Research Journal of Applied Sciences, Engineering and Technology 12(4): 407-414, 2016
DOI: 10.19026/rjaset.12.2380
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 7, 2015 Accepted: August 15, 2015 Published: February 25, 2016

Research Article

Location Privacy using Anonymous Beacon in Vehicular Ad Hoc Networks

Allam BalaRam and Dr. S. Pushpa
Department of Computer Science and Engineering, St.Peter's University, Chennai-600054, Tamil Nadu, India

Abstract: Vehicular Ad hoc Network (VANET) plays a significant role in safety communication and commercial applications. Applications necessitate to track the location of vehicles, have a strong impact on location privacy and security. Ensuring the correctness of location information is essential without it being disclosed to other vehicles. Conventionally, a privacy preservation mechanism disseminates anonymous beacons for providing location based services to the vehicles and it is verified by the Location Server (LS). In VANET, it is crucial to develop a technique that provides security and privacy with minimum overhead. This study proposes a lightweight mechanism called as Preservation of Location Privacy through Anonymous Beacon (PLPAB) that provides location-based services to the users in a secured manner. Initially at the time of registration, a vehicle receives a triplet from LS. The triplet has a short term symmetric key for beacon encryption and decryption and it generates two random integers to evaluate mysterious time-dependent value shared between LS and vehicle. PLPAB includes two mechanisms such as anonymous beacon generation and location verification. In beacon generation, the vehicles broadcast an anonymous beacon at a specific interval for providing the secure location information. Instead of generating the beacon at all the time, it enables a vehicle to generate a beacon adapting to its mobility. Thus, it reduces unnecessary beacon generation, resulting in less overhead. In location verification, LS verifies the claimed location in the beacon by determining the inference of location using signal strength and speed of the beacon originator. The simulation results show that the PLPAB system achieves and preserves a higher level of location privacy on vehicles and is more resilient to attacks when compared to the existing A-VIP scheme.

Keywords: Anonymous beacon, location privacy, location verification, VANET

INTRODUCTION

Vehicular Ad Hoc Network (VANET) is a promising approach and it plays a significant role in expediting road safety, traffic regulation and Location Based Services (LBS) to drivers and passengers. VANET has two types of nodes such as the self-organized high-speed vehicles and the fixed Road Side Units (RSUs) (Fussler *et al*., 2007; Nathan, 2006). The vehicles are equipped with On-Board Unit (OBU) and the RSU is acting as a fixed base station (Lin *et al*., 2008). The drivers should have awareness about their driving environment for taking preventive action about a traffic jam or accident. VANET facilitates two types of communication such as a vehicle to vehicle communication (V2V communication) and vehicle to infrastructure communication (V2I communication) (Lin *et al*., 2008). The vehicles in VANET periodically broadcast traffic messages that contain information about the current location of the vehicle, the speed of the vehicle, traffic, events, road condition, direction and steering angle (Sherali *et al*., 2012). Also, the vehicles send emergency messages such as an accident and the traffic conditions. The emergency messages assist the drivers to manage the unexpected delay in their journey. Despite these advantages, VANET has several security issues such as location privacy and security. Security and privacy are two conflicting issues in VANET.

The vehicles often disclose the identity information and thus susceptible to the location traceability of the vehicle to perform crime, spoofing and accident. Therefore, it is crucial to build security mechanisms that ensure high security and privacy. The vehicle privacy is very challenging and pseudonym verification is indispensable. The VANET should satisfy the two minimum requirements, the pseudonymity and the unlinkability. In a pseudonymity, the received packet should not explicitly contain the sender information and thus, the attacker cannot find the real identity of the sender. In a unlinkability, the messages received from two different vehicles are unlinkable and thus the event

Corresponding Author: Allam BalaRam, Department of Computer Science and Engineering, St.Peter's University, Chennai-600054, Tamil Nadu, India

of the attacker cannot determine the relationship between the received messages. The conventional protocols use LS for providing location related information to the vehicles in a secured manner.

The privacy is a major concern due to the characteristics of VANET such as dynamic environment, limited battery power and also there is no confidentiality of safety information. The vehicles normally use beacon messages for inter V2V communication. The beacon message contains the vehicle's original identity, such as the number plate, the driver name, the current location and the original ID of the vehicle. The attackers can easily trace the beacon messages and identify the location of the vehicles to perform various attacks. The previous approaches provide symmetric and asymmetric keys for encryption and decryption. The work in Malandrino *et al*. (2014) broadcast anonymous beacons to increase the anonymity level. An anonymous beacon does not contain the sender information. The beacons are generated continuously for a particular period increases the network overhead.

