International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Privacy and Security on Context Aware using P-Gene Based on Pseudonym in Vanets

P. Santhosh Kumar, S Parthiban, V. Jegatheeswari

Abstract: ***In recent times, Vehicular Ad hoc Networks (VANETs) have fascinated extensive considerations as the encouraging methodology to enhance the road safety, as well as refining driving experience. The main aspect in Vehicular Ad hoc network is privacy in safety-related application. The main confront in VANET is identification of user, site and data privacy. This is because of network and nature of transmission in the communication media. In order to overcome this problem we propose a new methodology called Privacy Preserving Communication System (PPCS). Privacy Preserving Communication System (PPCS) offers a complete output to unspecified communication endpoints, carry on the spot and identifier of a nod unlinkable, and pretense the survival of communication flows. To present a qualitative debate on strength against outside attackers and describe its performance trade-offs, the security issues on PPCS have been analyzed clearly. The mock-up outcome make obvious that PPCS has only 3% lower packet delivery ratio than existing multi-path routing protocols, while efficiently providing privacy service in VANETs. Many privacy patterns concern shifting pseudonyms occasionally to dodge connecting messages. In this project, we proposed a context privacy using P-Gene based pseudonym for VANETs. The P-Gene is constructed using the designed data hiding technique. Simulation based extensive analyses and demonstrating this scheme efficiently preserving the context privacy.***

Index Terms: ***VANET, Security, Context Privacy, P-Gene, Pseudonym, Trusted Third Party, Auditing***

I. INTRODUCTION

VANET are self-organized networks which can be molded by connecting the vehicles and Road Side Unit (RSU). The RSU are connected by high speed networks. Two communications in **VANETs** are Vehicles to Vehicles (V2V) and Vehicles to Infrastructure (V2I). It aims to increase safe driving and managing the traffic, driver and passenger use the internet access. The V2I communication is very much useful for the vehicles to communicate with a traffic light. In Contrast, the drivers can acquire an enhanced idea of what's going on in their driving environment and yield initial movements to respond to an abnormal situation by means of V2V communications. On-Board Unit (OBU) broadcasts traffic-related messages with the statistics of current time, location of vehicles, direction and speediness of the vehicles, status of the brake, steering angle, acceleration/deceleration, traffic settings and traffic events.

Moreover, emergency communications can be created and sent by OBUs in case of emergent braking, traffic jam, or other accidents. The Characteristics of VANETs are

i. Rapid changes in topology
ii. Variable network density
iii. High predictable mobility
iv. No power Constraints

II. LITERATURE REVIEW

Privacy in VANETs by using changing pseudonym at proper location (PCP) is proposed in [3] to achieve the location privacy. If the vehicles are gather in a temporary location, it is considered as the social spot. Many special features are proposed in PCP. First, vehicles temporarily stops at the particular location called social spot. Second, Key insulated Pseudonym Self-Delegation (KPSD) model, it breeds numerous short keys and it alleviate the vehicles theft. If the vehicle is not in the spot, automatically it broadcasts the safety message first which comprises of location, activities, velocity and time. The social spot is selected as small spot and large spot. If the vehicles stop at a road juncture is considered as a minor spot and the pseudonym change is performed when the traffic light goes to green.

Privacy in VANETs by using changing pseudonym based on security protocol is proposed in [4].The key note of this paper is to avoid the illegitimate traceability of vehicles during the communication. In general two approaches are proposed. First approach asks the central authority a new pseudonym after a particular time t for each vehicle. In second approach, after a particular time t each vehicle generates a new pseudonym. The main objective of this method is to change the pseudonym at a same interval time. In first approach, RSU broadcast its public key occasionally and vehicles send to CA. Central authority send to applicant vehicles. The vehicles always communicate with central authority to obtain the private communication. Second approach has a private and public key of all the vehicles. If the certificate is expired, a new private pseudonym is created.

