estimation error at this reference point.

After collecting the estimated distances from all reference points, a general estimation $\theta = [x, y]^T$ of an MN's location is calculated using (3). In addition, based on the knowledge of the probability density function (pdf) of the estimation error, i.e., η, parametric or nonparametric techniques can be used. Nonparametric techniques such as fingerprinting are employed if the error's pdf is not defined, whereas parametric techniques such as Bayesian and maximum-likelihood (ML) estimators are used when the error's pdf is known. The Bayesian approach is used in the presence of *a priori* probability of θ, i.e., $\pi(\theta)$, to minimize the cost function of estimating θ by using either the minimum mean square error (MMSE), i.e., $\hat{\theta}_{\mathrm{MMSE}}$, or the maximum posterior (MAP) estimations, i.e., $\hat{\theta}_{\mathrm{MAP}}$, as

$$\hat{\theta}_{\mathrm{MMSE}} = E\{\theta \mid Z\} \tag{6}$$

$$\hat{\theta}_{\mathrm{MAP}} = \arg\max_{\theta} P(Z \mid \theta)\pi(\theta). \tag{7}$$

On the other hand, ML estimation is used when $\pi(\theta)$ is unknown, to maximize the likelihood function. Thus

$$\hat{\theta}_{\mathrm{ML}} = \arg\max_{\theta} P(Z \mid \theta) \tag{8}$$

$$P(Z \mid \theta) = P_{\eta}\left(Z - f(x, y) \mid \theta\right) \tag{9}$$

where P_{η} is the conditional pdf of an estimation error condition on θ.

In RSS-based estimation, the error vector is assumed to be independent and is modeled as a zero-mean Gaussian. Therefore, (9) can be written as

$$P(Z \mid \theta) = \prod_{i=1}^{N} P_{\eta_i}\left(Z_i - f_i(x, y) \mid \theta\right) \tag{10}$$

$$P_{\eta_i} = \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(-\frac{\eta_i^2}{2\sigma_i^2}\right) \tag{11}$$

$$P(Z \mid \theta) = \frac{1}{(2\pi)^{N/2}\prod_{i=1}^{N}\sigma_i} \exp\left(-\sum_{i=1}^{N}\frac{\eta_i^2}{2\sigma_i^2}\right). \tag{12}$$

Hence, the ML estimator can be calculated as

$$\hat{\theta}_{\mathrm{ML}} = \arg\min_{[x,y]^T} \sum_{i=1}^{N} \frac{\left(Z_i - f_i(x, y)\right)^2}{\sigma_i^2}. \tag{13}$$

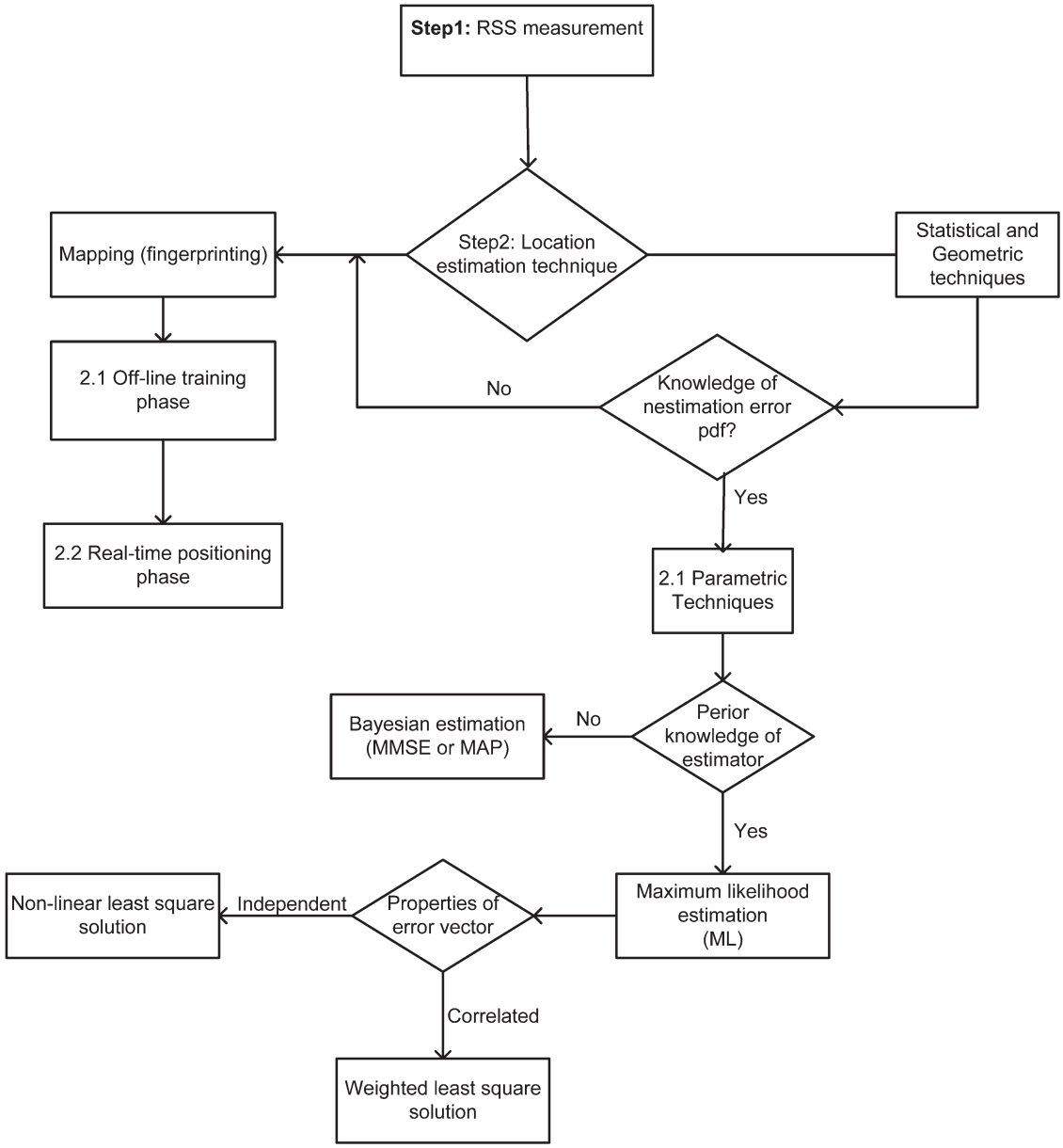

Fig. 3. Wireless position estimation.

However, if we assume correlated Gaussian error components instead of independent components, the estimated ML can be written as

$$\hat{\theta}_{\mathrm{ML}} = \arg \min_{[x,y]^T} \left(Z - f(x,y)\right)^T \Sigma^{-1} \left(Z - f(x,y)\right). \quad (14)$$

Fig. 3 shows the flowchart of an RSS-based positioning system.

III. Related Works

Due to the open nature of wireless networks, hiding the transmitted wireless signals and, hence, achieving physical-layer location privacy is considered as a challenging goal. In location privacy attacks, the attacker localizes the victim MNN by measuring its RSSs at certain reference points, as illustrated in Section II-B. To thwart these attacks, in [17], employing a scheme in sensor networks called Hyberloc is suggested. In this scheme, the anchor nodes protect their location from untrusted nodes, whereas trusted nodes can easily localize those anchor nodes. The main idea of Hyberloc is to choose and attach a random power value, which is used in transmitting signals, to the transmitted encrypted packets. Therefore, having a shared key, only trusted nodes can identify the true sender's location. However, changing the transmission power values is considered to provide only weak location privacy because the attacker can easily fix these changes by multiplying the RSS at all monitoring devices by a factor. In our proposed scheme, in addition to changing power levels as is done in Hyberloc, we confuse the attacker's monitoring devices by letting their measured RSSs be equalized for different MNNs; therefore, it becomes difficult for the attacker to mitigate the increase in power.

Another scheme, i.e., hidden anchor, which relies on adding noise to the transmitted signals, is proposed in [19]. In this

scheme, the anchor nodes use their neighbors' identities to hide their own identities from distrusted nodes and, at the same time, encrypt and attach their real identities in the transmitted packets sent to trusted nodes. However, changing the nodes' identities does not achieve a sender's physical-layer privacy; rather, it helps in achieving link-layer location privacy. In addition, both anchor and trusted nodes add noise to their transmitted messages to prevent untrusted nodes from measuring the RSSs and revealing their locations. However, adding noise to the transmitted messages affects transmission quality.

Obfuscation, *i.e.,* concealment, which is proposed in [18], is another way to protect a user's location privacy from location-based servers (LBSs). The idea of obfuscation is to replace real location information with fake information to decrease the accuracy of the localization process employed by LBS and, hence, increase a user's location privacy. Three obfuscation techniques are proposed in [18], i.e., enlarged area, shifted center, and reduced radius. In location-based applications, the user's location returned to the LBS represents an area rather than a specific location; therefore, obfuscation schemes are used to hide the true information about that area. However, these obfuscation schemes are not appropriate for Wi-Fi scenarios in which the adversary gets a specific MNN's location rather than an area. In our proposed scheme, we modify the idea of obfuscation to return a wrong location point rather than a wide area.