This study proposes Preservation of Location Privacy through Anonymous Beaconing (PLPAB) that includes two mechanisms such as anonymous beacon generation and location verification. In beacon generation, each vehicle generates a beacon without the sender information. The vehicle encrypts the beacon using triplet that is received from LS at the time of registration. The latter vehicle receives the beacon and it forwards the beacon report message to the LS. The beacon-report message comprises a report table and signal strength of the beacon. In location verification mechanism, the LS decrypt the beacon and validate the trustworthiness of the beacon by evaluating the inference of location of the beacon originator. The location of inference is determined using the signal strength of the beacon and speed of the vehicle. The LS detects the attack successfully by verifying the location of the vehicle. Thus, the PLPAB system attains high security due to anonymous beacon generation.

Contribution:

- The primary objective of the proposed PLPAB system is to preserve the privacy of the user through anonymous beacon distribution. The PLPAB includes two mechanisms such as anonymous beacon generation and location verification mechanism.
- Each vehicle registers its identity to the LS for getting triplet. A triplet contains a short term key for beacon encryption and decryption and two random integers for counter measurements. The vehicle and LS maintains a time mysterious dependent value.
- In beacon generation, the vehicles generate anonymous beacon to share their location and other events between them. The anonymous beacon does not contain the sender information and it only contains the encrypted location of the vehicle.
- In location verification, the beacon receiving vehicle measures the signal quality and attaches the signal quality with a beacon report message. The LS receives a beacon report message from beacon receiving the vehicle and it discovers the original location of the vehicle and compares that location with the beacon message for detecting attackers.

LITERATURE REVIEW

The work in Xiaodong *et al*. (2007) introduces a secure and privacy defending protocol based on Group Signature and Identity-based Signature (GSIS) technique. GSIS also provides traceability of vehicle's ID. GSIS simplifies the intricacy involved with the public key and the certificate. However, the overhead is high the GSIS and the performance level is average in GSIS. A security system has been proposed in Jinyuan *et al*. (2010) and it utilizes an identity (ID) based cryptographic technique. The security system does not require certificates for the authentication process and is not applicable in the large-scale network as the vehicles have high mobility in VANET.

A novel privacy (mix context) technique in Gerlach (2006) changes the pseudonyms over a particular period to increase anonymity. The mixed content technique prevents the location privacy of the user as the technique achieves higher anonymity. However, the overhead is high in mixed content technique due to inconstant pseudonym generation.

The set of cryptographic mechanism reinforces the users' privacy and it gives a trade-off between the privacy of the user and accountability using pairwise and group communication (Burmester *et al*., 2008). The pseudonyms are varied at only when it requires to reduce the overhead. The work in Kewei *et al*. (2006) proposes an adaptive privacy-preserving authentication mechanism to improve the privacy of the user in VANET. The authentication protocol offers a trade-off between privacy and resource utilization. As, the overhead is high in Kewei *et al*. (2006) due to encryption and decryption using an asymmetric key.

Density-Based Location Privacy (DLP) (Joo-han *et al*., 2009) approach fixes a threshold value to vary the pseudonym. The pseudonym changes take place based on the neighboring vehicle density. The DLP approach curtails the transmission delay as the DLP measures the delay distribution and the expected delay for the particular area. However, DLP determines some location related attacks while it cannot determine all such attacks. In Ying *et al*. (2011), Efficient Privacy Preservation (EPP) protocol provides privacy to the users through a smart card system. The smart card system is used for the authentication process. The EPP utilizes bilinear pairing scheme to provide a key pair. A public key is obtained from the pseudonym ID of the

user and RSU signs the private key of the user without their certificates.

The Random Encryption Periods (REP) scheme in Albert and Xuemin (2010) employs random encryption periods for providing location privacy to the user. REP provides efficient and flexible group communication that consists conditional full stateless property. REP performs the rekeying process as the revoked node density exceeds a certain value. REP cannot determine the compromised nodes internally. In Shokri *et al*. (2014), a MobiCrowd scheme preserves the location of the user from malicious vehicles against Bayesian localization attacks. The MobiCrowd scheme hides the user's query from the server.