Privacy in VANETs by using changing pseudonym based on the traffic is proposed in [5].This method is used achieve the high level location privacy and also it uses the radio silence technique. In TAPCS, vehicles continuously monitoring traffic related information according to that pseudonym change are performed. The proposed method consists of five phases.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
P. Santhosh Kumar*, Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India.
S. Parthiban, Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India.
V. Jegatheeswari, Department of Computer Science and Engineering, Tata Consultancy Services, Chennai, India.

- ✓ Congestion Detection Phase
- ✓ TAPC strategy's Initiator Election Phase,
- ✓ Silent Mix Zone Creation Phase,
- ✓ Silent Mix Zone Extension Phase,
- ✓ End of Traffic Congestion Detection Phase.

These phases are used to maximize the location privacy protection level beside a solid challenger model.

Pseudonym is one of the solutions for the privacy issue in VANETs.

Pseudonymity terminology is first proposed in [1] if the attacker falsifying the communication between sender and receiver, and monitoring whether the communication is occurring between sender and receiver. Pseudonym comes from Greek "Pseudonymn" meaning "false named" (pseudo: false; onuma: name). The pseudonym is the unique id and which is used to authenticate the sender messages. It is the identifiers of subject instead of real name between sender and receiver. The properties of pseudonym are restriction to a motionless amount of pseudonyms per issue, uniqueness, transferability to other subjects, opportunity and frequency of pseudonym swop, participation of users in forming the pseudonym.

III. CONFIDENTIALITY AND PROTECTION IN VANETS

The wireless vehicular communications and periodic broadcasting beacons messages impose severe privacy issues. By overhearing VANET communications, adversary may discover the physical characters of its interested nodes in network and profile them in terms of application accessing and personal information. Thus, several schemes have been proposed to enable privacy-preserving node in VANETs. Still, by overhearing the periodic beacons message, adversary may collect the location history of any node. They are various mechanisms to solve location privacy issue in VANETs they are

1. Anonymous certificate
2. Pseudonyms
3. Group signature
4. K-anonymity

Thus, to protect the identity privacy of each node, each node may use pseudonyms instead of its real identity in VANET communications.

A. Bogus Information Attack

The challenger may throw bogus messages to meet up a precise idea. For example, one may send a fake forthcoming disaster vehicle warning in order to push over the others such that it can influence to get a improved traffic condition.

B. Unauthorized Preemption Attack

An RSU could be worn to manage a traffic light when any evolving circumstance occurs. Parallel to the bogus information attack, the opponent may illegally disrupt a traffic light through the RSU in order to meet some definite reason.

C. Message Replay Attack

The adversary replays the valid messages previously sent by a legitimate source in order to disturb the traffic.

D. Message Modification Attack

A message is altered during or after transmission. The adversary may wish to change the source or content of the message in terms of the position and/or time information that had been sent and saved in its device to escape from the consequence of a criminal or traffic accident event.

E. Impersonation Attack

The adversary may pretend to be another vehicle or even an RSU to fool the others.

F. RSU Replication Attack

An RSU may be compromised such that the opponent can relocate RSU to commence any malicious attack, such as spreading false traffic information.

G. Denial-of-Service (DOS) Attack

The opponent sends immaterial mass messages to take up the channels and consume the computational resources of the other nodes, such as RF interference, overcrowding, and layer to packet flooding.

Since VANETs is on an open collective standard, this smooths the progress of the illegal collection and processing of information. After the adversary intercepts a significant number of messages in a certain region, the opponent may outline a vehicle in terms of its physical position and moving patterns simply through information analysis. Since drivers are concerned about leakage of the aforementioned sensitive information to the public, resolving such concerns becomes one of the major issues in the design of modern VANETs.

H. Personal Information Leakage

If information transmitted over a VANET is not protected, an adversary can easily collect the information by sniffing the network and discover some user-related sensitive information, such as a driver's name, address, and license. The personal information leakage could result in identity theft, which could disrupt the victim's personal life.

I. Site Privacy

After opponents seize a momentous quantity of messages in a definite region, the adversary may be able to outline a vehicle in terms of its physical position and moving patterns simply through information analysis.