With the goal of achieving obfuscation for users' information, in [27], user identity, time, and location obfuscation are achieved. User identity obfuscation, i.e., concealing the identity, is carried out by frequently changing a user's pseudonymity, whereas time obfuscation, i.e., concealing transmission time, is carried out by applying a silent period to thwart pseudonym correlation attacks. The silent period is defined in such a way as to increase a user's privacy level and, hence, decrease the positioning systems' accuracy. Unlike identity and time obfuscation that are mainly employed for link-layer obfuscation, location obfuscation is employed to achieve physical-layer location privacy. Considering a fingerprinting positioning system, in [27], location obfuscation is achieved by proposing a silent transmit power control (TPC) scheme that reduces the transmission power at each user. Therefore, the number of APs that detect the transmitted signals decreases, as does the accuracy of the attacker's localization. The challenge of silent TPC is to allow users to change their transmission power without exchanging any information with their APs. Our proposed cluster-based scheme employs the same idea of TPC to reduce a user's transmission power. However, unlike our proposed scheme, the silent TPC scheme considers location attackers located only in neighbor networks rather than those located in the user's current network.

In [28], two strategies for a user's location privacy have been proposed with a main idea of using a smart antenna that emits a directional radiation pattern instead of using isotropic antennas. In the first strategy, i.e., using a smart antenna, the MNN maximizes the transmission power of the signals directed to the AP located in its network while preventing other APs from receiving any signals transmitted from this MNN. Therefore, other APs cannot triangulate this MNN and, hence, fail to reveal its location. On the other hand, if an MNN fails to prevent at least four APs from receiving its signals, then the MNN tries the second strategy in which the MNN maximizes the RSS localization bias at the APs around this MNN. By increasing the localization bias, the MNN guarantees that its surrounding APs estimate its position incorrectly. To achieve the first strategy, the MNN first listens to the periodically received beacon packets that are transmitted by the nearby APs. The MNN then passively measures the RSSs of these beacon packets to estimate the APs' locations. However, if the APs change their power levels, then the MNN cannot estimate their locations and, hence, fails to protect this MNN's location privacy. In addition, the assumption of having a smart antenna in all MNNs is not reasonable due to their high cost.

In [29], a scheme called silent period is used to achieve physical- and link-layer location privacy. It thwarts correlation attacks so that an attacker cannot relate two pseudonyms to the same MNN. A silent period is defined as a constant period, followed by a variable length period in which MNN changes its pseudonym and then keeps silent, not sending any messages. When an MNN starts sending frames after the silent period, the attacker cannot correlate between the MNN's new and old pseudonyms. However, this scheme degrades network performance when the MNN stops its transmission for some periods. In addition, a precise duplicate address detection scheme must be employed to ensure that the new pseudonym does not conflict with any other addresses in the network.

Phantom is another scheme proposed in [30], to achieve a sender's physical-layer location privacy by creating a group of ghost transmitters, which retransmits the original transmitter's messages. Therefore, the attacker that uses an RSS-based fingerprinting localization scheme to localize the original transmitter receives a combination of both original signals and ghost signals. The power of the phantom comes from the inability of the adversary to distinguish between those signals. Although phantom achieves a high level of privacy, it also adds a large overhead when the number of ghosts and, hence, the energy consumed increases.

IV. System Models

A. Network Model

A NEMO-based public hotspot is installed inside a large van, which, in turn, constructs VANET communications with its neighbor vehicles, as shown in Fig. 1. In addition to running a VANET routing protocol, the OBU of this van also works as a NEMO MR and runs a NEMO BS protocol; hence, it is denoted as OBU/MR. Inside the large van, MNNs represent different mobile devices, such as cell phones, personal digital assistants, and laptops.

Initially, to create its network, the MR announces its responsibility for managing the mobility of the entire network by periodically broadcasting its mobile network prefixes (MNPs) acquired from the MR's home network. To join the network, each MNN selects a distinct MNP to be its address in the moving network. When moving out from its home network, the MR acquires a new care-of address (CoA) from the foreign

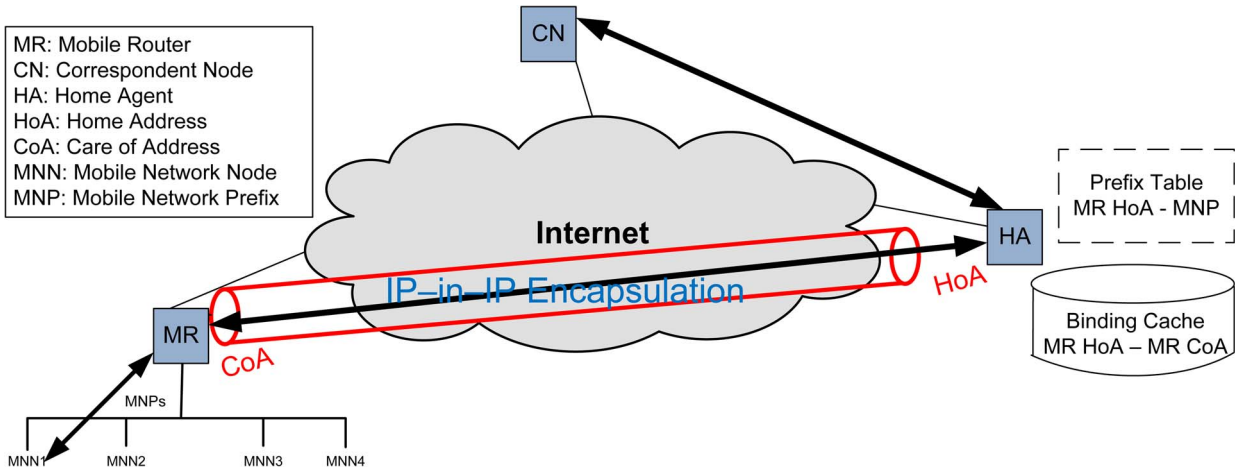

Fig. 4. NEMO.

agent (FA) located in the foreign network and sends home binding update messages to its home agent (HA) to bind its home address (HoA) with its new CoA. Two modes for the binding update messages are defined, i.e., explicit and implicit modes. The former attaches the MR's MNPs to the binding update messages, whereas the latter does not attach them because a dynamic routing protocol is running between the MR and its HA, which facilitates the HA's ability to identify the MR's MNPs. Accordingly, the whole network's movement is controlled by this MR. The HA keeps a binding cache and an extra prefix table to store the MR's HoA with CoA and MNPs, respectively. Finally, a tunnel between MR's CoA and HA is created; therefore, messages transmitted between MNNs and correspondent nodes (CNs) are sent first to the HA, as shown in Fig. 4.

We employ a MANET-centric approach to integrate NEMO and VANET protocols; therefore, only OBU/MR implements a NEMO BS protocol in addition to the MANET routing. All neighbor vehicles that are located on the OBU/MR-RSU path, including the RSU, implement only a MANET routing scheme, such as georouting protocols, as shown in Fig. 2(a).

The communications among an OBU/MR and MNNs are generally structured by using the IEEE 802.11 standard to form a Wi-Fi network. Additionally, the communications among OBU/MR and the roadside access points employed to support the OBU/MR with Internet connectivity are applied by integrating the NEMO BS protocol with VANET. In this paper, we focus on the communications of a vehicle's Wi-Fi network, which are indeed affected by the NEMO-VANET communications outside the vehicle.

Due to the varieties of link-layer connections in NEMO-based VANET, as shown in Fig. 1, three MR-passengers' communication types can be found in the WiFi hotspot, namely, in-vehicle, neighbor vehicles, and nested communications. The in-vehicle communications, which is the focus of this paper, are constructed among the in-vehicle MR that works as a hotspot's AP and passengers' devices inside the same vehicle. Neighbor vehicle communications can be created among an OBU/MR inside one vehicle and some passengers' devices inside neighbor vehicles. This kind of communication relies on the connectivity between vehicles; however, due to the diversity of vehicles' speeds and mobility models, neighbor communications face connection intermittencies, which lead to a degradation in network performance. Nested communications, which are also called nested-NEMO, are formed among a vehicle's MR and some passengers' devices under the control of another MR, which, in turn, is under the control of this vehicle's MR.

In our model of a hotspot, the OBU/MR is located in front of the vehicle and controls the whole hotspot, whereas all other MNNs are randomly located in the van, and the transmission power signal of OBU/MR is considered to be much higher than those of MNNs. In addition, considering the same transmission environment for all MNNs, we assume Gaussian noise with zero mean and σ^2 variance for the shadowing in all signals propagated inside the hotspot.

In addition, we assume that the OBU/MR logically divides the hotspots into k grid points and attaches them to its periodically transmitted beacon; therefore, MNNs inside the hotspot use those grid points to implement our proposed scheme, as illustrated in Section V.

