International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

Privacy-Preserving Scheme for Mobile Public Hotspots in Nested NEMO

A.V.Sujitha

PG Student, Department of CSE , Bharathiyar Institute of Engineering for Women Deviyakurichi ,Attur ,TamilNadu ,India

sujitha.av@gmail.com

***Abstract*— Mobility and physical-layer protection is one of the challenging research issue in vehicular ad-hoc network. 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. 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. physical-layer attackers can easily localize the MNNs by measuring their received signal strength (RSS). By modifying 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 sub schemes, and Nested NEMO, and its goal is to confuse the attackers by increasing the estimation errors of their RSSs measurements and, hence, preserving MNNs' location privacy and in which MNNs are controlled by an MR, which, in turn, is controlled by another MR .**

***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 (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 vehicleto-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.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

TABLE I
ABBREVIATION DEFINITIONS

d	Distance
MNN	Mobile Network Node
MR	Mobile Router
NEMO	Network Mobility
OBU	On-Board Unit
RPi	Reference Point I
RSS	Received Signal Strength
RSU	Road Side Unit
VANET	Vehicle Ad hoc Network

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, 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 variability is difficult to mitigate.

The fake point–cluster-based scheme combines two independent sub schemes, i.e., fake point and cluster based. The idea of the fake-point sub scheme 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 sub scheme 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 analyse 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 sub scheme 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 sub scheme with the fake-point sub scheme to decrease this probability. In addition, through extensive simulations, we show that our fake point–cluster-based scheme achieves 23%

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

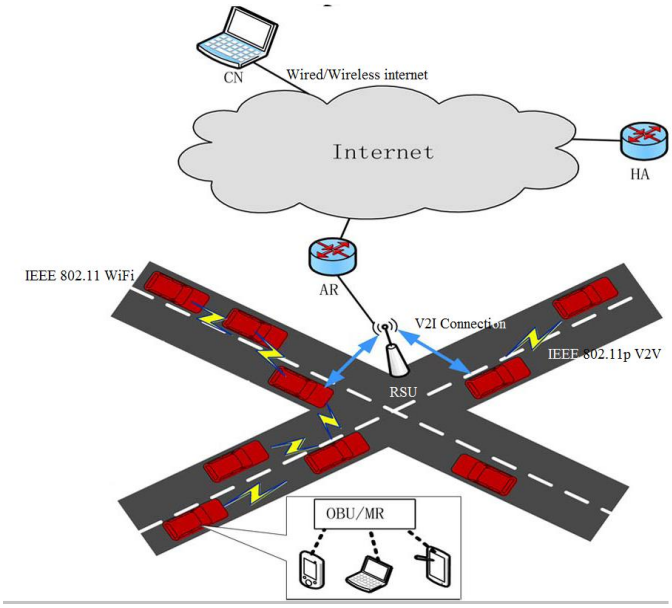

Fig. 1. NEMO based VANET

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 and . The proposed fake point–cluster based scheme and Nested NEMO is introduced in Section III. The security analysis and the performance evaluation are introduced in Sections IV. Finally, conclusions and future work are presented in Section V.

II. EXISTING SYSTEM

A. Wireless Position Estimation

To estimate the wireless position we use two steps to achieve

1) Distance measurement

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 .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., $\bar{}p$, as

$$\bar{}P(d) = P0 - 10n \log(d/d0)$$

where P0 is the received signal power from a known location that is located at distance d0 from the reference point, and n is the path loss exponent, which depends on the propagation model of the signal in the wireless environment. We need to consider about the received power also because it can be affect due to shadowing and fast fading .So the received power is modelled to include the path loss modelled in and the shadowing modelled as a zero-mean Gaussian random variable with variance σ2 to consider the variability of the signal fading conditions. The RSS measurement can be modelled as

$$P(d) \sim N(\bar{}P(d), \sigma 2)$$

After measuring the RSS at reference point i located in (xi, yi), the estimated distance to the sender, i.e., fi(x, y), is measured as

$$fi(x,y) = ((x-xi)^2 + (y-yi)^2)^1/2$$

2) Location estimation

For location estimation we need to use two techniques

Mapping (fingerprinting) **:** 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 .

Geometric and Statistical: 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.

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

B. Fake-Point Location Privacy Sub scheme

The proposed fake-point location privacy scheme is employed to protect MNNs' physical location privacy from insider passive attacks. 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.

The probability of having at least two MNNs choosing the same fake point's location that contains an attacker's monitoring device is calculated by 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.

$$Pr(x \geq 2) = 1 - (K!/(K-u)!\ K\hat{}u)$$

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

$$Pr(\text{fake point}) = [1-(K!/(K-u)!\ K\hat{}u)](A/K)$$

Since the number of passengers inside the hotspot is always much less than the defined spatial grid points (u K), we consider $K!/(K - u)!Ku \approx 0$. Therefore, the probability of successfully attacking the hotspot when employing the fakepoint sub scheme is calculated as

$$Pr(\text{fake point attacking}) = 1-(A/K)$$

MNN Attachment: To connect to the available hotspot, the MNN first calculates distance d MNN−AP to its AP as

$$d_{MNN-AP} = [(X_{MNN} - X_{AP})\hat{}2 + (Y_{MNN} - Y_{AP})\hat{}2]\hat{}1/2$$

where (XMNN, YMNN) 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., Pu, the MNN calculates its transmission power, i.e., Ptr, as

$$Pu = \alpha - 10\beta \log (d_{MNN-AP})$$

Where, β is the path loss and α is a function of transmission power Ptr. Instead of using the calculated transmission power, i.e., Ptr, the MNN uses another power, i.e., P′tr, calculated related to a fake location that the MNN selects in the next step

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

$$P_{ftr} = f(P'_{tr}) - 10\beta \log (d_{MNN-F})$$

$$d_{MNN-F} = [(X_F - X_{MNN})\hat{}2 + (Y_F - Y_{MNN})\hat{}2]\hat{}1/2$$

While using the above methods 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.