A pseudonym of one node is a transitory identifier without any apparent connection to its real identity. However, by collecting personal information and movement trajectory related to one pseudonym, an adversary may still derive the real identity of one node. Thus, frequent pseudonym change has been adopted in many schemes to protect the location privacy of vehicular nodes and reduce the personal information revealed by any pseudonym. Pseudonym can be generated by vehicle itself and send to certificate authority for sign and send to certificate authority. In second method, vehicle sends the message to the RSU, and then RSU generate the pseudonym and send to certificate authority. In third method, pseudonym can be generated by the manufacturer company. In fourth method pseudonym can be generated by certificate authority.

IV. CORRELATED MECHANISM

Figure 4.1describes the elementary knowledge of the Context-Aware Privacy Scheme which is to govern the accurate context in which a vehicle should modify its pseudonym. It wishes to raise the effectiveness of such modification besides tracking and avoid deteriorating pseudonyms in simply observable circumstances.

A vehicle observes repeatedly other vehicles found surrounded by its communication range and tracks their activities using Kalman filter. A vehicle monitors the surrounding vehicles and goes into silence when it discovers one or more neighbors silent. It continues beaconing with fresh pseudonym when its real state is to be mixed with the state of a silent neighbor.

A. Trusted Third Party

A trusted third party (TTP), which refers to a trusted organization with adequate computational and cargo space resources where all vehicles index and find their certificates for VANET usage, is accountable to hold the credentials and the identities of vehicles and to reveal the genuine identities of nodes whose certifications have been revoked. In addition, they are also in charge of RSUs. TTPs are fully trusted by all entities. In reality, a huge number of TTPs stay alive and each one of them is in charge for a specific geological area. Each vehicle and RSU should be registered with exactly one TTP.

B. Roadside Units

RSUs are infrastructures predetermined on the roadside, which are fully restricted by TTPs. RSUs, are quite susceptible because they are simply open to the attackers, so we must plant minimal trust in RSUs. For enhanced security, RSUs could directly communicate with TTP and if TTP considers that a detailed RSU has been compromised, it could repeal the RSU's admittance. The format of messages delivered in V2V scenario.

C. Vehicles

Vehicles are the moving nodes in the network, which are loaded with an OBU and a tamper-proof device. The OBU is used to enable vehicles to wirelessly communicate with each other and RSUs, and the TPD is used to store cryptographic materials, such as an Electronic License Plate (ELP) that is installed on every new vehicle and provides a unique ID number, and process cryptographic operations. TPD is a good second defense layer

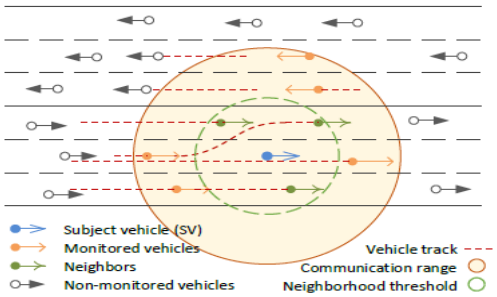

Figure: 4.1 Illustrations of CAPS

The CAPS works as follows,

i. Input tracks maintained for other vehicles, a road for the SV itself, ideals acknowledged by the SV at the prior time step (scan),the present SV state achieved from its sensors (actual state) and its recent status whether active or silent.
ii. The scrutinized vehicles are restructured by the conventional beacons using Kalman predict function.
iii. The candidates of silent neighbor are identified by means of get silent function. This function is used to find the neighbor footpaths which are not updated by a beacon for past failure beacon threshold time steps
iv. The pseudonym time exceeds the minimum pseudonym time (pseudonym min), the vehicle goes to muteness when there is a candidate or additional silent neighbors. We added randomization to the switching condition to prevent the adversary from guessing the exact time of turning to silence.
v. SV does not turn to silence; it continues to sends a beacon and updates its own track.
vi. Assume that SV is in silent mode, and then SV computes the type of the residual vector from its authentic state and using the function calc dist.
vii. The minimum norm of residual vectors is also calculated between its actual state and its silent neighbor tracks (min neigh dist) by calling the function calc min dist.
viii. If (min neigh dist) < (myself dist), then the actual state of the SV is probably combined with a track of those silent neighbors.
ix. It clearly states that, the opponent would obscure as well if this silent neighbor did not recommence its beaconing in the same time step.
x. A new pseudonym has been received from its preloaded loch and continues sending beacons to next time step, when SV exits its silent state.

