ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Survey on Privacy Preserving Scheme for Hotspots in VANETS

Balasubramanian.C [#1], Vijayalakshmi.G [#2]

[#]Department of CSE, P.S.R.Rengasamy College of Engineering for Women, Sivakasi, India

[#]Department of CSE, P.S.R.Rengasamy College of Engineering for Women, Sivakasi, India

ABSTRACT— Vehicular Ad-hoc NETworks (VANETs) has more significant interest and growing with the today's research efforts towards protecting the network from attackers to reach the adequate level, for the drivers and manufacturers to attain infotainment and safety of life. Due to open nature of wireless network, the adversary can easily attack the networks. The vigorous VANET has the need of dependability with their privacy and security features. Nested NEMO based VANETs (NN-VANETs) is a new approach that combines the NEMO protocol with VANETs. NN-VANET has the challenge of high routing delay. The study examines the incidence of physical layer attack and the various preserving technique by studying the existing research ideas and modify them like modified obfuscation technique and power variability ideas to increase the privacy as high. This paper concludes with possible future research fields of privacy preservation.methodologies used to preserve the privacy at physical layer. The existing research work has some inconsistencies, limitations or problems while achieving the privacy by using the existing techniques such as changing power and obfuscation techniques. The main goal of this survey is to propose a new privacy

KEYWORDS— VANET, NEMO, Privacy, NN - VANETs

I. INTRODUCTION

In recent years, there have been significant interest in the field of Mobility Management for Vehicular Networks [1] achieves flawless communications for mobile nodes (MNs) from both academic world and industry. Car-to-Car Communications Consortium (C2C-CC) and standardization organization IETF have been working on various issues in VANETs. C2C-CC [2] aims to develop an open industrial standard for inter-vehicle communication using wireless LAN (WLAN) technology.

For example, IEEE 802.11p or dedicated short range communications (DSRC) is an extension of 802.11 standards for inter-vehicle communication by IEEE working group.

IETF has standardized NEtwork MObility Basic Support (NEMO BS) for network mobility in VANETs [1], [3]. Mobility management protocols, such as Mobile IPv6 (MIPv6) and network mobility (NEMO) protocols, which are used to assurance the global Internet connectivity and mobile data services for MNs. 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. Both domains are used for safety applications.

In addition, non safety VANET applications, such as service infotainment and Internet access, have recently received a great deal of attention, particularly with the explosion of public hotspots installed inside large vehicles. Mobility management includes location management and handoff management Location management has the functions of tracking and updating current location of mobile node (MN). The proliferation of Wi-Fi hotspot a large van (bus, train, or plane) is called a NEMO-based VANET. 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.

In Nested NEMO based VANET [3], one MR controls and provide service to the other MR that resides on the another vehicle and so on (i.e.) Nested NEMO means that $(NEMO)^n$. It is hard to define privacy in a way that is broadly accepted. As new technological advances open up new ways of how privacy can be affected, we need to continuously reassess our understanding of privacy and how it should be protected.

By measuring the Received Signal Strength (RSS), 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. The 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. The fake point–cluster-based scheme is proposed to confuse the attackers by increasing the estimation errors of their RSSs measurements. Thus by the scheme achieves the privacy on Physical Layer Location of Mobile Public Hotspots. To analyze the location privacy scheme, there are three different metrics, namely, correctness, accuracy, and certainty are used.

II. Security Requirement

A. Privacy

Keeping the information of the drivers away from unauthorized users, this information like real identity, trip path, speed etc… The privacy could be achieved by using temporary (anonymous) keys, these keys will be changed frequently as License Plate) is used, this license is installed in the factory for every new vehicle; it will provide an identification number for the vehicle. With the RFID technology [4] to grip the ELP it is used to identify the vehicle in anywhere. In case, when the police or any official wants the real identity, it can take an order from the judge and that can recover the specific vehicle's ELP identity.

B. Physical layer

The network has the physical layer as the bottom or lower level layer, it pass the data as raw bits rather than the logical data. It transmits data as signal to the Physical Layer (PL) of other network whereas, Data Link Layer (DLL) acts an interface between physical layer and Network Layer (NL). The physical layer can be easily attacked by the adversaries by measuring the RSS (Received Signal Strength) since; it passes the data as signal. And each signal may have the frequency for transmission. These transmitted signal strength are monitored and is used for find out location of mobile user with in the hotspots area.