C. Cluster-Based Location Privacy Sub scheme

Another sub scheme to achieve MNN location privacy in NEMO -based VANET. That the probability of successfully violating the MNN's location privacy, when our proposed fake-point sub scheme 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 sub scheme; 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 sub scheme 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 sub scheme consists of three steps

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

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 divide s the network area into smaller n sub areas called cells, i.e., c1, c2, . . . , cn. For each cell, i.e., ci, the OBU/MR assigns an AP, which is a reference point RPi that works as a local AP for all MNNs located within distance r around RPi. 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.

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, IDRP, its coverage area's radius, r, and its required received signal's power, PRRP . Considering the knowledge of its location, i.e., (XMNN, YMNN), the MNN calculates the transmission signal power for its messages directed to its chosen RP as

$$FSPL\ (DB) = 20 \log10(r) + 20 \log10(f) + 32.45$$

$$TPMNN = PRRP \times FSPL$$

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

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. 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.

III. PROPOSED SYSTEM

D. Fake Point–Cluster-Based Location Privacy Scheme

To increase the MNN's location privacy, a combination of the fake-point- and cluster-based sub schemes 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., {(XRP1, YRP1), (XRP2, YRP2), . . . , (XRPm, YRPm)}. 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 sub scheme, 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 sub schemes prevents some attacker's monitoring devices located inside neighbor clusters from detecting the sender's transmitted signals. In addition, the fake point–cluster-based sub scheme selects a fake point inside the sender's cluster to ensure higher location privacy and consume lower power.

E. Nested NEMO based privacy scheme

This is a scheme of route optimization with location privacy (ROLP) in nested mobile networks. Proposed scheme achieves better throughput, and reduction in End-to-End Delay as compared to NEMO Basic Support Protocol. Nested NEMO, in which MNNs are controlled by anMR, which, in turn, is controlled by another MR. The challenge in this scenario is the high message 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.

IV. PERFORMANCE EVALUTION

Here, NS2- has been conducted to evaluate the performance of the fake point–cluster-based scheme. We simulate a 45x45m hotspot installed inside one vehicle. To create VANET communications, we consider six vehicular sub networks, each of which is covered by one RSU, and vehicles inside the VANET can roam from one sub network 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., *RPi*, covers an area of 25 m2, with 1-m overlapping area with each neighbour 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.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

TABLE III
SIMULATION PARAMETERS

Road width	5500m x 10m
Road's network size	1000m x 10m
Road's network number	6
Vehicle number	36000
Wi-Fi size	45m x 45m
Wi-Fi node number	600
Frequency	2.4GHz
AP transmission power	5mW≈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. 2 shows the MNN transmission power for the fake point–cluster-based, fake-point sub scheme, cluster-based sub scheme, 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 sub scheme 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 sub scheme 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 sub scheme, when combining the fake-point sub scheme with the cluster-based sub scheme, 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 increasingMNNs' 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 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.

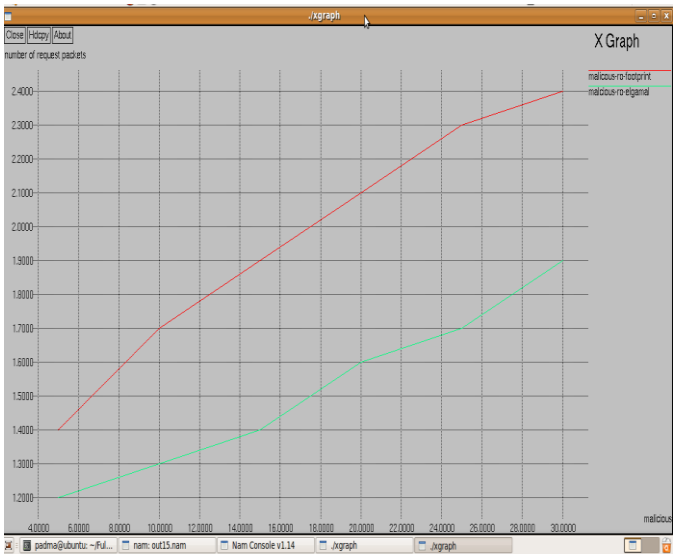

Fig. 2. Fake Point–Cluster-Based Location Privacy Scheme

The increases in distances and power are our cost to achieve high MNN location privacy. 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.

V. 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

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 3, 2014. ISSN: 2348-6600
Reference ID: IJCS-044. PAGE NO: 249-255.

to apply our proposed scheme o other NEMO scenarios, such as nested NEMO, in which MNNs are controlled by a 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.

REFERENCE

[1] 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.

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

[3] 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, pp. 1–6, Jun. 6–8, 2007.

[4] 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.

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

[6] 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.

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

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

[9] 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, pp. 246–257, 2007.

[10] 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.