An Anonymous Verification and Inference of Positions (A-VIP) (Malandrino *et al*., 2014) is a security and privacy framework and it tracks the vehicles continuously. The A-VIP allows the vehicles to exchange their positions using the anonymous beacon generation technique. Anonymous beacon is generated for every time T seconds. The A-VIP measures the signal quality of the anonymous beacon to detect various types of security attacks. However, the overhead is high in A-VIP due to periodic beacon generation and the attack detection accuracy is low as the signal quality likely to be affected by same frequency vehicles.

A Pseudonym Changing at Social spots (PCS) in Rongxing *et al*. (2012) improves the anonymity level to preserve the real identity of the user from misbehaving vehicles. PCS uses a Key-insulated Pseudonym Self-Delegation (KPSD) scheme to mitigate the risk due to vehicle theft. In Qin *et al*. (2011), Identity-Based Group Signatures (IBGS) scheme divides a large scale vehicular network into small groups. The IBGS employs a set of mechanisms to provide strong privacy and security in VANET. The work in Zhou *et al*. (2011) proposes a lightweight and scalable protocol for detecting a Sybil attack. The Sybil attack detection scheme in Abbas *et al*. (2009) detects a Sybil attack based on signal strength.

PRESERVING LOCATION PRIVACY THROUGH ANONYMOUS BEACONING (PLPAB) SYSTEM

The PLPAB system is considered as a Wireless Access in Vehicular Environment (WAVE) based VANET repressed of vehicles communicating with one another and sporadically with RSUs. The RSUs are placed within a particular distance and any one of the RSU covers the vehicles at all times. Vehicles are equipped with Global Positioning System (GPS) to learn about their positions. Each vehicle can communicate with LS and reports its encrypted location periodically to the LS through RSU. If the RSU does not cover the vehicle, it employs a 3G/LTE cable to communicate with LS. The LS gathers and verifies the location claims which is generated by different vehicles in VANET. PLPAB system prevents the location privacy of the user in VANET using anonymous beacon generation and location verification. If a vehicle is launched from its home network, it accomplishes the registration process with LS. The LS provides a triplet to the vehicle for encrypting the beacon message in a secure manner and it also calculates a mysterious value to the corresponding vehicle using a triplet. Each vehicle in VANET frequently broadcasts an anonymous beacon for a particular period to inform about their location to other vehicles. The beacon receiving vehicles send a beacon report message, including report table and signal strength to the LS over a secure channel. The beacon report message comprises of information such as signal strength of the receiving beacon, beacon generation and receiving time, the speed of the vehicle, the location of the reporter and encrypts the location of the vehicle. The LS decrypts the encrypted beacon message using triplet for determining the location of the corresponding beaconing vehicle. The report information is stored in a report table. To validate the beacon message, the LS divides the road topology into segments for discovering the inference of location of the vehicle. LS considers traffic measurements for avoiding unnecessary beacon generation. The LS compares both the determined location information and report table location information. If the locations are found mismatched, the LS announces the beacon generating vehicle to be malicious. Moreover, the LS determines the attacker and prevents the location privacy of the user. The proposed SARLP system is shown in Fig. 1.

System model: The network is represented as a communication graph G (N, E) and the network size is represented as X*Y. The network G contains the number of vehicles (N_V) and number of RSUs (N_{RSU}) and $N = N_v + N_{RSU}$. The set E contains all directional links between vehicle i and j, where i, j ϵN_v. In VANET, a vehicle $v_i \epsilon N_v$ is equipped with OBU for enabling V2V and V2R communications, where R represents RSU ϵN_{RSU}. The speed of the vehicle v_i is represented as S_i. Consider a vehicle v_i has started from its home network region and accomplishes registration process with LS for getting triplet (K_i, a_i, b_i). K_i is a short term key and a_i and b_i are two integers that are used for counter measurement. The vehicle v_i employs triplet to estimate the time-dependent mysterious value $X^{n,}$ which is shared between the corresponding vehicle and LS and location encrypted message E_i. The E_i encloses the location of the vehicle $L_{i,}$ which is concatenated with a one-bit flag F^{i-1} using the short-term key K_i. A vehicle v_j receives a beacon from vehicle v_i. The beacon receiving vehicle v_j sends a beacon report message to the LS for verifying the credibility of the beacon message. The report message contains the beacon receiving time (t_{ji}), beacon generation time (t_{ij}), speed (S_i) of the vehicle ($v_{i)}$, encrypted beacon message (E_i), location of the beacon receiving vehicle L_j and signal quality of the received