Location Based Server (LBS) is an application server which is used to exploit the information about the user's location. For instance, the information about the can be used to notify a grouping of friends where and when a pal is near in the neighborhood or to insist optimal routes for the automobile drivers. Conventionally, computer network security has various aspects of message authentication, confidentiality and integrity. But the wireless network has the issue of location privacy because the drivers move between different media and network.

III. Taxonomy Of Existing Techniques

A. Hyberloc scheme

R.El-Badry et al proposed the technique Hyberloc to preserve the privacy at physical layer of the mobile public hotspots inside on the vehicle. The paper [5], describes that the Hyberloc scheme is used to prevent the attacker localizes the victim MNN by measuring its RSSs. 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. While maintaining high localization accuracy at trusted nodes, the scheme used the idea of dynamically changing of their transmission power value following certain probability distribution for anchor nodes, regarding the accuracy of localization at un-trusted nodes.

By using the Additive White Gaussian Noise (AWGN), the Probability Density Function (PDF) of RSS is:

$$\frac{1}{2\mu^2}\exp\left(-\frac{rss+ct}{2\mu^2}\right)I_0\left(\frac{\sqrt{rssct}}{\mu^2}\right) \quad ------(1)$$

where

rss – received signal strength.

c – channel gain which is a function of distance.

t – transmission power

$2\mu^2$ – total variance of noise.

$I_0(x)$ – modified Bessel function of order 0.

To make the estimation error on the measurement of RSS the likelihood function (E) is used with the independent measurements and expressed as:

$$E=\prod_{i=1}^{k}\frac{1}{2\mu^2}\exp\left(-\frac{rss_i+ct_i}{2\mu^2}\right)I_0\left(\frac{\sqrt{rss_ict_i}}{\mu^2}\right) \quad -----(2)$$

Based on the values of c and $t_{i,}$ the E can be maximized to confuse the attacker and prevents the privacy at the physical layer of the mobile public hotspots in VANETS.

In the Hyberloc scheme, changing the transmission power values is considered to provide only weak location privacy, since the attacker can easily fix these changes by multiplying the RSS at all monitoring devices by a factor.

B. Hidden Anchor

M.youssef et al proposed the hidden anchor technique to preserve the privacy of mobile nodes inside the hotspots in VANETs. The paper [6], states an algorithm

(Hidden anchor) to provide the physical layer location privacy for different classes of localization algorithms. The Hidden Anchor algorithm uses the noisy wireless channel and identity to take duplication of neighboring trusted nodes and thus by make anchors unobservable to un-trusted nodes while granting complete information to trusted nodes. Evaluation of the Hidden Anchor algorithm through analysis and simulation prove that it can hide the identity, and hence the location, of anchor nodes with low overhead. In addition, the results show that by adding mock noise, and can achieve considerable progress in anchor & a position's location privacy.

The localization error and the RSS measurement error can be achieved by the following equations:

$$E_{lerr} = l_s + rand_{i=1}^{k}(l_f) \quad ------ (3)$$

$$E_{serr} = \sum_{i=1}^{k}(tp_s + t'p_f) \quad ----- (4)$$

The equation (3) and (4) are used to calculate the estimation error on the location of sender point and the estimation error on the received signal strength respectively.
Where
E_{lerr}- Estimation error of localization
l_s – location of sender
l_f –location of fake sender
E_{serr} – Estimation error of signal strength
tp_s – transmission power from original sender
$t'p_f$ – transmission power from fake sender

Hidden anchor Scheme, which relies on adding noise to the transmitted signals. In this scheme, the anchor nodes use their neighbors' identities to hide their own identities from distrusted nodes. At the same time, encrypt and attach their real identities in the transmitted packets sent to trusted nodes. Obfuscation, *i.e., concealment is* another way to protect a user's location privacy from location based servers (LBSs).

In the Hidden anchor scheme has the drawback of "changing the nodes' identities does not achieve a sender's physical-layer privacy". "Adding noise to the transmitted messages affects transmission quality". "Obfuscation schemes are not appropriate for Wi-Fi scenarios".

C. VANEMO (NEMO meets VANET)

R.Baldessari et al proposed VANEMO technique which deals with the deploy-ability analysis of the mobility of network in Vehicular communication. The paper [7], that the creation 'VANEMO' which is the integration of VANETs and the NEMO protocol. The major consideration of VANEMO is to define the requirements of deployable system architecture in terms of economic, functional and performance facets.

