**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 2, February 2014, pg.645 – 652*

**RESEARCH ARTICLE**

# SECURE NETWORK SHARING NEMO BASED AD-HOC

**V.Pavithra[1], M.Mohankumar[2]**

Applied Electronics, Sri Eshwar College Of Engineering, Coimbatore
Electronics and Communication Engineering, Sri Eshwar College Of Engineering, Coimbatore

[1] pavithrasreep218@gmail.com; [2] mail2mohanphd@gmail.com

***ABSTRACT** the paper analyzes the deploy ability of approach for Network Mobility (NEMO) in wireless Vehicular Ad-Hoc Networks (VANETs).The vision for VANETs is road safety and commercial comfort application enabled by short range wireless technology. A Network Mobility (NEMO) based VANET is a new intend to integrate the NEMO based VANET. The advance of NEMO based VANET is a tracking system to prevent attackers from localizing the user inside the hotspot in a vehicle. It is used to communicate between roadside unit (RSU) and vehicle to provide the internet access in a public transportation system (e.g. bus, train) by using different mobile networks (MNN). The passengers can enjoy the full internet access such as cell phone and physical assistants. Because of the open wireless network environment the attackers present in the OSl model can easily localize the mobile networks nodes by measuring their received signal strength (RSS). In these papers modify the scheme called concealment and by using the idea of power variability, proposed a new scheme, (i.e.) Fake point and cluster based sub scheme, its goal to confuse the attackers by increasing the estimation error in received signal. By using correctness, certainty, metrics, the fake point based sub scheme targets the higher MNN's secured location the number of grid points decreases. The annexation simulation shows the fake point cluster based scheme archives 23% and 37% decrease in the sender power with MNN's route length and also compared with fake point sub scheme.*

***Keywords**— Network Mobility (NEMO) Based VANET, Physical Layer Location Privacy, Physical Layer Security*

## 1. Introduction

The vehicular ad-hoc networks are known as VANET. The vehicular ad-hoc networks are currently used in both industries and academic. The aim of the VANET is to improve the road safety and traffic efficiently and comfort. The network

 

enthusiastic to communicate between vehicle and roadside units. The mobility management for vehicular networks attain unified communication for mobile nodes (MN)., and protocol such as mobile ipv6(mipv6) and ipv4(mipv4) and network mobility (NEMO) . [1]The NEMO protocol is a type of IP which is created by internet engineering task force for standard communication protocol is used to design and allow the mobile device to move from one network to another network by maintaining the same IP address .the NEMO protocol is used in guarantee localize internet connectivity and mobile data service in MN. It is the standard organisation used in car-to-car communication syndicate and also support intelligent transportation system application including real-time traffic video streaming in VANET there are three types of communication vehicle to vehicle to vehicle to infrastructure, vehicle to roadside. Vehicle to Vehicle (V2V) communication approach is mainly for short range communication. It is fast and reliable.[4] Vehicle to infrastructure (V2I) approach provides the longer range communication .vehicle to roadside (V2R) approach communicate with roadside for broadcast the message to vehicle.[6] But in this paper we are considering only the vehicle to infrastructure to mate use for previous infrastructure networks and these domain mainly used for safety such as road accident and weather warning. It also includes non safety purpose in service infotainment and internet uses, have a currently received a great deal of considering especially with the propagation of public Wi-Fi hotspot equipped inside a large vehicles (i.e train, bus or planes).[4] Having the same aim for supporting universal internet connectivity the mobility management protocol can be divided into host mobility and network based mobility. In host mobility the protocol such as Mipv6 every traffic destined to the MN will be encapsulated in Ipv6-in-IPv6 tunnel and send to the COA of MN So the network involvement in mobility is minimal. But in network mobility protocol such as proxy Mipv6 it does not require any modifications of mobile nodes (MNs).[7]No requirement for modification of MNs is expected to accelerate deployment of PMIPv6,it also manage mobility migrating network as one unit. so NEMO is the suitable trend shown in figure 1,the Wi-Fi hotspot is assembled in large vehicle such as (Train, bus) it is called NEMO based VANET.[6] In such network the OBU works as a mobile router (MR) to support a group of mobile networks nodes (MNNs) located for vehicle with communications.[8]