D. By shifting the pseudonym with Mix Zone:

As altering pseudonyms addresses many of the privacy problems, one of the behaviors to guard vehicles' location privacy is to have them modify their pseudonyms in encoded regions known as mix zones. Each vehicle can establish its mix zone dynamically when its pseudonym is close to termination by transfer a request to a third trusted unit for launching its mix zone. Then, each vehicle in the mix zone fix on if it will be cooperating by taking into consideration its current reputation and location privacy. In this approach a special location called MIX ZONE as shown in figure 4.2, with high density of traffic is chosen. In this mix zone vehicle retain radio signal silence and change their pseudonym simultaneously. Because of this special gap between last message sent by the old pseudonym and first message sent by new pseudonym after mix zone, can't be linked.

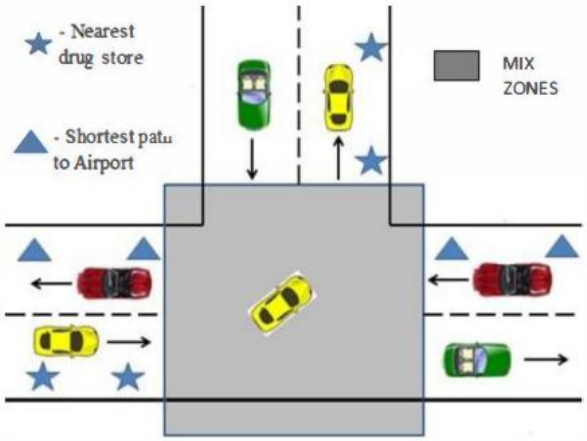

Figure 4.2: Mix Zone

V. PROPOSED SYSTEM

The main objective of the paper is proposing an context privacy using P-Gene based Pseudonym (CPUP) which enhances the context privacy by using P-Gene techniques in VANETs. Each node in VANETs constructs the P-Gene using simple mathematical calculation operation, which is used to hide the data and effectively reporting the data to the RSU to increase the efficiency of context privacy.

A method for P-Gene generation is independent of cryptographic algorithms.

The distributive scheme that ensures context privacy, this process built on the data hiding technique. Figure 5.1describes the process of P-Gene and data reporting process. Individual node perturbs its private data in this scheme through its P-Gene without additional data exchange, and the aggregate outcome can be improved from the hidden data in the RSU. In data hiding technique, each node hides its private data using fabricated P-Gene, and then sends the concealed data to its RSU. After receiving the recording data of its cluster participants without obtaining P-Gene, RSU can get all the P-Genes from the hidden data and obtain the aggregation outcome.