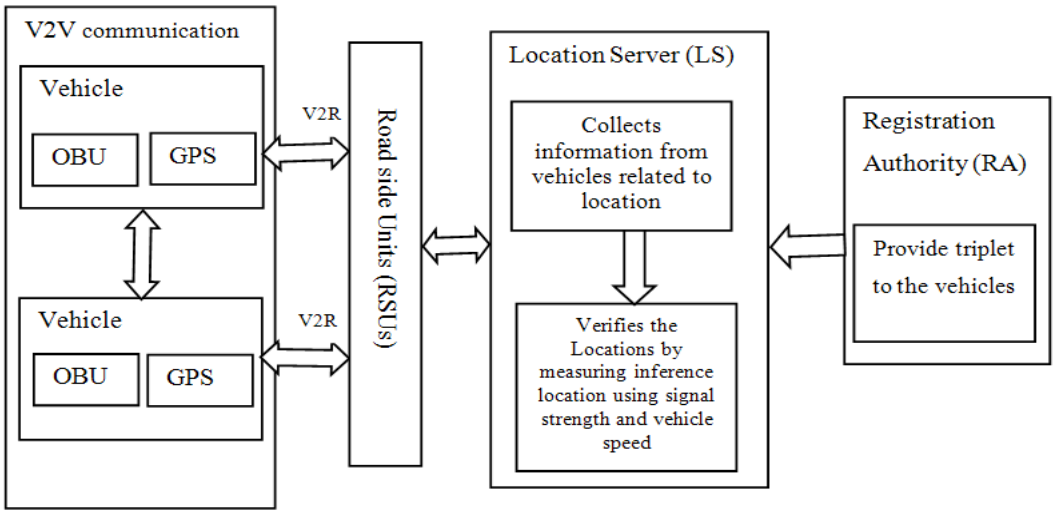

Fig. 1: Block diagram of PLPAB system

beacon (SQ_{ij}). The LS determines the current location (L_i) of the beacon generating vehicle using vehicle speed. The current location information is compared with the precomputed location information in the report table and the PLPAB system efficiently preserves the privacy of the users.

Anonymous beacon generation mechanism: If a vehicle is started, it sends the registration request to the LS at a time (t_i). The LS stores the request receiving time of the vehicle in a table and it provides triplet to the vehicle. The triplet consists of three parts such as a short term key (K_i) and two random integers (a_i, b_i). K_i is a 128-bit asymmetric key. The triplet is valid for a particular period. The LS and Vehicle estimate a mysterious value using a triplet. The LS utilizes the short term secret key to validate the freshness of an anonymous beacon transmission and also find the location of the beacon originator. A counter is initialized to the random integer (a_i) and it is incremented by the random integer (b_i) at the time of beacon request generation. A vehicle generates an anonymous beacon at a particular time interval. The vehicle uses a short term key to encrypt the counter measurement using Advanced Encrypted Standard-Current Transaction Report (AES-CTR). The encrypted value is the time dependent secret $X^n = E_k (a_i + b_i) = Y^n$. The LS requires a higher amount of energy for storing the computed values of all vehicles in its area.

A vehicle disseminates beacon at a particular time interval (t) in its communication area. The beacon transmission takes place in a precise time interval to avoid an unnecessary collision in the network. The anonymous beacons do not have the real identity of the vehicle while it employs a fresh random Medium Access Control (MAC) layer address (Papadimitratos *et al*., 2008). The beacon non-transmitting vehicles overhear the beacon distribution of other vehicles in its area. A vehicle generates a multiple number of beacons in the network. The beacons are assembled using triplet that is obtained from LS at the time of registration. Likewise, the vehicle generates a multiple number of beacons into the network and the vehicle arranges the beacons using a triplet. In PLPAB system, the vehicles that wait in the queue do not generate beacon to reduce the overhead on the network. Conclusively, the n^{th} beacon of the vehicle contains two kinds of information such as current encrypted location and mysterious time dependent value.