VANEMO deals with the observation of VANET as the traditional model such as MANET (Mobile Ad-hoc NETwork) ie., VANET as MANET, to They regard the vehicular network as a conventional mobile ad hoc network (VANET as a MANET), simplify the possible solutions and categories them into two ample approaches such as MANET centric approach and NEMO centric approach. Since the integration approach can help to preserve the privacy at physical layer of the system with their specialized merging scenario.

In this proposal, the two MANET and NEMO centric approaches were analyzed in the basis of basic requirements of VANET. And this has the conclusion of MANET centric approach meets the basic functional requirements, deployable cost and performance requirements better than the NEMO centric approach.

With the use of MANET centric approach in NEMO based VANETs scenario, it has the problem while preserving the privacy at physical layer since, the current and past locations of mobile users can easily identified by the attackers. The MANET centric approach is the best suited integration scheme for NEMO based VANETs. For Nested NEMO based VANETs, the NEMO centric approach is used to integration of VANETs and NEMO.

D. Novel Anonymity on Link layer

T.Wang and Y.Yang proposed the mechanism to implement the mutual authentication protocol with verifiable link-layer location privacy. In this paper [8], the novel anonymous mutual authentication protocol is proposed to achieve the provable link layer location privacy. The design of proposed protocol ie., mutual authentication protocol has the intention of attaining the mutual authentication between the the Access Point(AP) and Mobile Unit (MU) with link layer forward secure location privacy scheme

The secure location privacy is forwarded after the security model is formulated on the link layer. The novel anonymous mutual authentication protocol is proposed between the MUs and the access point (AP) based on the devised keys with location and time awareness.

In this paper, the formal security model was introduced on link layer. The forward secure location privacy aims to attain the anonymous communication in wireless networks. This security model for location privacy is by the fact that an attacker still cannot learn how long an MU has resided at the current location, although he alters the MU's current location privacy.

Based on the security model, a novel anonymous mutual authentication protocol between the AP and each MU has been proposed by considering the advantages of location- and time-aware keys. They had also developed a forward-secure location privacy protocol at the link layer and proved that the location privacy is tightly related to the symmetric encryption semantic security according to the provable security technique. This scheme has the drawback of the revocation cost and the certificate updating overhead are high.

E. Antenna Synthesis scheme

T.Wang et al proposed the antenna pattern synthesis model to protect the location privacy from Received Signal Strength (RSS) localization system. In the paper [9], the problem of location privacy protection in wireless

LAN (WLAN) environment is discussed. In which the received signal strength (RSS) at access points (AP) can potentially be obtained by adversaries to obtain the location of a legitimate mobile station.

A two-step location privacy protection scheme is using a linear smart antenna array on the mobile station. Current RSS localization techniques can be generally grouped into fingerprint based approaches and propagation model based approaches.

Fingerprint localization usually consists of an off-line phase and an on-line phase. Before the positioning system can operate, the off-line phase is required to collect Received Signal Strength (RSS) measurements at known locations and a database is built up for pattern matching. During the on-line phase, the actual RSS measurement of the target mobile station is compared with the stored database to return location estimation. Fingerprint of wireless signal highly depends on the specific environment and is not transportable to different places. Consequently, for every different interested area, the off-line phase must be conducted from the very beginning. Additionally, any change of the infrastructure distribution and the physical environment will necessitate an update of the localization system and the collection of new training data.

In propagation based RSS localization schemes, large scale path loss is related to the distance. Location Privacy Protection Using Antenna Pattern Synthesis between the transmitter and the receiver. Obstacles and noise can also be taken into account in the model. Then given the path loss from the transmitter to the receiver, the distance between them can be estimated and the location of the transmitter can be computed.

The weakness of fingerprint localization is that it requires lots of human work and is time consuming and also the attackers can easily collect required information from target users.

F. Phantom Approach

S.Oh, T.Vu et al proposed the phantom technique to achieve the physical layer cooperation for the location privacy protection. In the paper [10], Phantom, a novel approach is proposed to permit mobile devices thwart unauthorized adversary's location tracking by creating fake locations.