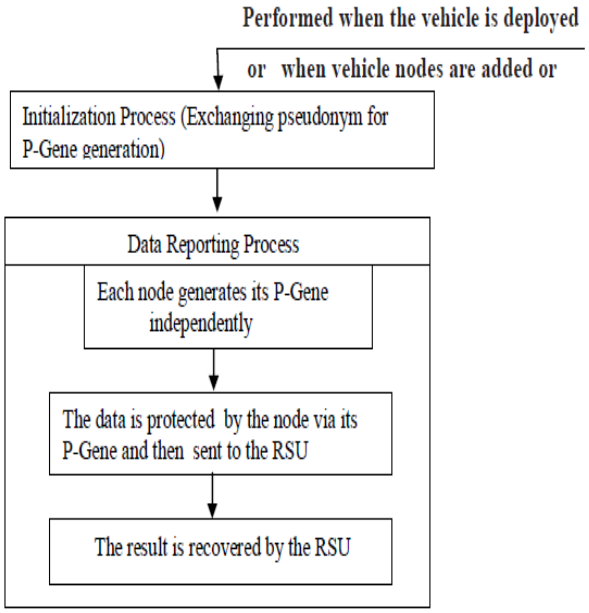

Figure 5.1 P-Gene based Pseudonym

We proposed a new routing protocol in collaboration with genetic algorithm which guarantees the Quality of Service (QoS). The QoS is used to prejudice by cracked links stuck between vehicles and the transmission of failure packets in a Vehicular Adhoc NETwork (VANET). Furthermore, through the mathematical results, it is revealed that the projected system is extensively superior when associated with protocols of the Intersection Based Routing (IBR) and Connectivity Aware Routing (CAR) in terms of broadcast interruption and packet loss rate. The genetic algorithm GA is exploited to enhance the universal existing path which fulfills the QoS requirements.

Proposed Modules

A. Initialization Process For Pseudonymn Generation And Maintainace

The process of pseudonym generation and maintenance is analyzed through three cases

Case 1: Number of vehicles nodes are communicating in cluster

Step 1:

Initially for each node 'y' arbitrarily produces (n-1) data as pseudonym based on P_{zy}. Now each encrypted P_{zy} is directed to the equivalent neighboring node 'z' through the use of shared pair wise key $S_{k(y,z)}$:{ P_{zy}}$S_{k(y,z)}$. Likewise, the neighboring node 'y' receives pseudonym P_{zy} from node 'z'.

Step 2:

Once the pseudonym exchanged, node b set the pseudonym table that contains all of its generated pseudonym Pcband those that are received from the other cluster members.

Pseudonym Table for node y:T_y

C	1	2	....	n-1	N
P_z^y	P_1^y	P_2^y	.....	P_{n-1}^y	P_n^y
P_y^z	P_y^1	P_y^2	.....	P_y^{n-1}	P_y^n

Table 5.1: Pseudonym Table T_y of Node y

Case 2: A Vehicle node fails

When node 'y' is reported that cluster member 'z' fails, node y deletes Pzy and Pyz from table Tb.

Case 3: New vehicle nodes are added:

When node 'y' is reported that new cluster members have been included *d*, node *y* generates pseudonym Pdy, which is then added to table Ty and sent to *d*: { Pdy }Sk(y,z).. Similar to Case 1, individually inserted cluster member produces pseudonym for all other cluster members and then leads these pseudonym to the parallel cluster members. Respectively included cluster member *d* also preserves its pseudonym table for P-Gene generation. After this practice, each pair of valid cluster members (*y*, *z*) only shares the two secret pseudonym, namely, {Pzy, Pyz }.

B. Data Reporting Process

The vehicle node gathers data and hides its data through its P-Gene, and drives the hidden data to its RSU. RSU recovers the aggregation outcome after receiving all data from each node. A random node '*y'* customs their secret from P-Gene to safeguard its private data. The data that node *y* directed to its RSU has the hidden data Dy= (dy+Py) mod U (8).

Step 1: According to pseudonym {Pzy}, a random node *y*achieves all the P-pseudonym(P-Pzy), where each is the lowest *l* bits of T(Pzy). Afterward, node *y*calculates the P-Pseudonym as follows:

$$P\text{-}Pyy = U - (\Sigma\ Pzy) \bmod U \quad \ldots\ldots \quad (5.1.1)$$

According to the corresponding pseudonym {Pzy}, node *y* finds all the P-pseudonym, {Pyz} which have the bottom most *l* bits of T (Pyz). Thereafter, node *y* determines its P-Gene Py according to{Pyz} as follows:

$$P\text{-}Py = (\Sigma Pyz) \bmod U \quad \ldots\ldots \quad (5.1.2)$$

Node *y*hides its sensory data with as dywith Py as Dy= (dy+Py) mod U (8), and then sends {Dy, y} to its RSU.