Anonymous beacon and report message format: The encrypted message contains the vehicle speed, beacon generation time, the current location of the vehicle and random integers. The encrypted current location of the beacon originator is linked with a one-bit flag value. The encrypted location is XOR'ed with two integers that are in the triplet. The encrypted message is used to find the replay attack in VANET. The anonymous beacon format is depicted as follows:

$$E_{ki} = K_i \{(S_i + t_{ij} + (L_i \| Z^{(i-1)})) \oplus (a_i + b_i)\}$$

The vehicle distributes the beacon message to another beacon requesting vehicle. The beacon receiving vehicle stores the anonymous beacon receiving time in a report table and it estimates the signal strength of the receiving beacon. Signal quality is the ratio of signal power to the noise power:

$$SQ_{ij} = P_r/N_r \quad (1)$$

$$P_r = P_t /D \quad (2)$$

In Eq. (2), P_t is the beacon transmitting power and P_r is the beacon receiving power. D is the distance between beacon transmitting and receiving the vehicle and it is estimated as follows:

$$D = \sqrt{(X_{vi} - X_{vj})^2 + (Y_{vi} - Y_{vj})^2} \quad (3)$$

In Eq. (3), (X_{vi}, Y_{vi}) is the Cartesian coordinates of the sender and (X_{vj}, Y_{vj}) is the Cartesian coordinates of the receiver. The noise power is the impact on signal power reduction due to network interference. Noise power depends on the Temperature (T_0) and Bandwidth (B). It is measured as follows:

$$P_n = KT_0B \quad (4)$$

where, K is the Boltzmann constant with $K = 1.38\times10^{-23}$ Joule/Kelvin. The beacon receiving vehicle sends a beacon report message, including signal strength to the LS for verifying the belief of the anonymous beacon. The beacon report message comprises of the beacon generation time, the beacon receiving time, the speed of the beacon originator, the current location of the reporter vehicle, the signal quality of the receiving beacon and encrypted beacon message. The beacon report message format is as follows:

$$E_{ki} = K_i \{(S_i + t_{ij} + (L_i \| Z^{(i-1)}) + SQ_{ij}) \oplus (a_i + b_i)\}$$

The vehicle transmits the report message to the LS through RSU over a secure channel. In the proposed work, a vehicle can act as a beacon generating and also as receiving vehicle. After receiving the report message, the LS verifies the report message to determine the attackers.

Location verification mechanism: The LS receives the report message from a vehicle and it stores the information in its report table. The LS performs two functions to validate the trustworthiness of the beacon message. The two operations are location determination and attack determination. The LS splits the road topology into segments for discovering the actual location of the beacon generating vehicle. After, the LS compares the determined location with that of the specific location in the report table for identifying the fake vehicles.

Attack detection: The LS compares the current location of the vehicle with that of the location specified in the report message. If the locations are found matched, the LS stores the flag value, location information and signal quality. It discards the report message if it is mismatched, the LS identifies the vehicle v_i to be an attacker. To reinforce the attack detection, the LS additionally calculates the location of the vehicle using vehicle speed. The LS takes the vehicle speed from the previous beacon history and evaluates the actual position of the vehicle.

The LS divides the road topology into multiple segments to determine the location of the corresponding vehicle. The LS and vehicle already have a triplet value for beacon encryption and decryption process. LS decrypts the beacon message and estimates the location of the corresponding vehicle using short term key. For providing strong privacy, the LS starts to calculate the actual position of the vehicle using vehicle speed. Road topology is represented as set A and the set contains multiple road segments such that anyone segment of the set should contain the corresponding vehicle. The PLPAB system assesses the vehicle speed from the previous history. In previous beacon, the location of the vehicle is denoted as X_{iP} and the speed of the vehicle is S_i. The location of a vehicle is predicted as follows:

$$L_C = L_P + (T_C - T_B)*S_i \quad (5)$$

In Eq. (5), T_C and T_B are the current time and a beacon receiving time for the corresponding vehicle. Likewise, the PLPAB system estimates the current location of the vehicle, the vehicle traveled under any one segment of the set. Moreover, the proposed PLPAB system improves the user's privacy accuracy.

Attack against PLPAB system: The PLPAB system determines the various attacks such as Transmit power attack, Wormhole attack, Replay attack, False location attack and Sybil attack.

Transmit power attack: In transmit power attack, an attacker changes the transmit power level to announce the false location to other vehicles. The proposed PLPAB system measures the signal quality of the beacon for determining the transmit power attack in VANET. The signal quality measurement shows that whether the attacker vehicle is nearer or farther from the actual one.