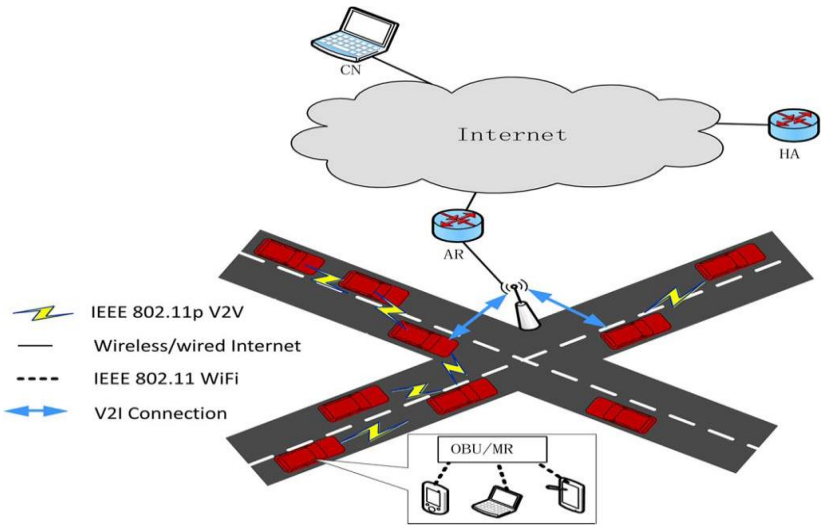


**Fig 1 NEMO based VANET**

So maintaining the user location secrecy in such public Wi-Fi hotspot for NEMO based VANET is a dispute. Resist a mobile user's location isolation may lead in some cases to losing their life[10]. In NEMO based VANET, the information effusion at a physical layer is important to ensure the user's location secrecy in wireless environment, even though secret with data link layers. However it is an open nature of wireless surrounding, a attackers present in the OSI model can easily localize the user's

 

by receiving signal strength (RSS) of the user's. [2] By using isotropic antenna, the mobile device inside the Wi-Fi hotspot cannot hide the transmitted signal to the OSI model. By using cheap equipment such as received signal strength indicator the OSI model can identify the mobile user's location. The internet protocol (IP) layer security can be equipped for physical layers some scheme are limited in power variability which has different power in transmitted signal. This scheme is called triangulation. To overcome these schemes called obliteration and by idea of power variability it is used to confuse the attackers by error in the receiving signal.[11]

## 2. CONTRIBUTION

To confuse the attackers we are creating a fake point cluster based scheme .it has two independent scheme.,, fake point sub scheme and cluster based sub scheme .In a fake point sub scheme passengers in a vehicle , each senders selects the random point, these is known as fake point. However, a passenger in a hotspot selects the same fake point, so the attackers received a error signal to confuse the attackers. Thus the attackers calculate the wrong sender's location. So sender's locations are protected. The cluster based sub scheme also extent the monitoring devices to detect the senders received signal and it also decrease the accuracy of the attackers systems [5]. Therefore proposed scheme involves the combination of both cluster based sub scheme with fake point sub scheme to reduce the probability of the system. Through the simulation it also extent the fake point cluster based sub scheme targets higher 23% and 37% reduce in average power senders and MNN-AP routing path compared to fake point sub scheme to get a fake point cluster based scheme [1].

## 3. NEMO Based VANET

Now a day's Mobile IP (MIP), it is design for moving a single IP device from point to point on the Internet without dissipate any superior level connections. However, with the propagation of IP it always remain connected to the Internet the entire networks of IP devices moving calm from one place to another.[4] By using standards mobile IP it is possible to implement mobility for these entire device. However this would require all devices to be capable of Mobile IP and generate excess overhead as every device has to perform Mobile IP functions. Another solution to the problem is Network Mobility (NEMO). NEMO works by moving the mobility functionality from Mobile IP mobile nodes to a mobile network's router. The router is able to change its attachment point to the Internet in a manner that is transparent to attached nodes[6].

## 4. TERMINOLOGY USED IN NEMO

The following area unit vital for understanding the fundamentals of Mobile information process and NEMO can be used throughout[12].

Access Router (AR): Mobile router access the net through a router.

Care of Address (COA): It is a mixture of two IP address .mobile router and internet attachment point.

Correspondent Node (CN): Mobile network node communicate via IP through every IP device.

Foreign Agent (FA): The NEMO familiar with the access router and serve to support mobile router.

Home Agent (HA): A moderator on the home network permits the mobile router to roam.

Home Network (HN): A Network of the Mobile Router does not roam but the network associated with home agent of network link.

Mobility Agent (MA): Each IP device combines Mobile Router and Home Agent to achieve the mobility functions.

Mobile Network Node (MNN): The MNN's does not need knowledge about the network mobility; the MNN's had permanent address to the mobile networks.