B. Threat and Trust Models

A passive physical-layer location privacy attacker deploys monitoring devices inside the whole network to detect any transmitted signal and estimate the location of the sender by using the RSS, as illustrated in Section II-B. The attacker's monitoring devices are assumed to have high sensing and processing capabilities, and their positions in the network can be changed by the attacker. Using the measured RSSs, each monitoring device estimates and transmits the distance to the intended sender to the attacker. Employing an ML estimation technique, the attacker uses the received distance estimations from all monitoring devices to estimate the exact location of the MNN. (For more information about the ML statistical technique, see Section II-B.)

To attach itself to a hotspot, each MNN authenticates itself to the hotspot's MR and shares a secret key to encrypt its data-link frames, including its medium access control (MAC) address. Being unable to decrypt the transmitted frames' MAC addresses, the attacker only depends on the RSS measurements to localize the MNN. Many data-link authentication and

location privacy schemes [8], [31]–[37] can be used to secure a data-link layer's frames.

To apply a mutual authentication scheme among the MNNs and the OBU/MR, the OBU/MR periodically transmits its public-key certificate inside the hotspot, and we consider that there exists an online certificate verification server whom MNNs trust and use to verify the OBU/MR's certificate. Due to the multihoming technology that enables mobile devices to simultaneously attach to different networks, the MNNs can access the online certificate verification by an alternative Internet connection other than the mobile hotspot connection. For example, a cell phone can use its cellular network to connect to the Internet and verify the received certificates.

V. Fake Point–Cluster-Based Physical-Layer Location Privacy Scheme

The proposed fake point–cluster-based scheme is a combination of two subschemes, i.e., fake point and cluster based, that can be individually employed to provide physical-layer location privacy for MNNs inside a NEMO-based VANET hotspot. The fake-point subscheme achieves a higher location privacy level if the attacker's monitoring devices are located at the selected fake points' locations, whereas the cluster-based subscheme achieves a higher location privacy when preventing the attacker's monitoring devices from detecting the transmitted signals. In Section VI, we show that the proposed fake point–cluster-based scheme increases the MNN's location privacy level. In the following sections, fake-point- and cluster-based subschemes are presented, and then, a scheme for their combination is explained.

A. Fake-Point Location Privacy Subscheme

The proposed fake-point location privacy scheme is employed to protect MNNs' physical location privacy from insider passive attacks, which are explained in Section IV-B. The main idea is that inside the hotspot, the MNNs select random locations, which are called fake points, are used to confuse the attacker. The MNNs consider these fake point when calculating their transmission signal power. Therefore, if an attacker's monitoring devices are located at these fake points, then the measured RSS values at the monitoring devices are similar for all MNNs selecting the same fake point. In Section VI-B, the probability of having at least two MNNs choosing the same fake point's location that contains an attacker's monitoring device is calculated. Therefore, these monitoring devices encounter some error when estimating the distances to MNNs. Depending on the error, the overall MNNs' location estimations also have some deviations, and hence, the MNNs' location privacy is ensured.

Bootstrapping the Hotspot: Working as an AP, the OBU/MR broadcasts inside its network some beacon frames that contain its location, i.e., $(X_{\mathrm{OBU/MR}}, Y_{\mathrm{OBU/MR}})$, and a unique received signal power, i.e., P_u, that all MNNs in the network must consider when calculating their transmission signal power. Using the AP's location and the required received power, the MNNs can define the distances to their AP and, hence, calculate

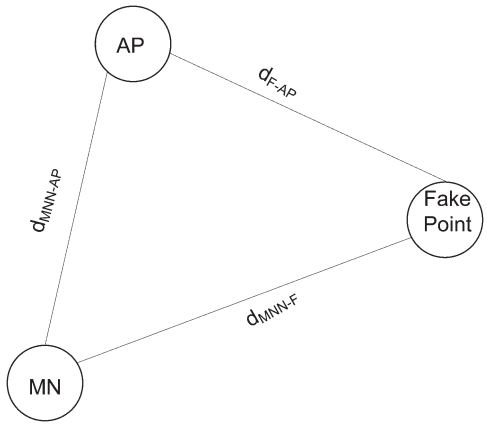

Fig. 5. Fake-point selection.

appropriate transmission signal power. The beacon frames also contain the MNPs for each MNN to select a unique MNP and, hence, to be able to attach to the MENO, AP's certificate (CERT) for the MNNs, to check the authenticity of the AP. An authentication scheme such as in [8] can be used to achieve mutual authentication between MNNs and AP. After the successfully mutual authentication between the MNN and AP, the AP virtually divides the hotspots into K spatial grid points and securely sends the grid points' list to the authenticated MNN. In the remainder of this paper, we use AP, OBU/MR, and MR interchangeably to represent the Wi-Fi AP.

MNN Attachment: To connect to the available hotspot, the MNN first calculates distance $d_{\mathrm{MNN-AP}}$ to its AP as

$$d_{\text{MNN-AP}} = \sqrt{(X_{\mathrm{MNN}} - X_{\mathrm{AP}})^2 + (Y_{\mathrm{MNN}} - Y_{\mathrm{AP}})^2} \quad (15)$$

where $(X_{\mathrm{MNN}}, Y_{\mathrm{MNN}})$ is the MNN's current location measured by the MNN's Global Positioning System. Using this calculated distance and the required received power at AP, i.e., P_u, the MNN calculates its transmission power, i.e., P_{tr}, as

$$P_u = \alpha - 10\beta \log(d_{\text{MNN-AP}}) \quad (16)$$

where β is the path loss and α is a function of transmission power P_{tr}. Instead of using the calculated transmission power, i.e., P_{tr}, the MNN uses another power, i.e., $\acute{P}_{\mathrm{tr}}$, calculated related to a fake location that the MNN selects in the next step.

Identifying the Fake Point: Inside its network, the MNN randomly selects a location, which we will call the fake point, from the grid point list that the AP securely sends to the authenticated MNN, as mentioned in the "Bootstrapping the Hotspot" phase. Therefore, the fake point is one of the K spatial grid points that is defined by the AP and represents location (x, y) inside the hotspot. Using (15), the MNN recalculates its distance to the AP as the sum of the MNN-fake point distance and the fake point-AP distance, and then, the MNN employs this distance to recalculate transmission power $\acute{P}_{\mathrm{tr}}$ using (16). Therefore, the MNN recalculates transmission power $\acute{P}_{\mathrm{tr}}$ in such a way that the MNN's signal is transmitted first to this fake point then to the AP. However, in our scheme, the MNN does not send its signals to this fake point; indeed, it sends the signals directly to its AP. This deceiving action is only to confuse attackers. As shown in Fig. 5, the distance between

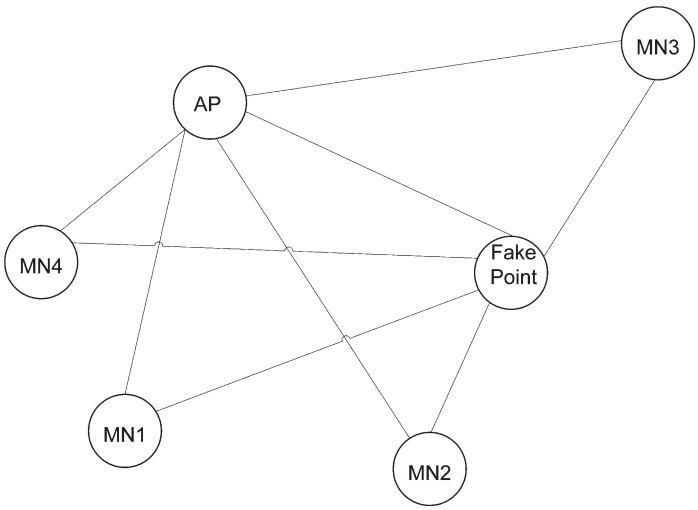

Fig. 6. MNNs select the same fake point.

the MNN and its AP, i.e., $d_{\mathrm{MNN-AP}}$, is always less than the sum of the distances of the MNN-fake point, i.e., $d_{\mathrm{MNN-F}}$, and the fake point-AP, i.e., $d_{\mathrm{F-AP}}$. Therefore, the power needed to transmit a packet from the MNN to the AP directly, i.e., P_{tr}, is always less than that needed for the packet to go through the fake point, i.e., $\acute{P_{\mathrm{tr}}}$. Consequently, using the larger power, i.e., $\acute{P_{\mathrm{tr}}}$, in message transmission guarantees that our proposed scheme negatively affects the packet-dropping probability. The main goal of selecting a fake point in the network is to have a possibility that one of the attacker's monitoring devices is located at this fake point. Therefore, when many MNNs select the same fake point and an attacker's monitoring device is located in this fake point, as shown in Fig. 6, the estimated distances calculated by this monitoring device encounter much more estimation error than those calculated by other monitoring devices. Since the measured RSSs at the monitoring device are functions of the distances to the MNN, the recorded error increases as the distance between MNNs that selected the same fake points increases. In Section VI, the error encountered at the monitoring devices is measured to show the strength of the MNN's location privacy when using our proposed scheme.