Replay attack: The malicious vehicle overhears the beacons of other nodes and replays it to that node like a genuine vehicle. The PLPAB system determines and verifies the locations of the beaconing vehicle based on signal quality and speed of the vehicle. In addition, the LS compares the flag value and the mysterious value in the beacon with the precomputed flag. The mysterious value in its report table with the LS in the PLPAB determines the replay attack in VANET.

Sybil attack: In Sybil attack, a malicious attacker can pretend as multiple vehicles for injecting false information into the network (Douceur, 2002). It is easy to launch any attack into the network as the occurrence of Sybil attack. The attacker requires multiple identities to perform a Sybil attack. The proposed PLPAB system provides a secret triplet to the vehicle and the vehicle utilizes the triplet for encrypting beacons. Also, the PLPAB system predicts the location using signal quality and speed of the vehicle.

Wormhole attack: In the wormhole attack, an attacker records a packet of other nodes from one location and tunnels the packet into another location (Yih-Chun

et al., 2006). In PLPAB system, the LS precisely verifies the location that is attached in the beacon. The LS verifies the time dependent mysterious value in the beacon. If the same message is received from multiple vehicles, the LS discards both original beacon and duplicate beacon.

False location attack: A malicious attacker distributes false location as it pretends different location from the actual vehicle and also it agitates the beacon-reporting operation. In PLPAB system, the LS and vehicle maintain a mysterious time dependent value. The LS determines the false location attack through the verification process.

Performance evaluation:

System setup: The efficacy of the proposed PLPAB system is substantiated through Network Simulator. The simulations are performed on a random topology of 100 vehicles and 25 RSUs. The vehicles are distributed randomly on the road in the area of 3×3 km^2. The communication range of a vehicle and RSU is 250 m and 300 m, respectively. The nodes employ Ad hoc On-demand Distance Vector (AODV) routing protocol as the overhead is low in AODV. Constant Bit Rate (CBR) in the application layer and User Datagram Protocol (UDP) in the transport layer is implemented with a packet size of 512 bytes in the interval of 2 ms the link bandwidth is 2 Mbps. The average high speed of the vehicle is 50 km/hr. The simulation runs for 500 s. The simulation concentrates on metrics such as Location Prediction Accuracy (LPA), overhead, energy level and Maximum Verification Time. The proposed PLPAB system is compared with existing A-VIP scheme (Malandrino *et al*., 2014) for analyzing the performance.

Simulation results:

Communication overhead: Communication overhead is the number of beacons generated in PLPAB for preserving the privacy of the user. Figure 2 shows the relationship between vehicle density and communication overhead. In PLPAB system, the vehicles do not generate beacons when traffic occurs in the network. The vehicle and LS set the period as constant for low traffic, while the period is variable in high traffic. It is used to maintain the time dependent mysterious value between the LA and vehicle effectively. Thus, reduces the network overhead considerably. In Fig. 2, the PLPAB system and A-VIP scheme attains 1.45 and 1.54 overhead for 300 vehicles.

Energy level: Each node in VANET has an amount of energy to perform network functions. Figure 3 depicts the relation between the number of attackers and energy level of vehicles. The number of attackers is the ratio of a number of attacker vehicles to the total number of vehicles. For improving detection accuracy, the PLPAB