 

Mobile Node (MN): An IP device changes its attachment point to access an internet which maintains the higher connectivity in a mobility function.

## 5. RELATED WORKS

The wireless network as the open nature environment by hiding the transmitted wireless signals is a great challenging goal. The MNN measures the received signal strength in certain reference point while attackers localize the signals. To confuse the attackers a new strategy sensor network called Hyberloe. In these schemes the secret nodes protect their location from uncertainty nodes. However the assurance nodes can easily confine the anchor nodes. The idea of Hyberloe to select the random power value used in transmitted signals to transmit encrypted packets. The hyberloe shared key used only for the trusted nodes to identity the sender true location. The attackers can easily fix their value by multiplying RSS at all monitoring device .so we are considered the transmission power value only at weak signals. So it used to confuse the attackers by measuring their RSS be equal to different MNN. It is very difficult to the increasing the power for attackers.[8]

## 6. SYSTEM MODELS

### *A) FAKE POINT CLUSTER BASED SCHEME*

In the fake point cluster based scheme it has two independent schemes fake point sub scheme and cluster based sub scheme. These two sub scheme can be separately secure the location of the mobile networks nodes inside the Wi-Fi hotspot NEMO based VANET.[5] The fake point sub scheme targets as superior region level .the attackers can monitor the devices which are located at the same fake point area. In cluster based sub scheme it target superior secure region and also preventing the monitoring device to detect the transmitted signal to user location privacy scheme.[7] We proposed scheme called Fake point cluster based increasing the MNN location secure level and also compared each sub scheme level explained below.

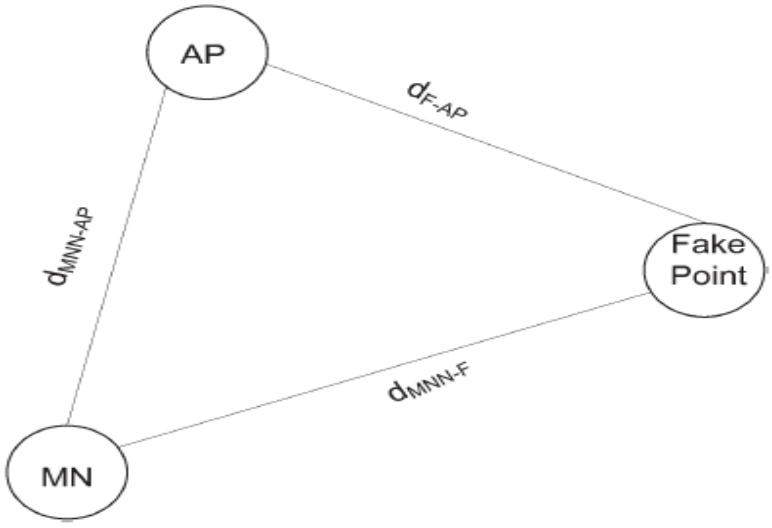


**Fig 2 fake point scheme**

### B) *FAKE POINT AND CLUSTER BASED SUB SCHEME*

The intended fake point locality secure strategy is occupied to protect the MNN's the substantial localities secure inside the Wi-Fi hotspot NEMO based VANET. The idea inside the hotspot the MNN selects the fluky location and used to

 

confuse the attackers called fake point. Depending on the blunted the MNN regions have deviation and secure the ensured region. The intended another sub scheme to fulfil MNN region secure in NEMO based VANET. The feasibility of success infringes the MNN's region privacy our intended fake point sub scheme occupied.[10] When the number of attackers monitoring devices decreases at the ratio (A/K) and number of spatial grid points increase at K, then K is larger than A. The idea of the cluster based sub scheme is separate the Wi-Fi hotspot area in to shorter cells; Cluster assigns a new AP for each cell. The MNN's prevent the allocation by monitoring the devices to detect the transmitter signal and it was little power to transmit the message and get confused by increasing the estimation error the RSS.[11]