To calculate transmission signal power $\acute{P_{\mathrm{tr}}}$, the MNN randomly selects a fake point, i.e., (X_F, Y_F). Given that the received signal power at AP is P_u, the signal power at the fake point, i.e., P_{ftr}, can be calculated as

$$P_u = f(P_{\mathrm{ftr}}) - 10\beta \log(d_{F\text{-AP}}) \tag{17}$$

$$d_{F\text{-AP}} = \sqrt{(X_F - X_{\mathrm{AP}})^2 + (Y_F - Y_{\mathrm{AP}})^2}. \tag{18}$$

The MNN can then calculate the transmitted power to the fake point as

$$P_{\mathrm{ftr}} = f(\acute{P_{\mathrm{tr}}}) - 10\beta \log(d_{\mathrm{MNN}\text{-}F}) \tag{19}$$

$$d_{\mathrm{MNN}\text{-}F} = \sqrt{(X_F - X_{\mathrm{MNN}})^2 + (Y_F - Y_{\mathrm{MNN}})^2}. \tag{20}$$

The MNN transmits its messages with the new calculated power, i.e., $\acute{P_{\mathrm{tr}}}$. In addition, the MNN selects a new fake point for each transmitted signal; therefore, the possibility of having the same location as the attacker's location will be increased.

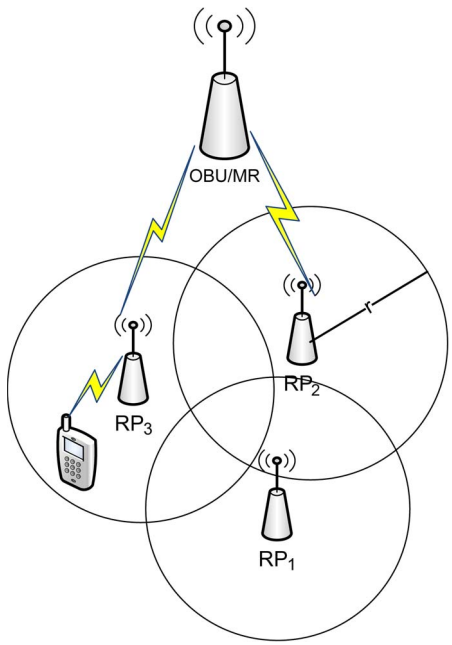

Fig. 7. Cluster-based subscheme.

B. Cluster-Based Location Privacy Subscheme

Here, we propose another subscheme to achieve MNN location privacy in NEMO-based VANET. In Section VI, we show that the probability of successfully violating the MNN's location privacy, when our proposed fake-point subscheme is employed, decreases as the ratio (A/K) of the number of the attacker's monitoring devices, i.e., A, to the number of defined spatial grid points, i.e., K, increases. Since K is always much larger than A, the probability of violating the MNN's location is quite large. Therefore, we propose the cluster-based subscheme; hence, when it is combined with the fake-point scheme, the probability of violating the MNN's location is decreased. The main idea of the cluster-based subscheme is to divide the hotspot area into smaller cells, *i.e.,* clusters, and assign a new AP for each cell. Thus, the MNN uses little power value to transmit its messages and, hence, prevents an attacker's monitoring devices from detecting the MNN's signals. Hence, the attacker cannot employ the positioning scheme to localize the MNN because the attacker cannot measure the RSS of the undetected transmission signal. The cluster-based subscheme consists of three steps, i.e., NEMO bootstrapping, MNN attachment, and reference point selection.

Step 1—NEMO Bootstrapping: At the time of constructing the Wi-Fi as NEMO-based VANET communications, the OBU/MR that works as an AP for the whole network divides the network area into smaller n subareas called cells, i.e., $c_1, c_2, \ldots, c_n$. For each cell, i.e., c_i, the OBU/MR assigns an AP, which is a reference point RP_i that works as a local AP for all MNNs located within distance r around RP_i. Considering each cell's coverage area as a circle, r represents the cell's radius, and we assume that all cells have the same radius, and they may overlap with each other, as shown in Fig. 7. From an attacker's perspective, we consider that there is, at most, one attacker's monitoring device in each cell.

Step 2—MNN Attachment: Working as a local AP, each RP broadcasts a beacon packet; hence, only MNNs under its coverage area receive this beacon. The beacon message contains information about the RP, including its identity, ID_{RP}, its coverage area's radius, r, and its required received signal's power, P_{RRP}.

Considering the knowledge of its location, i.e., $(X_{\mathrm{MNN}}, Y_{\mathrm{MNN}})$, the MNN calculates the transmission signal power for its messages directed to its chosen RP as

$$\text{FSPL (DB)} = 20\log_{10}(r) + 20\log_{10}(f) + 32.45 \tag{21}$$

$$\text{TP}_{\mathrm{MNN}} = P_{RRP} \times \text{FSPL} \tag{22}$$

where FSPL is the free-space path loss [38], which depends on the cell's radius in meters, i.e., r, and the transmitted signal frequency in megahertz, i.e., f.

Step 3—Reference Point Selection: When an MNN attaches to the hotspot, it receives m beacons from m different RPs. The MNN sorts the received m beacons' signal power and chooses the RP with the strongest signal to be its local AP. As shown in Fig. 7, the MNN transmits all its messages with the calculated low transmission power to the selected RP, which, in turn, retransmits the messages to the OBU/MR that works as the hotspot's AP.

C. Fake Point–Cluster-Based Location Privacy Scheme

In our cluster-based subscheme, since clusters can be spatially overlapped, the MNN's transmitted signals may be received by many clusters and not only by the intended cluster. Therefore, if one attacker's monitoring device is in each cluster, the monitoring devices in the clusters that receive the MNN's signals can collude to reveal the MNN's location by applying a statistical positioning scheme. To increase the MNN's location privacy, a combination of the fake-point- and cluster-based subschemes can be applied.

In addition to receiving OBU/MR beacon messages, the MNN also receives some RPs' beacon messages that contain RPs' positions, i.e., $\{(X_{RP_1}, YRP_1), (X_{RP_2}, YRP_2), \ldots, (X_{RP_m}, YRP_m)\}$. After calculating its transmission power as depicted in the cluster-based subscheme, the MNN randomly selects a fake point that is located in its cluster.

Using the fake-point subscheme, the MNN calculates the required power at the fake point and then adjusts its transmit power to this power. Therefore, the MNN confuses some of the attacker's monitoring devices and, hence, increases the estimation error resulting from the attacker's monitoring devices' collusion.

This combination between the fake-point- and cluster-based subschemes prevents some attacker's monitoring devices located inside neighbor clusters from detecting the sender's transmitted signals. In addition, the fake point–cluster-based subscheme selects a fake point inside the sender's cluster to ensure higher location privacy and consume lower power.

VI. Analytical Location Privacy Evaluation

Here, an analytical evaluation for the proposed scheme, i.e., the fake point–cluster-based scheme, is presented. Similar to the evaluation analysis in [39], we employ three metrics, namely, correctness, accuracy, and certainty. Correctness measures the additional estimation error that is added by our proposed scheme, accuracy measures the probability of an attacker's success in breaking the MNN's location privacy, and certainty measures the entropy of the achieved privacy.

A. Correctness

Fake-Point-Based Subscheme: When m different MNNs choose the same fake point, which, in turn, may be a location of an attacker's monitoring device, the attacker estimation error for the MNN's localization increases. Using the signal propagation model in [40], the MNN's RSS can be calculated as

$$\text{RSS} = \frac{\text{AP}_t}{B + d^{\alpha} + C(\log_{10} d)^{\beta} + D} \tag{23}$$

where A, B, C, D, α, and β are a signal's parameters that can be estimated by the attacker. However, the attacker cannot estimate the MNN's transition power P_t while distance d to the target MNN is also unknown. Using Frii's formula, P_t can be expressed as

$$P_t = \text{RSS} - G_t - G_r - 20\log_{10}\frac{\lambda}{4\pi d} \tag{24}$$

where G_t and G_r are a sending and receiving channel's gains. Therefore, substituting (24) in (23), RSS can be written as

$$\text{RSS} = \frac{A\left(G_t + G_r + 20\log_{10}\frac{\lambda}{4\pi d}\right)}{A - B - d^{\alpha} - C(\log_{10} d)^{\beta} - D}. \tag{25}$$

By (25), the attacker can measure the RSS values, i.e., $\text{RSS}_1, \text{RSS}_2, \ldots, \text{RSS}_m$, for m different MNNs that select the same fake point in the fake-point subscheme, as

$$\text{RSS}_i = \frac{A\left(G_t + G_r + 20\log_{10}\frac{c}{4\pi f d}\right)}{A - B - d^{\alpha} - C(\log_{10} d)^{\beta} - D} \tag{26}$$

where C is the speed of the light, and f is the signal's frequency, which is one of the channel parameters. Assuming that 2.4 GHZ is the frequency band that is used in the hotspot, m MNNs select any of the 14 channels that are assigned in this band. The channels' frequency bands are spaced 5 MHZ apart; therefore, the differences in the term $\log_{10}(c/4\pi f d)$ for each MNN are negligible. Thus, (26) yields the same RSS's value for all MNNs that share the same fake point.