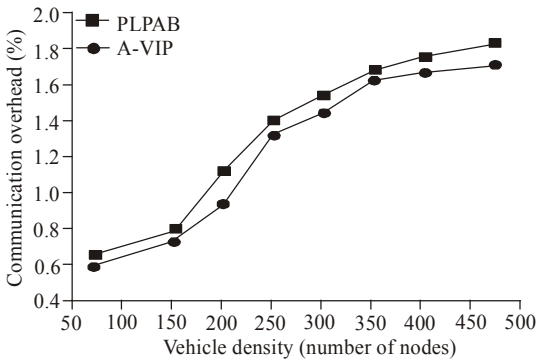

Fig. 2: Vehicle density vs communication overhead

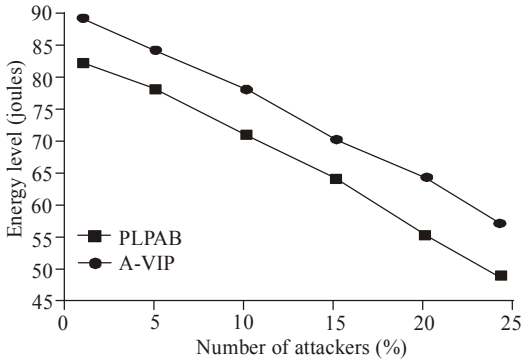

Fig. 3: Number of attackers vs. energy level

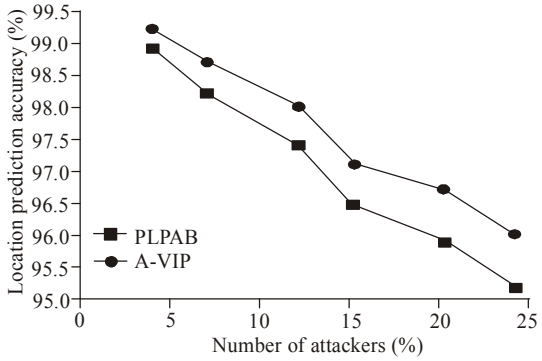

Fig. 4: Number of attackers vs. location prediction accuracy

system verifies the beacon using the signal strength and the vehicle's speed while the A-VIP scheme verifies the beacons using signal strength only. The PLPAB requires high energy for verification when compared to A-VIP. In Fig. 3, the PLPAB and A-VIP require 71 and 78 joules for detecting 15 attackers.

Location prediction accuracy: Location prediction accuracy is the number of vehicle's location to be preserved from the total number of vehicles. Figure 4 demonstrates the relationship between the number of attackers and location prediction accuracy. The PLPAB system predicts the location of each vehicle in two stages such as signal strength based prediction and

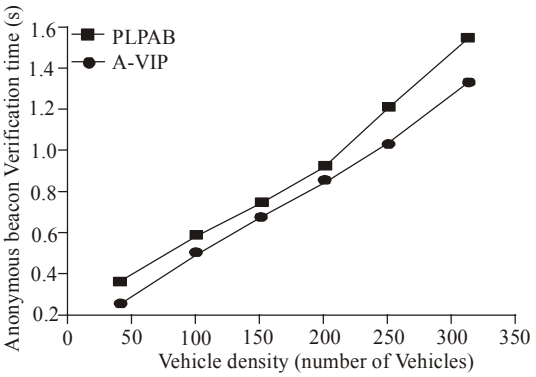

Fig. 5: Vehicle density vs. anonymous beacon verification time

vehicle speed based prediction. In Fig. 4, the PLPAB and A-VIP scheme achieves 97.1 and 96.1% location prediction accuracy.

Maximum verification time: The anonymous beacon verification time is the time taken by the LS to verify the anonymous beacons. Figure 5 illustrates the relationship between vehicle density and anonymous beacon verification time. In an urban area, the vehicle density is high and huge beacons of the vehicle are waiting in the queue for LS verification. Thus, increases the beacon verification time. In Fig. 5, the PLPAB and A-VIP achieve 0.25s and 0.6s for 100 vehicles.

CONCLUSION

This study concentrates on the privacy of the users and it proposes a PLPAB system, including anonymous beacon generation mechanism and location verification mechanism. In PLPAB system, a vehicle distributes anonymous beacon in a particular time interval while the beacons are not distributed at high traffic. Thus, reduces the communication overhead. The vehicles employ triplet for beacon encryption and decryption. In location verification mechanism, the LS verify the location that is in report message to validate the trustworthiness of the beacon. The LS uses the signal quality level and vehicle's speed for predicting the accurate location of the beacon originator. Consequently, the PLPAB system significantly improves the privacy standards of the users. The PLPAB system is compared with conventional A-VIP scheme and the simulation results demonstrate the efficacy of the PLPAB system.

REFERENCES

Abbas, S., M. Madjid and D. Llewellyn-Jones, 2009. Signal strength based Sybil attack detection in wireless ad hoc networks. Proceeding of the 2nd IEEE International Conference on Developments in eSystems Engineering (DESE, 2009), pp: 190-195.

Albert, W. and S. Xuemin (Sherman), 2010. REP: Location privacy for VANETs using random encryption periods. Mobile Netw. Appl., 15(1): 172-185.

Burmester, M., E. Magkos and V. Chrissikopoulos, 2008. Strengthening privacy protection in VANETs. Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp: 508-513.