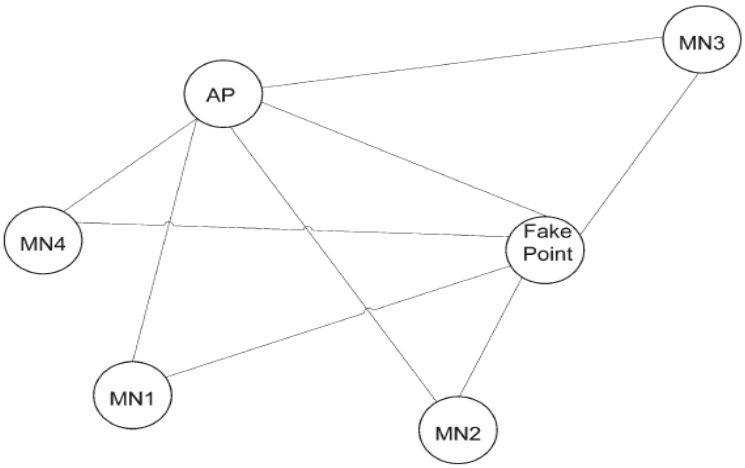


**Fig 3 cluster based sub scheme**

**C)** ***FAKE POINT CLUSTER BASED LOCATION IN PHYSICAL LAYER SCHEME***

In cluster based sub scheme the cluster extend when the MNN transmitted signal can be accepted the information from many cluster but not only engaged cluster. If any attackers monitoring the device in the cluster, the cluster having the monitoring device will send the information to the MNN's signal to intrigue to admit by statistical positioning scheme.[5] The synthesis of fake point and cluster based sub scheme can be adapted to increase the MNN region. [7]These two sub scheme prevents the attackers inside the hotspot detect the sender to transmit the signal, it also includes the fake point cluster based sub scheme select the fake point randomly in a cluster to achieve the higher privacy and consume lower power.[6]

## 7. PERFORMANCE EVALUTION & RESULTS

Here a NS2 simulation has been conducted to judge the performance of faux purpose cluster theme .we have to require price of hotspot purpose to simulate 45m*45m that area unit put in within a 1 vehicle and VANET communication to be created, we have a tendency to area unit considering six vehicle sub network, is roofed by one RSU ,vehicle within the VANET is employed to cast from one sub network .the hotspot features a mounted location and vehicle have linear quality model . The hotspot in AP is AN one hop communication to simulate faux the imbricate cluster and cluster of reference has been dispose such how every reference covers 25min 1m overlapping space in every Neighbour cluster.[12]

 

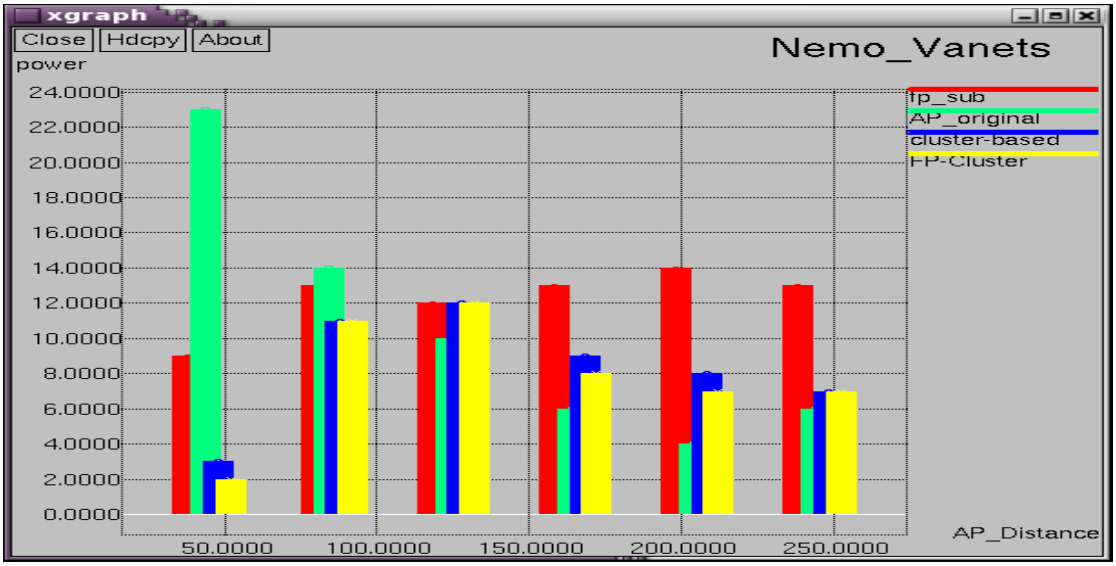


**Figure 4 Power Vs AP-Distance**

Figure 2 shows power consumed at different MNN-AP distances. The 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.