From (26), the attacker estimates the distance between its location, which is the fake point's location, i.e., (x_f, y_f), and the target point's location, i.e., (x_i, y_i), as

$$d_i = \sqrt{(x_i - x_f)^2 + (y_i - y_f)^2}. \tag{27}$$

Since $d_i, i = 1, 2, \ldots m$ has the same value and (x_f, y_f) is a fixed point for all MNNs, then the attacker calculates the same

estimated location (x_e, y_e) for an MNN$_i$'s true location (x_i, y_i). Hence, (4) is expressed as

$$Z_i = d_i + \eta_i + \delta_i, \qquad \delta \geq 0 \tag{28}$$

where δ_i is a deviation of the estimated distance that is added when applying the fake-point subscheme. It can be calculated as

$$\delta_i = \frac{|y_i - y_e|}{|x_i - x_e|}. \tag{29}$$

Therefore, (4) changes as

$$Z = d + \eta + \delta, \qquad \delta \geq 0. \tag{30}$$

The attacker then uses ML estimation as in (13) to determine the MNN's position as

$$\begin{aligned}\hat{\theta}_{\mathrm{ML}} &= \arg\min_{[x,y]^T} \sum_{i=1}^{N} \frac{(\eta_i + \delta_i)^2}{\sigma_i^2} \\ &= \arg\min_{[x,y]^T} \sum_{i=1}^{N} \frac{\eta_i^2}{\sigma_i^2} + \frac{\delta_i^2 + 2\delta_i\eta_i}{\sigma_i^2}\end{aligned} \tag{31}$$

where N is the number of an attacker's monitoring devices. Note that the term $\delta_i^2 + 2\delta_i\eta_i/\sigma_i^2$ is the added value to the ML estimation. The additional estimation error is called the correctness of the estimated position, and as it increases, the MNN's location privacy increases as well.

Cluster-Based Subscheme: The goal of this subscheme is to decrease the transmit power by employing TPC in such a way that only a small number of an attacker's monitoring devices, i.e., L, from all monitor devices, i.e., N, can detect the MNN's signal and measure the RSS. Therefore, the attacker calculates the ML estimation as

$$\hat{\theta}_{\mathrm{ML}} = \arg\min_{[x,y]^T} \sum_{i=1}^{L} \frac{(z_i - d_i)^2}{\sigma_i^2}. \tag{32}$$

For $L = 1$, which means only one monitoring device can detect the MNN's signal, (32) can be written as

$$\hat{\theta}_{\mathrm{ML}} = \frac{(\eta)^2}{\sigma^2} + \delta_{\mathrm{cluster}} \tag{33}$$

where $\delta_{\mathrm{cluster}}$ is the added estimation error resulting from the lack of information as only one monitoring device measures the MNN's RSS. $\delta_{\mathrm{cluster}}$ decreases as the number of monitoring devices increases, which, in turn, gives an indication of a lower location privacy level.

Fake Point–Cluster-Based Scheme: Depending on the analysis of both fake-point- and cluster-based subschemes, the estimation error for the combination of the two subschemes can be expressed as

$$\begin{aligned}\hat{\theta}_{\mathrm{ML}} &= \arg\min_{[x,y]^T} \sum_{i=1}^{L} \frac{(z_i - d_i)^2}{\sigma_i^2} \frac{\delta_{\mathrm{cluster}}}{L} \\ &= \frac{\delta_{\mathrm{cluster}}}{L} \arg\min_{[x,y]^T} \sum_{i=1}^{L} \frac{\eta_i^2}{\sigma_i^2} + \frac{\delta_i^2 + 2\delta_i\eta_i}{\sigma_i^2}.\end{aligned} \tag{34}$$

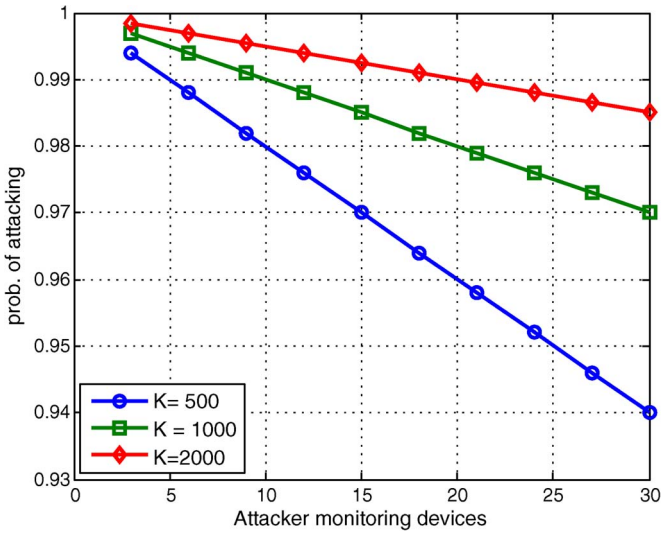

Fig. 8. Fake-point subscheme attacking probability.

B. Accuracy

Here, the accuracy of the fake point–cluster-based scheme is calculated by measuring the accuracy of the positioning system employed by the attacker. We measure the accuracy of the positioning system by calculating the probability of attacking the hotspot while our proposed scheme is implemented. According to the fake-point subscheme explained in Section V-A, the accuracy of this subscheme depends on the possibility of confusing the attacker by having many MNNs select the same fake point and having an attacker's monitoring device located in this fake point. Considering that the hotspot is spatially divided into K grid points that the OBU/MR periodically sends to all MNNs, the probability that at least two MNNs select the same fake point from those K points is calculated using the birthday paradox probability

$$\Pr(x \geq 2) = 1 - \frac{K!}{(K-u)!K^u} \tag{35}$$

where $1 < u$ is the number of MNNs in the hotspot. In addition, the probability that the selected fake point is an attacker's monitoring device's location is A/K, where A is the number of an attacker's monitoring devices in the network. Therefore, combining the two probabilities, the probability that an attacker's monitoring device is located at the fake point's location selected by at least two different MNNs can be calculated as

$$\Pr(\text{fake point}) = \left[1 - \frac{K!}{(K-u)!K^u}\right] \frac{A}{K}. \tag{36}$$

Since the number of passengers inside the hotspot is always much less than the defined spatial grid points $(u \ll K)$, we consider $K!/(K-u)!K^u \approx 0$. Therefore, the probability of successfully attacking the hotspot when employing the fake-point subscheme (see Fig. 8) is calculated as

$$\Pr(\text{fake-point attacking}) = 1 - \frac{A}{K}. \tag{37}$$

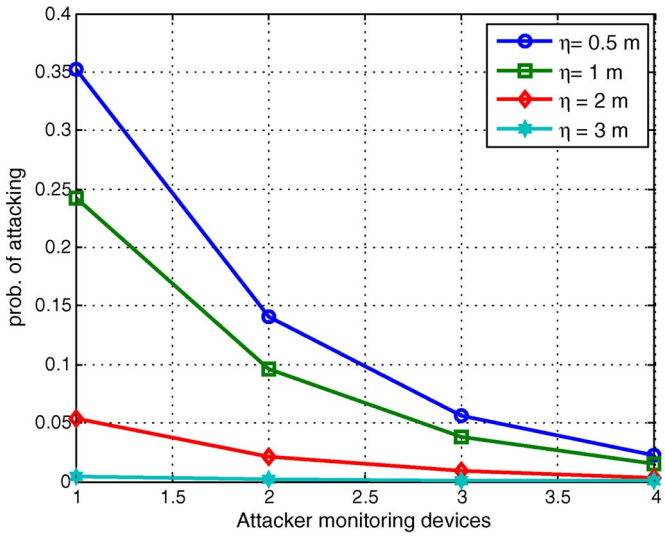

Fig. 9. Cluster-based subscheme attacking probability.

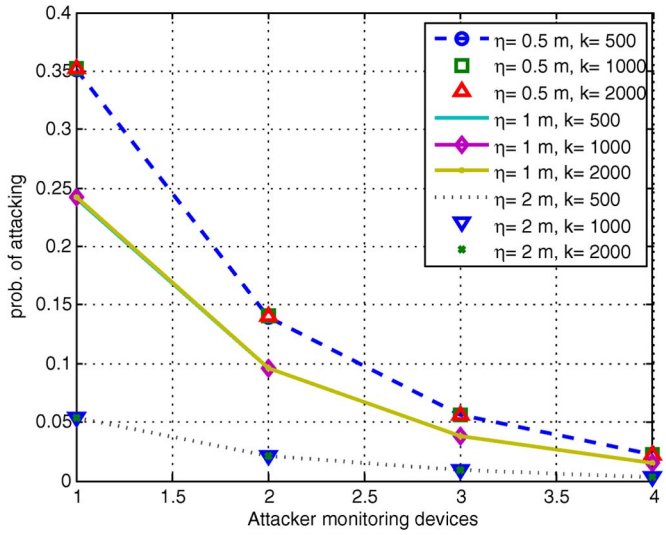

Fig. 10. Fake point–cluster-based scheme attacking probability.

As shown in Fig. 8, the probability of attacking decreases when the ratio (A/K) of the number of the attacker's monitoring devices, i.e., A, to the number of defined spatial grid points, i.e., K, increases, because the possibility that the selected fake point is an attacker's monitoring device's location increases, and hence, the attacker is confused. Intuitively, this ratio increases when A increases and/or K decreases.