Douceur, J.R., 2002. The sybil attack. Proceeding of the 1st International Workshop on Peer-to-Peer Systems. Springer Berlin, pp: 251-260.

Fussler, H., S. Schnaufer, M. Transier and W. Effelsberg, 2007. Vehicular ad-hoc networks: From vision to reality and back. Proceding of the 4th Annual IEEE/IFIP Conference on Wireless on Demand Network Systems and Services (WONS, 2007), pp: 80-83.

Gerlach, M., 2006. Full Paper: Assessing and Improving Privacy in VANETs. Retrieved from: www.network-on-wheels.de/downloads/escar2006gerlach.pdf. (Accessed on: May, 2010)

Jinyuan, S., Z. Chi, Z. Yanchao and F. Yuguang, 2010. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE T. Parall. Distr., 21(9): 1227-1239.

Joo-Han, S., V.W.S. Wong and V.C.M. Leung, 2009. Wireless location privacy protection in vehicular ad-hoc networks. Proceedings of the IEEE International Conference on Communications. Dresden, pp: 1-6.

Kewei, S., X. Yong, S. Weisong, L. Schwiebert and Z. Tao, 2006. Adaptive privacy-preserving authentication in vehicular networks. Proceeding of the 1st International Conference on Communications and Networking in China, pp: 1-8.

Lin, X., R. Lu, C. Zhang, H. Zhu, P.H. Ho and X. Shen, 2008. Security in vehicular ad hoc networks. IEEE Commun. Mag., 46(4): 88-95.

Malandrino, F., C. Borgiattino, C. Casetti, C.F. Chiasserini, M. Fiore and R. Sadao, 2014. Verification and inference of positions in vehicular networks through anonymous beaconing. IEEE T. Mobile Comput., 13(10): 2415-2428.

Nathan, B., 2006. Introduction to Vehicular Ad Hoc Networks and the Broadcast Storm Problem. Retrieved from: https://www.google.com.pk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAAahUKEwjxlcvcp73HAhVG2hoKHZy8B3E&url=http%3A%2F%2Fnathanbalon.com%2Fprojects%2Fcis695%2Fintro_to_vanet.pdf&ei=KL7YVfHhE8a0a5z5nogH&usg=AFQjCNHYmzuhfJ7A6jXRUSmSrA.

Papadimitratos, P., L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung and J.P. Hubaux, 2008. Secure vehicular communication systems: Design and architecture. IEEE Commun. Mag., 46(11): 100-109.

Qin, B., Q. Wu, J. Domingo-Ferrer and L. Zhang, 2011. Preserving security and privacy in large-scale VANETs. In: Qing, S. *et al*. (Eds.), ICICS, 2011. LNCS 7043, Springer-Verlag, Berlin, Heidelberg, pp: 121-135.

Rongxing, L., L. Xiaodong, T.H. Luan, L. Xiaohui and S. Xuemin (Sherman), 2012. Pseudonym changing at social spots: An effective strategy for location privacy in VANETs. IEEE T. Veh. Technol., 61(1): 86-96.

Sherali, Z., H. Ray, C. Yuh-Shyan, I. Angela and H. Aamir, 2012. Vehicular ad hoc networks (VANETS): Status, results and challenges. Telecommun. Syst., 50(4): 217-241.

Shokri, R., G. Theodorakopoulos, P. Papadimitratos, E. Kazemi and J.P. Hubaux, 2014. Hiding in the mobile crowd: LocationPrivacy through collaboration. IEEE T. Depend. Secure, 11(3): 266-279.

Xiaodong, L., S. Xiaoting, H. Pin-Han and S. Xuemin, 2007. GSIS: A secure and privacy-preserving protocol for vehicular communications. IEEE T. Veh. Technol., 56(6): 3442-3456.

Yih-Chun, H., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Sel. Area. Comm., 24(2): 370-380.

Ying, B., D. Makrakis and H.T. Mouftah, 2011. Efficient privacy preservation protocol using self-certified signature for VANETS. Proceeding of the 7th International Conference on Wireless and Mobile Communications, Tech-Republic, pp: 301-306.

Zhou, T., R.R. Choudhury, P. Ning and K. Chakrabarty, 2011. P2DAP-Sybil attacks detection in vehicular ad hoc networks. IEEE J. Sel. Area. Comm., 29(3): 582-594.