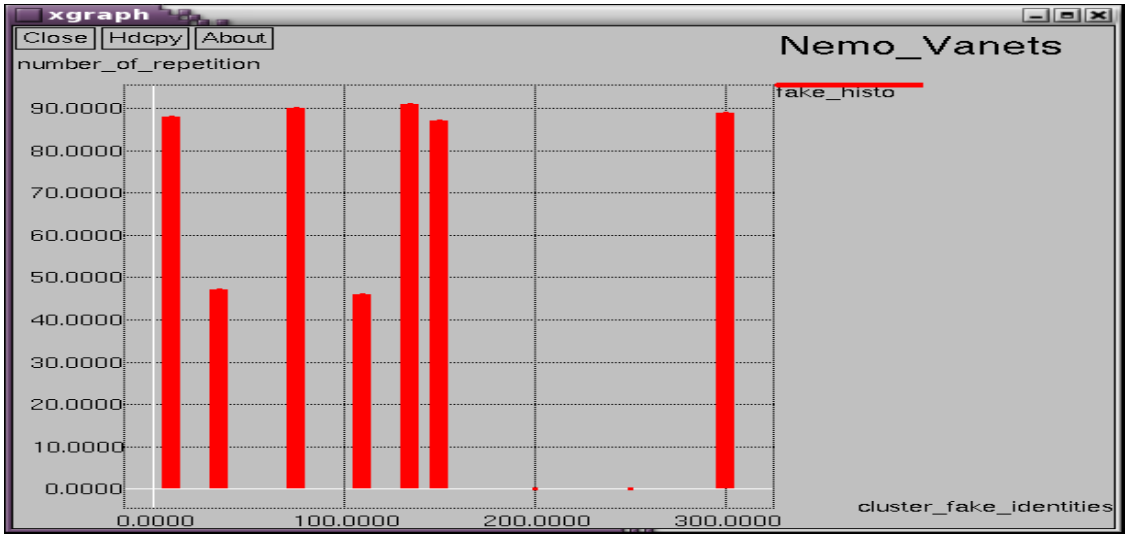


**Figure 4 Number of Repetition Vs Cluster Fake Identities**

Figure 4 shows the number of MNNs that select the same point reaches six, This difference occurs because, in the fake-point sub scheme, 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 neighbour clusters.

 

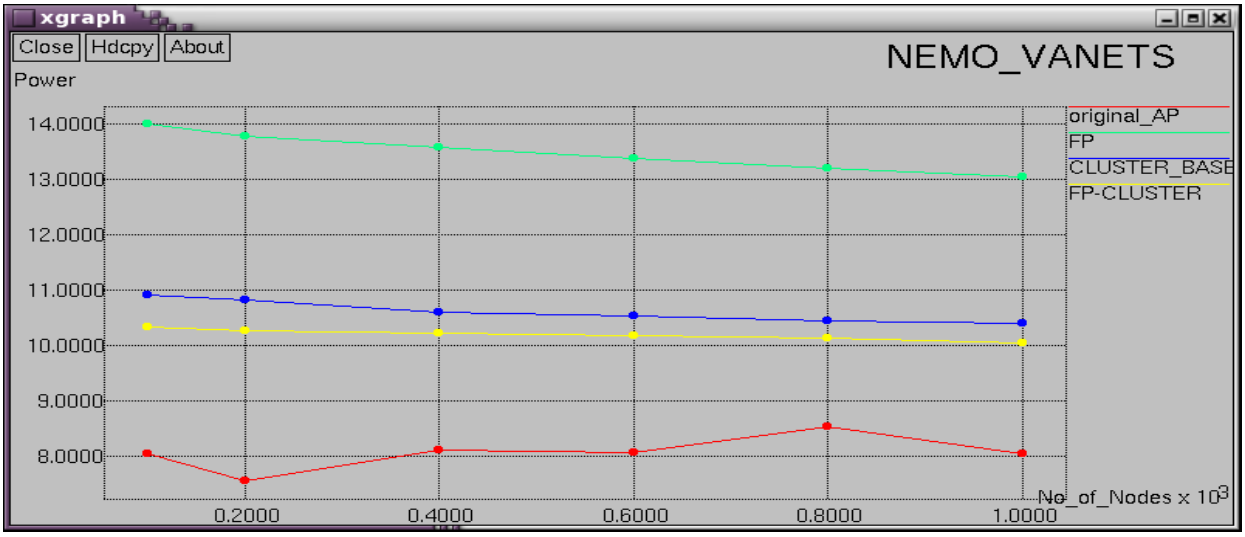


**Figure 5 Power Vs Numbers of Nodes**

Figure 5 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 reference. The original communication scheme, where a fake point–cluster-based scheme is not implemented, has the smallest transmission power.