For the cluster-based subscheme, the number of overlapping clusters, i.e., O, that intersect with the MNN's cluster affects the probability of achieving an MN's location privacy. This probability is calculated as

$$\begin{aligned}\Pr(\text{cluster}) &= \Pi_{i=1}^{O} P_{\eta_i} \\ &= \Pi_{i=1}^{O} \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(-\frac{\eta_i^2}{2\sigma_i^2}\right). \end{aligned} \tag{38}$$

As shown in Fig. 9, the maximum number of overlapping clusters and, hence, number of attacker monitoring devices, is four.

Combining the fake-point-based with cluster-based probabilities, we get the probability of achieving location privacy with a fake point–cluster-based scheme as

$$\left[\left[1 - \frac{K!}{(K-u)!K^u}\right]\frac{A}{K}\right] \Pi_{i=1}^{O} \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(-\frac{\eta_i^2}{2\sigma_i^2}\right). \tag{39}$$

Fig. 10 shows the combination of fake-point- and cluster-based probabilities.

C. Certainty

An entropy model measures the uncertainty of an attacker's location privacy scheme, which is calculated as

$$H(x) = \sum_i \Pr(x_i) \log \frac{1}{\Pr(x_i)}. \tag{40}$$

Therefore, the entropy for our proposed schemes is shown in Fig. 11.

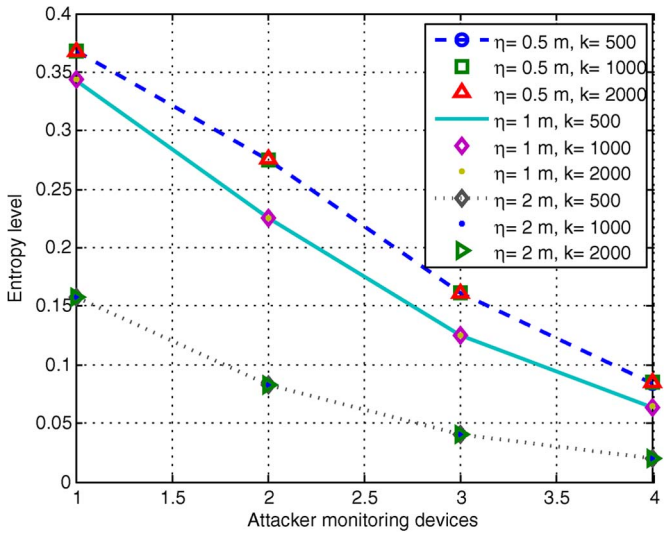

Fig. 11. Fake point–cluster-based entropy.

VII. Performance Evaluation

Here, a MATLAB simulation has been conducted to evaluate the performance of the fake point–cluster-based scheme. We simulate a 45 m × 45 m hotspot installed inside one vehicle. To create VANET communications, we consider six vehicular subnetworks, each of which is covered by one RSU, and vehicles inside the VANET can roam from one subnetwork to another. The vehicles have a linear mobility model, whereas MNNs inside the simulated hotspot have fixed locations, or they may move inside the vehicle in such a way that they are still reachable by the hotspot's AP with one-hop communication. To simulate the overlapping clusters, a group of reference points has been deployed in such a way that each reference point, i.e., RP_i, covers an area of 25 m^2, with 1-m overlapping area with each neighbor cluster. The centralized AP and all RPs define specific received power that each MNN must consider while sending its signals to AP or any RP. Table II gives our simulation parameters.

TABLE II
SIMULATION PARAMETERS

Road width	$5500m \times 10m$
Road's network size	$1000m \times 10m$
Road's networks number	6
Vehicles number	36000
WiFi size	$45m \times 45m$
Wi-Fi nodes number	600
Frequency	$2.4GHz$
AP transmission power	$5mW \simeq 7dBm$
cluster area	$25m^2$
AP required received power	$5dBm$
Cluster required received power	$3dBm$
overlapping area among clusters	$1m$
Length of the phy header	$0byte$
Thermal noise	$0dB$

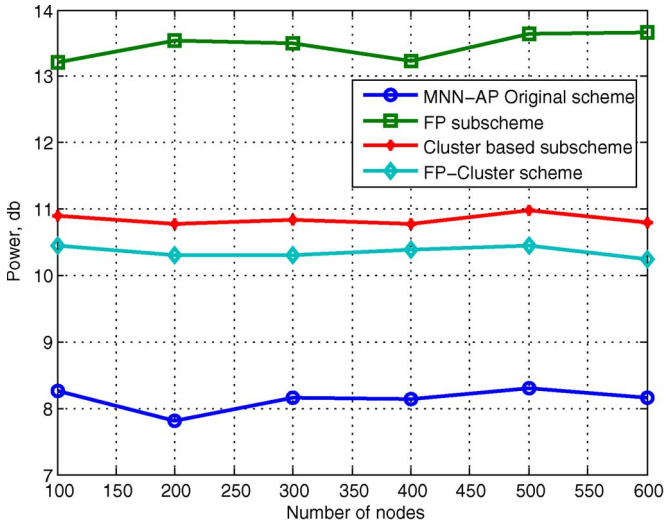

Fig. 12. MNN transmission power.

Fig. 12 shows the MNN transmission power for the fake point–cluster-based, fake-point subscheme, cluster-based subscheme, and the original Wi-Fi communication scheme as a reference. As shown in the figure, the original communication scheme, where a fake point–cluster-based scheme is not implemented, has the smallest transmission power. On the other hand, there is a 65.5% power increase when employing the fake-point subscheme because the selected fake point can be found very far from the MNN; thus, more power at the MNN is needed to equalize RSS at this fake point. The power required in the cluster-based subscheme depends on the received power at the RP, which is always less than the received power at the AP; therefore, only a 37.5% increase in MNN transmission power is recorded. Compared with the fake-point subscheme, when combining the fake-point subscheme with the cluster-based subscheme, we get a 23% decrease in transmission power. The reason for this power saving is that when employing the fake point–cluster-based scheme, the MNN selects a nearer fake point, which is located in its cluster.

The distances between MNNs and APs contribute to increasing MNNs' transmission power, as shown in Fig. 13. The shortest distance between MNN and AP, which is employed in an MNN-AP conventional scheme, always needs less transmission power, whereas the indirect distances from MNN to the fake

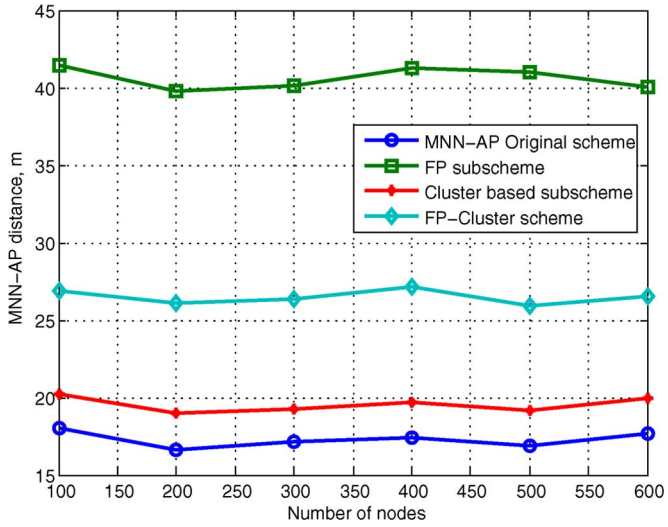

Fig. 13. MNN–AP route distances.

point then to the AP, which are employed in our proposed schemes, consume more power. Compared with the reference MNN-AP conventional scheme, fake point, cluster-based, and fake point–cluster schemes encounter distance increases of 135%, 17.6%, and 52.9%, respectively. The increases in distances and power are our cost to achieve high MNN location privacy. Fig. 14 shows power consumed at different MNN-AP distances. Our proposed schemes achieve lower power consumptions than that in the conventional scheme at MNN-AP distances less than 5 m. At such small distances, location protection is much more important than it is at large distances where MNN locations can be easily revealed. Therefore, at lower distances, the fake point–cluster scheme achieves both less power consumption and high location privacy, whereas the conventional scheme has higher power consumption without protecting the MNN location.

In Section VI, we calculate the entropy of our proposed scheme, which relies on the probability that many MNNs have the same fake point. Here, as shown in Figs. 15 and 16, we practically measure the histogram for both the fake-point subscheme and the fake point–cluster scheme, respectively. In Fig. 15, the number of MNNs that select the same point reaches six, whereas in Fig. 16, it reaches 90 out of 300 MNNs. This difference occurs because, in the fake-point subscheme, each MNN can select its fake point among large varieties of fake points that are distributed all over the network, whereas in the fake point–cluster-based scheme, these varieties have shrunk to only fake points in neighbor clusters. Therefore, the fake point–cluster-based scheme achieves higher location privacy than does the fake-point subscheme.