Phantom influences the cooperation among multiple mobile devices in close vicinity. It utilizes synchronized transmissions among those nodes to confuse localization efforts of adversary systems. The estimation error of the RSS can be achieved from the following equation:

$$err = \sum_{i=1}^{k} tr_s + tr_{g_i} \quad ------(5)$$

Where

tr_s – transmission power of sender

tr_{g_i} - Transmission power of ghost

err – estimation error of RSS

This scheme Phantom was proposed to protect wireless users from adversaries who try to localize users without their permission. Phantom enables users to dynamically create confusion about their location by creating additional ghost transmission from different locations with the same identity. We introduced protocols for generating such ghost nodes through simultaneous transmissions from multiple nodes. It also implements a proof of concept using software defined radios as transmitters and explored issues related to frequency and time synchronization of such transmitters. Through indoor test-bed experiments, we demonstrated the feasibility of inducing localization errors through cooperative transmissions.

This proposal has the weakness of obfuscation schemes are not appropriate for Wi-Fi scenarios.

G. Silent Period Technique

L. Huang et al proposed the scheme [11] called silent period which is used to achieve both link-layer and physical layer location privacy. Its main goal is to thwart the attacks on correlation and hence the attacker cannot correlate the two pseudonyms to the same MNN. The variable length period is consider as constant period ie., silent period in which MNN changes its pseudonym and then keep silent and not sending any messages. After the silent period, MNN starts sending frames for the fixed period of time, the attacker cannot correlate between the old and new pseudonym.

$$RSP = T_d + T_r \quad -----(6)$$

Where

RSP – Received Signal Power

T_d – deterministic silent period

T_r – transmission power that varies between 0 to T_r^{max}

$$T^{min} = T_d \ and \ T^{max} = T_d + T_r^{max} \quad -----(7)$$

Where

T^{min} – minimum transmission power

T_r^{max} - Maximum transmission power

The larger value of T_r^{max} will offer better possible privacy at physical layer of the hotspots in vanets. When the MNN stops its conversation for a period will degrades the network performance. Additionally, it requires the duplicate address detection scheme to know whether the new pseudonym does not conflict with any other address in the network.

IV. CONCLUSIONS

This survey describes the importance of security issues such as privacy at physical layer and the preserving scheme of privacy at mobile public hotspots in Nested NEMO based VANETs (NN-VANETs). This study focused with the security issues for MNN's privacy and describes various techniques, to thwart the physical layer attack on the hotspots. The discussed schemes are applied on the mobile public hotspots like wifi to preserve the privacy at physical layer. The above discussion will bring the new idea about the privacy preservation and limitations of using such schemes on hotspots in Nested NEMO based VANETs.

REFERENCES

[1] 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.

[2] 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.

[3] Sanaa Taha, Xuemin Shen, “A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs” IEEE Transactions on ITS, 2013

[4] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, ” Security Analysis of Vehicular Ad Hoc Networks (VANET)” 2nd International Conference on Network Applications, Protocols and Services, 2010.

[5] 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, 2010.

[6] R. El-Badry, M. Youssef, and A. Sultan, “Hidden anchor: A lightweight approach for physical layer location privacy,” Comput. Syst., Netw. Commun., vol. 2010..

[7] R. Baldessari, A. Festag, and J. Abeille, “NEMO meets VANET: A deployability analysis of network mobility in vehicular communication,” in *Proc. 7th IEEE Int. Conf. ITST,* Sophia Antipolis, France, 2007.

[8] 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.

[9] 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.

[10] S. Oh, T. Vu, M. Gruteser, and S. Banerjee, “Phantom: Physical layer cooperation for location privacy protection,” in *Proc. IEEE INFOCOM,* 2012.

[11] 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

[12] NIST:National Institute of Standards and Technology, 2011. Available: http://www.nist.gov/ index.html.

[13] Pa rno.B and Perrig.A, (2005) “Challenges in Securing Vehicular Networks,” Proc.Fourth Workshop Hot Topics in Networks (HotNets IV), pp125-128.

[14] Plo.K¨ ßl, Nowey.T, and Mletzko.C, (2006) “Towar ds a Security Architecture for Vehicular Ad Hoc Networks,” Proc. First Int’l Conf. Availability, Reliability and Security (ARES ’06), pp. 24-29.

[15] U.S Department of Transportation, “Vehicle safety communications project task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC,” http://www.its.dot.gov/research docs/pdf/59vehicle-safety.pdf, March 2005.