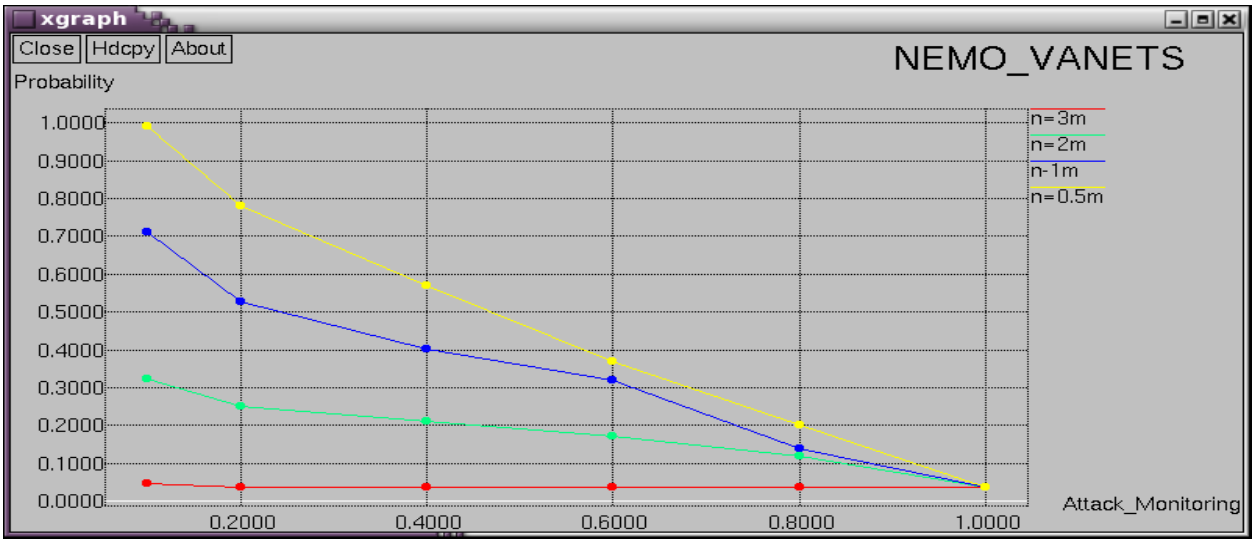


**Figure 6 Probability Vs Attack Monitoring**

Figure 6 shows the maximum number of overlapping clusters and, hence, number of attacker monitoring devices, is four. Combining the fake-point-based with cluster-based probabilities, get the probability of achieving location privacy with a fake point–cluster-based scheme.,

## 8. CONCLUSION

In this paper ,we have powerful an facility physical layer location privacy theme i.e. the faux purpose cluster primarily {based} theme to stop the physical layer attackers and attain MNN's location privacy for mobile by install a public hotspot in vehicle NEMO based VANET. The faux purpose Cluster based mostly theme target senders location privacy by confusing the attackers and additionally increase the senders RSS. In moreover, planned a theme are often enforced by high chance of getting 2 nodes

 

choose a same faux purpose and additionally increase the network performance as a result of its less routing delay than quality management protocol.

**REFERENCES**

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

[2]. E. Perera, V.Sivaraman, and A.Senev iratne, ( Apr 2004) "Survey o n network mobility support," SIGMOBILE Mobile Comput. Commun. Rev. , vol. 8 , no. 2, pp. 7–19,.

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

[4]. S. Taha and X. Shen, .( Dec 2011) "Anonymous home binding update scheme for mobile IPv6 wireless networking," in Proc I EEE GLOBECOM , Houston, TX, USA, , pp. 1–5,.

[5]. S. Taha and X. Shen, (Jun 2013 "Fake point location privacy scheme for mobile public hotspots in NEMO-based VANETs,")in Proc. I EEE ICC , Budapest, Hungary, pp. 630–634,.

[6]. Y. Peng and J. Chang, .( Feb 2010) "A novel mobility management scheme for integ ration o f vehicular ad hoc networks and fixed IP networks," Mobile Netw Appl., vol. 15, no. 1, pp. 112–125,.

[7].Krontiris, F. Freiling, and T. Dimitriou(Oct 2010), "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,.

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

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

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

[11].R. El-Badry, A. Sultan, and M. Youssef,( May23–27) "Hyberloc: Providing physical layer location privacy in hybrid sensor networks," in *Proc. IEEE ICC*,Cape Town, South Africa,2010, pp. 1–5.

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

 