Step 2: RSU checks the individual clusters whether all the nodes have sent their data.

i. If so, RSU computes*D*= (ΣDy) mod *U* (9), which is equivalent to Σdy. RSU then guides {D,m}to the next hop node.

ii. Or else, by arrogant that node *c* does not responding, RSU asks *c* to report. If node *c* responds, RSU continues testing and computing as (i).

VI. SIMULATION OUTCOME

In this section, we identify following specific metrics to study the performance of proposed system. The evaluation metrics are Success ratio, Entropy and anonymity.

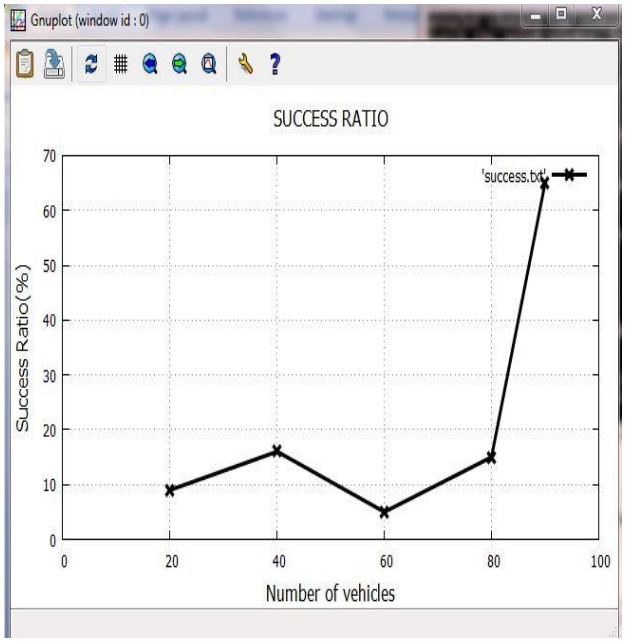

Figure: 6.1 Success Ratio

Figure 6.1 represents the success ratio of CPUP fewer than 70%. .The result shows that the number of vehicles increasing in the range 20.The success ratio of delivery packets is increasing gradually. When the number of vehicles is 90, the success ratio is 65%.The effectiveness of CPUP in terms of success ratio is mainly due to the improved version of data hiding technique using pseudonym.

Figure 6.2 presents the Entropy of CPUP increases when compared to TAPCS.TAPCS proposed in [7].

$$\mathbf{H(x)= -\sum_{i=1}^{n} P_i \log_2 P_i}$$

igure 6.3 explains when the number of the user increases the privacy is decreases. The privacy is depending upon the information is shared between the user. When the privacy is high, there is less number of users.