To show the impact of integrating the NEMO protocol with VANET, Fig. 17 presents the total sender's handover time when applying NEMO, MIPv6, and MIPv4 protocols. Compared with other mobility protocols, a sender employing the NEMO BS protocol requires the smallest handover delay, because only the MR implements the NEMO-BS; hence, the cost of the delay is distributed over all MNNs inside the Wi-Fi. In addition, this delay constantly increases with the vehicle speeds, allowing our scheme to be used for scalable networks. On the other hand, for

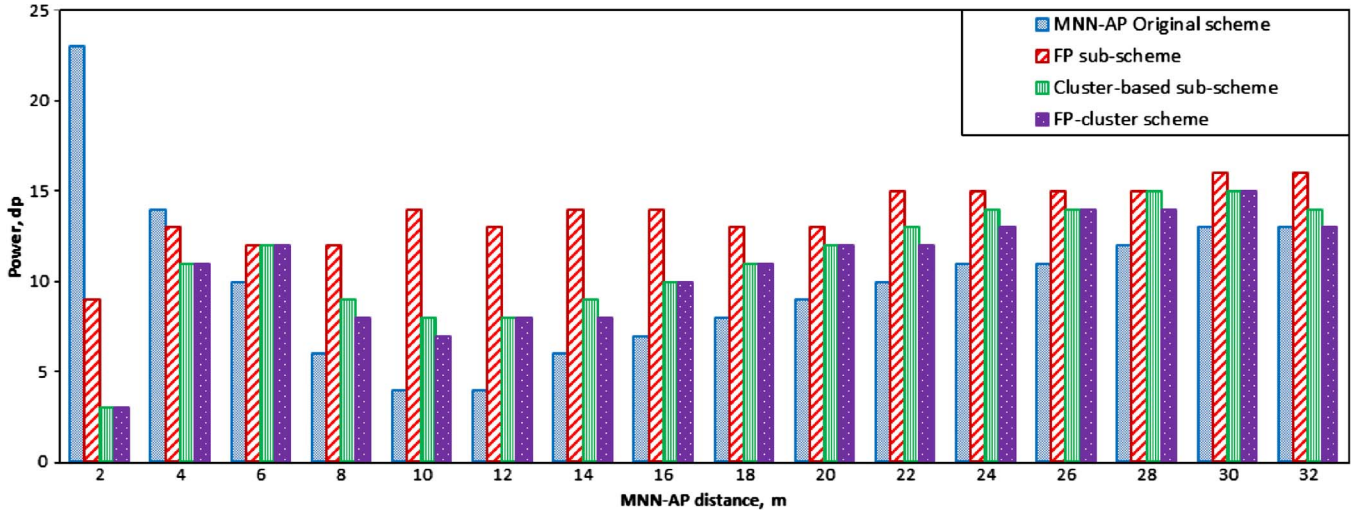

Fig. 14. Average power consumption at different distances.

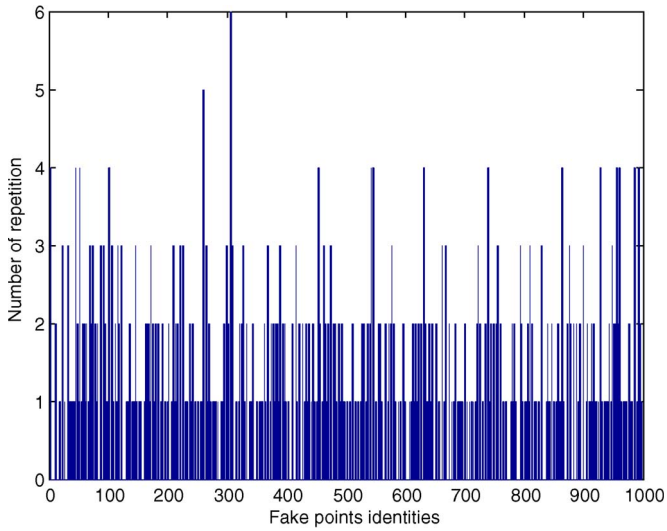

Fig. 15. Fake-point histogram.

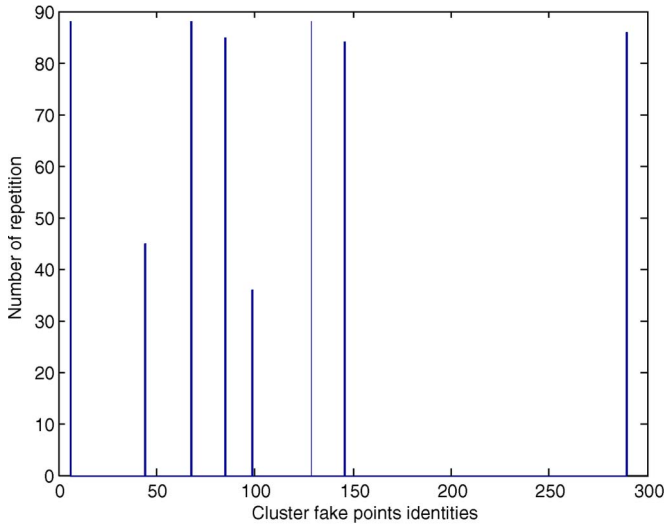

Fig. 16. Fake point–cluster-based histogram.

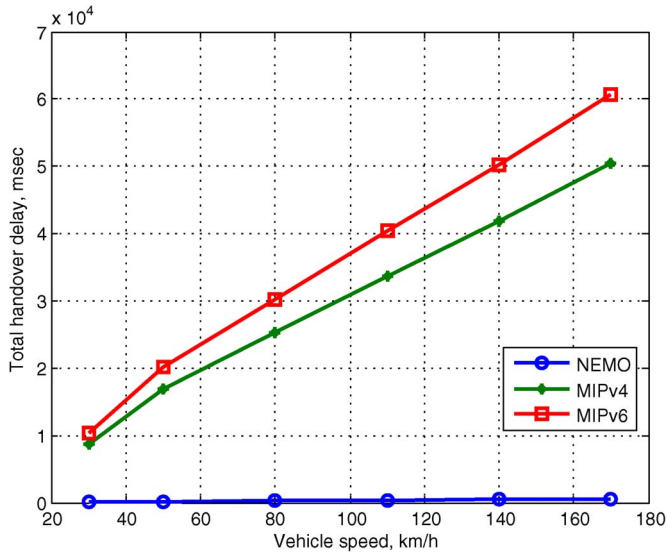

Fig. 17. Total handover delay.

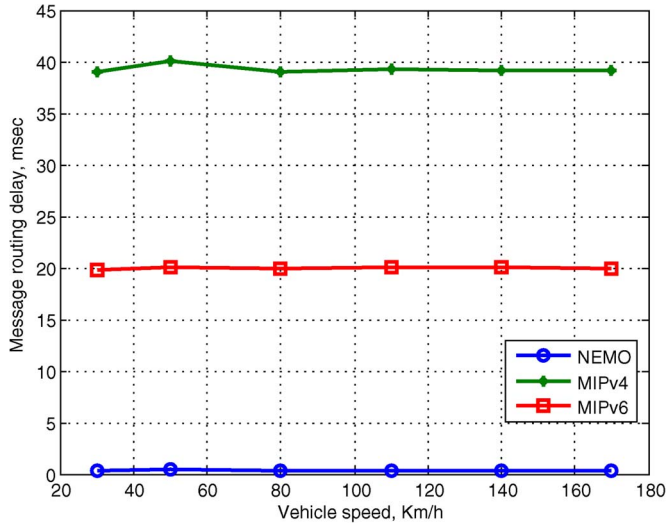

Fig. 18. Message routing delay.

the MIPv6 and MIPv4 protocols, the handover delays linearly increase with vehicle speeds, because the number of handovers increases accordingly. The MIPv6 protocol costs many more delays than that in the MIPv4 protocol, due to the addition of the correspondent binding update messages transmitted to the sender's correspondent nodes.

Fig. 18 shows the total message's routing delay when applying different mobility management protocols. The NEMO BS protocol achieves 95% and 97% delay decreases compared with those in the MIPv6 and the MIPv4, respectively.

VIII. Conclusion and Future Work

In this paper, we have proposed an efficient physical-layer location privacy scheme, i.e., the fake point–cluster-based scheme, to thwart physical-layer attackers and achieve MNNs' location privacy for mobile public hotspots in NEMO-based VANETs. The fake point–cluster-based scheme achieves sender's location privacy by increasing the attacker's confusion when measuring senders' RSSs. In addition, our proposed scheme can be practically implemented due to the high possibility of having two nodes select the same fake point, and it increases the network performance because it requires less routing delay than those required for other mobility management protocols.

In our future work, we plan to apply our proposed scheme to other NEMO scenarios, such as nested NEMO, in which MNNs are controlled by an MR, which, in turn, is controlled by another MR. The challenge in this scenario is the high message routing delay resulting from sending the transmitted messages through many home agents. In addition, a scheme for reducing power consumption will be proposed to save MNNs' power while achieving our location privacy-preserving scheme.

References

[1] S. Taha and X. Shen, "Fake point location privacy scheme for mobile public hotspots in NEMO-based VANETs," in *Proc. IEEE ICC*, Budapest, Hungary, Jun. 9–13, 2013, pp. 630–634.