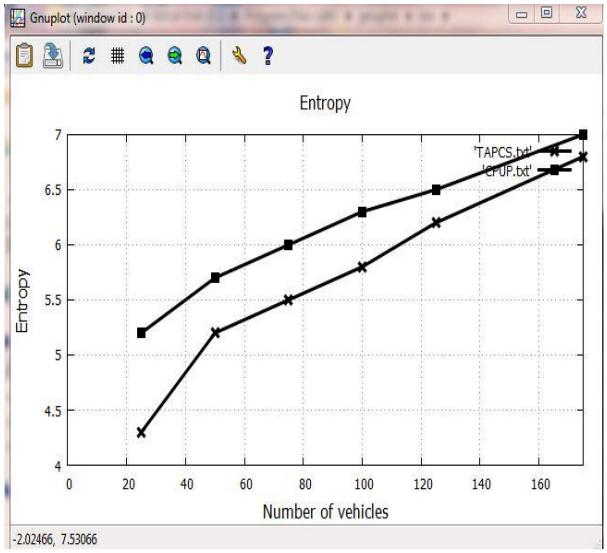

Figure 6.2: Entropy

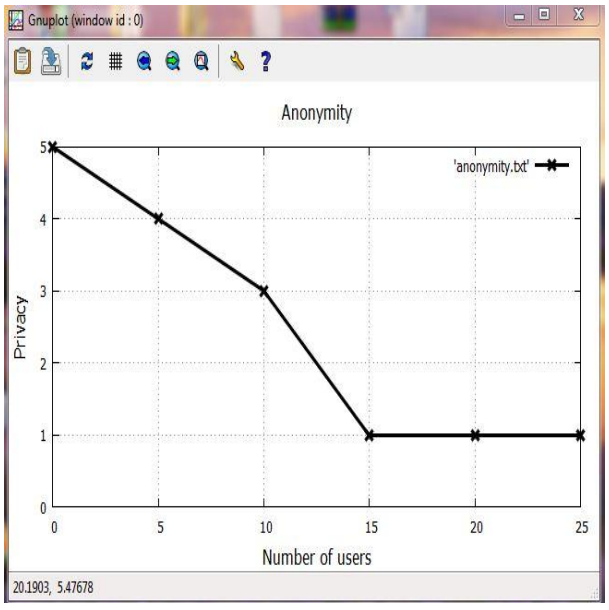

Figure 6.3: Anonymity

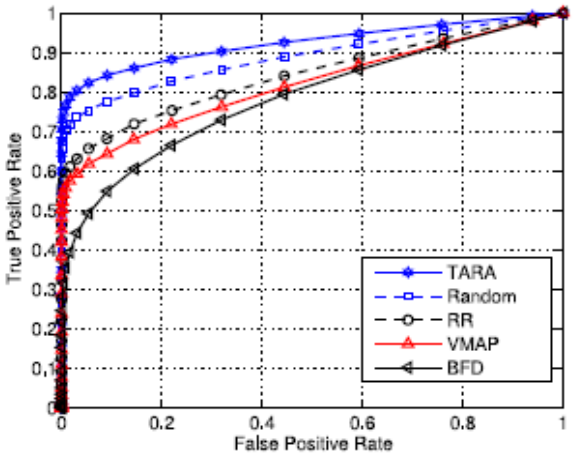

Figure 6.4: Receiver Operation Characteristics

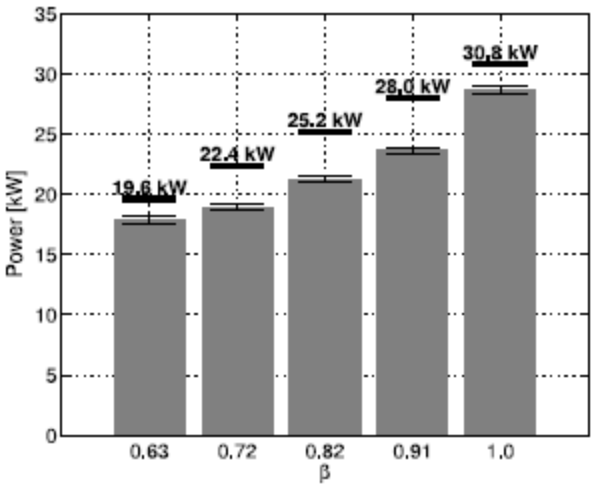

Figure 6.5: Power Consumption by VANET

Figure 6.4 shows the ROC of VANET and of its challenging algorithms. When the resource is enough to control all the VM requests, VANET outperforms the other algorithms. We also scrutinize that VANET constantly outperforms the other algorithms for different power budgets. Haphazard placement and RR prove superior detection rate than VMAP and BFD because they naturally stretch the VMs similarly as TARA does, ensuing in a great number of lightly-loaded servers in which unexpected hotspots can easily be identified. In fact, while VMAP and BFD are very energy efficient as both of them consolidate VMs, they make the temperature map change due to irregular events insignificant, resulting in low detection rate.

Figure 6.5 illustrates the normal power consumption gives a power financial plan (here b0 ¼ 0:55). We can conclude that, as a replacement for utilizing the hole power budget, TARA investigate the result space to find the most power-efficient design that can offer the highest achievable detection accuracy for a given power budget.

VII. CONCLUSION AND FUTURE ENHANCEMENT

Our paper addressed the problem of privacy issues in VANET environments. There are various techniques to solve the privacy issues, we proposed a context privacy scheme P-Gene based Pseudonym that adapts to dynamically changing reporting nodes. Simulation based extensive analyses and demonstrating this scheme efficiently preserving the context privacy.

Below is the list of major contributions:

- ✓ Presented survey of various location and context privacy issues and techniques to solve the issues.
- ✓ Proposed P-Gene based Pseudonym that significantly reduces communication and computational overhead.

REFERENCES

1. LeventeButtyan, Tamas Holster, Andre Weimerskirch, William Whyte, "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs" in Proc. IEEEVehicular Networking Conference (VNC),pp.1-8, October 2009.
2. AbdelwahabBoualouacheand Samira Moussaoui,"S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs", in Proc. International Conference on Advanced Networking Distributed Systems and Applications, June 2014.
3. Chang An, Celimugr Wu, Tsutomu Yoshinaga, Xianfu Chen, Yusheng Ji, "A Context-Aware Edge-Based VANET Communication Scheme for ITS" in sensors, Jun 24, 2018 doi: 10.3390/s18072022
4. Emara, Karim, Wolfgang Woerndl, and Johann Schlichter," CAPS: context-aware privacy scheme for vanet safety applications", in Proc. ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp.21, June 2015.
5. Emara, Karim, Wolfgang Woerndl, and Johann Schlichter, "POSTER: Context-adaptive user-centric privacy scheme for VANET", in Proc. International Conference on Security and Privacy in Communication Systems, vol 164, pp 590-593, 2015.
6. Mathews, S. Jinila," An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet", in Proc.IEEE International Conference on Electronics and Communication Systems (ICECS), pp. 1-6, 2014.
7. Qu, Fengzhong, "A security and privacy review of VANETs." IEEE Transactions on Intelligent Transportation Systems, pp.2985-2996, 2015.
8. AbdelwahabBoualouache, Samira moussaoui,"TAPCS: Traffic-aware pseudonym changing strategy for VANETs ", Peer-to-Peer networking and Applications, pp.1-13, 2016.
9. Ram Shringar Raw, Manish Kumar, Nanhay Singh, "Review on privacy preservation methods in vehicular adhoc networks" in Proc. IJCAT - International Journal of Computing and Technology, Volume 2, Issue 3, March 2015.
10. Huang, Dijiang, SatyajayantMisra, MayankVerma, and GuoliangXue, "PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs" IEEE Transactions on Intelligent Transportation Systems, pp 736-746, september 2011.
11. AbdelwahabBoualouachea, Sidi-Mohammed Senoucib, Samira Moussaouia,"HPDM: A Hybrid Pseudonym Distribution Method for Vehicular Ad-hoc Networks" in proc. The 7th International Conference on Ambient Systems, Networks and Technologies, 2016

AUTHORS PROFILE

P. Santhosh Kumar, pursuing his Research work under the domain Cloud computing in Sathyabama University, Chennai. He is working has an Assistant Professor in CSE at Veltech University. He completed his M.E (CSE) in Anna University. He has 9 years of teaching experience in the department of CSE. He is very much expertise in the field of Cloud Computing, Internet of Things, Data Ming, Software Engineering. He has published around 10 papers in various reputed Journals.

S. Parthiban Research scholar and working as Assistant Professor in Veltech Uiversity. He had completed M.Tech(IT) in sathyabama University. He has 11 years of teaching Experience in CSE and he is expertise in various areas such as Cloud computing, Image processing, Data Mining and data structures and algorithms. He has published 7 papers in various reputed journals.

V.Jegatheeswari, currently working has IT analysts in Tata Consultancy Services, Chennai. She completed her M.Tech (IS) in Pondicherry University. She has 5 years of experience in software has a developer. She published 4 papers in various reputed journals. She is expertise in Java, Data Mining, Software Engineering and Cloud Computing.