[2] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, "Mobility and handoff management in vehicular networks: A survey," *Wireless Commun. Mobile Comput.*, vol. 11, no. 4, pp. 459–476, Apr. 2011.

[3] A. Festag, R. Baldessari, W. Zhang, L. Le, A. Sarma, and M. Fukukawa, "Car-2-X communication for safety and infotainment in Europe," *NEC Tech. J.*, vol. 3, no. 1, pp. 21–26, Mar. 2008.

[4] Y. Peng and J. Chang, "A novel mobility management scheme for integration of vehicular ad hoc networks and fixed IP networks," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 112–125, Feb. 2010.

[5] E. Perera, V. Sivaraman, and A. Seneviratne, "Survey on network mobility support," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 8, no. 2, pp. 7–19, Apr. 2004.

[6] S. Taha and X. Shen, "Anonymous home binding update scheme for mobile IPv6 wireless networking," in *Proc. IEEE GLOBECOM*, Houston, TX, USA, Dec. 5–9, 2011, pp. 1–5.

[7] S. Taha, S. Cespedes, and X. Shen, "EM^{3}A: Efficient mutual multi-hop mobile authentication scheme for pmip networks," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 10–15, 2012, pp. 873–877.

[8] S. Taha and S. Shen, "A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET," in *Proc. Globecom CISS*, Anaheim, CA, USA, Dec. 2012, pp. 1004–1009.

[9] J. Lorchat and K. Uehara, "Optimized inter-vehicle communications using NEMO and MANET," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.: Comput., Netw., Services*, San Jose, CA, USA, Jul. 17–21, 2006, pp. 1–6.

[10] R. Baldessari, A. Festag, and J. Abeillé, "NEMO meets VANET: A deployability analysis of network mobility in vehicular communication," in *Proc. 7th IEEE Int. Conf. ITST*, Sophia Antipolis, France, Jun. 6–8, 2007, pp. 1–6.

[11] S. Cespedes, X. Shen, and C. Lazo, "IP mobility management for vehicular communication networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 187–194, May 2011.

[12] A. Prakash, S. Tripathi, R. Verma, N. Tyagi, R. Tripathi, and K. Naik, "Vehicle assisted cross-layer handover scheme in NEMO-based VANETs (VANEMO)," *Int. J. Internet Protocol Technol.*, vol. 6, no. 1/2, pp. 83–95, Jun. 2011.

[13] I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.

[14] T. Whalen, "Mobile devices and location privacy: Where do we go from here?" *IEEE Security Privacy*, vol. 9, no. 6, pp. 61–62, Nov./Dec. 2011.

[15] K. Bauer, D. McCoy, B. Greenstein, D. Grunwald, and D. Sicker, "Physical layer attacks on unlinkability in wireless LANs," in *Privacy Enhancing Technologies*. New York, NY, USA: Springer-Verlag, 2009, pp. 108–127.

[16] B. Hood and P. Barooah, "Estimating DOA from radio-frequency RSSI measurements using an actuated reflector," *IEEE Sensors J.*, vol. 11, no. 2, pp. 413–417, Feb. 2011.

[17] R. El-Badry, A. Sultan, and M. Youssef, "Hyberloc: Providing physical layer location privacy in hybrid sensor networks," in *Proc. IEEE ICC*, Cape Town, South Africa, May 23–27, 2010, pp. 1–5.

[18] C. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in *Proc. Data and Applications Security XXI*. Redondo Beach, CA, USA: Springer-Verlag, Jul. 8–11, 2007, pp. 47–60.

[19] R. El-Badry, M. Youssef, and A. Sultan, "Hidden anchor: A lightweight approach for physical layer location privacy," *J. Comput. Syst., Netw. Commun.*, vol. 2010, pp. 749298-1–749298-12, 2010.

[20] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, RFC 3963: Network Mobility (NEMO) Basic Support Protocol, 2005. [Online]. Available: http://tools.ietf.org/pdf/rfc3963.pdf

[21] C. Perkins, "RFC 3344: Ip mobility support for IPv4," Network Working Group, 2002. [Online]. Available: http://tools.ietf.org/html/rfc3344

[22] D. Johnson, C. Perkins, and J. Arkko, "RFC 3775: Mobility support in IPv6," IETF, Jun. 2004. [Online]. Available: http://tools.ietf.org/html/rfc3775

[23] J. Choi, Y. Khaled, M. Tsukada, and T. Ernst, "IPv6 support for VANET with geographical routing," in *Proc. 8th ITST*, Phuket, Thailand, Oct. 2008, pp. 222–227.

[24] V. Sandonis, M. Calderon, I. Soto, and C. Bernardos, "Design and performance evaluation of a PMIPv6 solution for geonetworking-based VANETs," *Ad Hoc Netw.*, 2012, to be published. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S157087051200025X

[25] R. Baldessari, W. Zhang, A. Festag, and L. Le, "A MANET-centric solution for the application of NEMO in VANET using geographic routing," in *Proc. 4th Int. Conf. Testbeds Res. Infrastruct. Dev. Netw. Communities*, Innsbruck, Austria, Mar. 18–20, 2008, p. 12.

[26] S. Gezici, "A survey on wireless position estimation," *Wireless Pers. Commun.*, vol. 44, no. 3, pp. 263–282, Feb. 2008.

[27] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. 5th Int. Conf. MobiSys*, San Juan, Puerto Rico, 2007, pp. 246–257.

[28] T. Wang and Y. Yang, "Location privacy protection from rss localization system using antenna pattern synthesis," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 10–15, 2011, pp. 2408–2416.

[29] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2005, vol. 2, pp. 1187–1192.

[30] S. Oh, T. Vu, M. Gruteser, and S. Banerjee, "Phantom: Physical layer cooperation for location privacy protection," in *Proc. IEEE INFOCOM*, 2012, pp. 3061–3065.

[31] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[32] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.

[33] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[34] F. Armknecht, J. Girao, A. Matos, and R. Aguiar, "Who said that? Privacy at link layer," in *Proc. 26th IEEE INFOCOM*, Anchorage, AK, USA, May 6–12, 2007, pp. 2521–2525.

[35] E. Ryu, E. Yoon, and K. Yoo, "More robust anonymous authentication with link-layer privacy," in *Proc. IEEE APSCC*, Hangzhou, China, Dec. 6–10, 2010, pp. 441–446.

[36] Y. Fan, B. Lin, Y. Jiang, and X. Shen, "An efficient privacy-preserving scheme for wireless link layer security," in *Proc. IEEE GLOBECOM*, New Orleans, LA, USA, Nov. 30/Dec. 4, 2008, pp. 1–5.

[37] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 13–18, 2008, pp. 1229–1237.

[38] P. Katev, "Propagation models for WiMAX at 3.5 GHz," in *Proc. ELEKTRO*, Rajecké Teplice, Slovakia, May 21–22, 2012, pp. 61–65.

[39] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. SP*, 2011, pp. 247–262.

[40] R. Ezzine, A. Al-Fuqaha, R. Braham, and A. Belghith, "A new generic model for signal propagation in Wi-Fi and WiMAX environments," in *Proc. 1st IFIP WD*, Dubai, United Arab Emirates, Nov. 24–27, 2008, pp. 1–5.

Sanaa Taha (S'13) received the B.Sc. and M.Sc. degrees from Cairo University, Giza, Egypt, in 2001 and 2005, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2013.

She is currently an Assistant Professor with the Department of Information Technology, Faculty of Computers and Information, Cairo University. Her research interests include wireless network security, mobile network security, mobility management, and applied cryptography.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees from Rutgers University, New Jersey, Camden, NJ, USA, in 1987 and 1990, respectively, all in electrical engineering.

He is a Professor and the University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. From 2004 to 2008, he was the Associate Chair for Graduate Studies. He is a coauthor/editor of six books and has published more than 600 papers and book chapters in wireless communications and networks, control, and filtering. His research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks.

Dr. Shen served as the Technical Program Committee Chair for the IEEE 72nd Vehicular Technology Conference (VTC'10 Fall), the Symposia Chair for the IEEE International Conference on Communications (ICC'10), the Tutorial Chair for the IEEE 73rd Vehicular Technology Conference (VTC'11 Spring) and the IEEE ICC'08, the Technical Program Committee Chair for the IEEE Global Communications Conference (Globecom'07), the General Cochair for the International Conference on Communications and Networking in China (Chinacom'07) and The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine'06), and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications and Peer-to-Peer (P2P) Communications and Networking. He also serves/served as the Editor-in-Chief for the IEEE NETWORK, *P2P Networking and Application*, and the *Institution of Engineering and Technology (IET) Communications*; a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Computer Networks*, and *Association for Computing Machinery (ACM) Journal of Wireless Networks*; and a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS MAGAZINE, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo; the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a Registered Professional Engineer in the Province of Ontario. He is a Fellow of the Engineering Institute of Canada and the Canadian Academy of Engineering. He is a Distinguished Lecturer with the IEEE Vehicular Technology Society and the IEEE Communications Society.