IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-10 E-ISSN: 2347-2693

Green Computing Approaches on Vanet Using ACPN Method

S.Suganya[1*], N. Vasunthira Devi[2]

[1*]M.Phil Research Scholar, Dept. of CS, AVC College (Autonomous), Mannampandal, Mayiladuthurai
[2]Asst. prof of CS, AVC College (Autonomous), Mannampandal, Mayiladuthurai

Available online at: www.ijcseonline.org

Received: 20/Sep/2016 Revised: 29/Sep/2016 Accepted: :22/Oct/2016 Published: 31/Oct/2016

***Abstract*— VANET's are a confident instruments to permit correspondence between methods for transportation on streets. VANET deals with the consistent premise of ongoing framework where the automobile s more as hubs and go with rapid on streets. There are numerous security issues like verification, passage assaults, insightful framework approach, impact identification, clog shirking and so on.,. Various techniques have been offered to manage different issues in VANET. In this manuscript, we demonstrate a model of Authentication Structure with Restricted Privacy-Preservation and Non-Repudiation automobile way to deal with bolster green automobile correspondence for urban operation safeguard. Utilizing vehicular innovation could benefit operation protect automobile s by empowering every automobile spreads the data related before landing at the episode put. With an end goal to comprehend the operation protect exercises, thinks about working on this issue study are briefly examined. Green automobile interchanges necessities are displayed to demonstrate the significance of utilizing vehicular innovation. Tests utilizing .Net to quantify the normal defer time per trek and normal throughput for three distinct situations are exhibited.**

Keywords- VANET, Vehicle Communication, Green Computing, Ad Hoc Network, Wireless Network, ACPN.

I. INTRODUCTION

A vehicular system is a sort of wireless systems that has risen in wireless innovations and the automobile business. Vehicular system is framed between moving automobile s furnished with wireless interfaces that could be of homogeneous or heterogeneous innovations. These systems, otherwise called Vehicle Ad Hoc Network (VANET), are deliberated as one of the specially appointed system genuine applications, empowering communications among close-by automobile s and also amongst automobile s and **close**-by developed gear (roadside hardware). VANET an extraordinary sort of Mobile Ad Hoc Network (MANET) which had some expertise in vehicular communications.

VANET depends on smart automobile s and base-stations, which share data through wireless communications. This exchange of material may greatly affect wellbeing and driving, decreasing the quantity of mishaps and advancing transport. Automobile s can be either private, possess by people or privately owned businesses, or open transport (e.g., transports, trains, squad cars, fire trucks, helicopters, and so forth.). Settled gear can have a place with the administration, private system administrators or specialist organizations. The developing vehicular systems will empower an assortment of uses for security which will be connected to lessen mishaps and also to spare lives and diminish wounds, activity proficiency. Enhancing the activity creek and diminish clog may help driver in getting to the precise data and great communications among the drivers and travellers.

II. RELATED WORK

Communication is the most central characteristic for rescue group members in rescue operations and natural disaster conditions. Researchers [15] have projected the use of multicast MANETs as a message media in such surroundings. They used simulation tools to discover the effectiveness of their approached. MANETs are suitable for rescue operations; because of their characteristics such as self-organizing which require non-infrastructure network. Maazen Alsabaan [15] simulated two realistic scenarios in finding any survivors at a mountain and gas pipe explosion. They used Multicast Adhoc On-demand Distance Vector Routing Protocol (MAODV) and On Demand Multicast Routing Protocol (ODMRP) as different multicast protocols. Based on their mock-up results, ODMRP has healthier Packet Delivery Ratio (PDR) and lower potential in both situations. They settled that MANETs can be used for reliable communication in real rescue operations.

M.Dixit, R.Kumar & Anil Kumar Sagar et al. [11] established the MIDAS Data Space (MDS) to obviously share material among rescue requests in MANETs. They applied optimistic replication in MDS for getting the acceptable level of reliability and availability for important information. Consistency management and complexity are the most significant problems which caused by optimistic replication. They solved these problems by means of the tailor-made solutions for emergency and rescue applications.

Meanwhile, investigators in [13] studied the competence of some routing and MAC protocols under the Client- Server architecture to explore MANET usage in rescue and relief applications at emergency situations. Ad hoc networks (e.g. MANET, VANET) can be organized quickly, and ensure communications during the rescue operations because of their adaptive and dynamic MAC and routing protocols. They performed different scenarios rescue operations, respectively.

© 2016, IJCSE All Rights Reserved

In [14], researchers projected MANET-based Observing of Battlefields or Rescue Routes in Urban Scenarios. Satellites are used for portable nodes observing with high precision in open locations such as deserts. However when publication processes occurred in urban surroundings, satellite grounded observing was not capable to detect the automobile s at the parking space inside the building. In this situation, adding the camera to the mobile units is one of the solutions for high precision monitoring in rescue operations and battlefields which has been projected in [14]. The captured images and videos are gathered by using Manet's mechanism. The data is sent immediately to the headquarter using long range communication or central control office for making a true decision.

A.Karmokar & A.Anpalagan et al. [7] projected three types of announcement which are an intra-team announcement, an inter-team statement and a world-wide internetworking for a specific team called unmanned aerial automobile s (UAV) for tactical information operations. When the autonomous team flying close composed, it fashioned ad-hoc manner network to allow information exchanges. The experiment showed that their network architecture supported the operational functionality for multiple autonomous teams.

Meanwhile, R.Singh & S.Miglani et al. [10] conducted the autonomous underwater automobile s (AUVs) for ocean searching operation. The underwater automobile s are communicated through a command and control unit (CCU) within a limited announcement range. In similar situation, [9] projected the disaster-relief grid style by using self-organizing ad hoc networks which enable earlier response to characteristic communications with high bandwidth. It is importance for rescue workers to get accurate and consistent information to control and coordination the rescue operations.

Rendering to above works reviews, most of the preceding approaches have focused on routing, MAC and multicast protocols in MANET environments for investigation of rescue operations. Thus, a new model or framework which includes all these ideas needs to be industrial. Seeing that the foremost mechanisms of rescue operations are automobile s such as ambulances, helicopters and police automobile s, using the VANET as network infrastructure would be a better solution.

III. VEHICLE AD HOC NETWORK

The technology of establishing a network from automobile s with embedded wireless equipment is known as Vehicular Ad-Hoc Networks (VANETs) which is a special type of Mobile Ad- Hoc Networks (MANETs). VANETs vary from substructure grounded networks such as cellular grids in the demanded gear to form a portable network. The forthcoming typical feature in the next group of automobile s, the wireless network interfaces, is the only needed VANETs investment. Safety and traffic organisation are regarded as unique of the chief VANETs abilities whereby unconfident road conditions, traffic jams, or rapid halts can be stated by an automobile to others.

A. The VANET Challenges

The special conduct and features of VANETs generate some experiments for vehicular communications, which can greatly impact the future deployment of these networks. Below we try to enumerate some of those challenges.

- The design of the conveyance procedure for VANETs is somewhat at its first phase. Here we font have transport procedure modified for vehicular networks so far, and it is also very difficult to design new protocols or adapt existing protocols by modifications or enhancement.
- Hardware engineers for VANETs has no full or sufficient capitals and capacity for a full functional mobile ad hoc network this stances a thoughtful scalability issue for the hardware designers. For example, a small node density situation would involve very few cars to communicate in which some automobile s may be out of range completely. As for great concentration circumstances, sharing bandwidth may pose to be a challenge for VANETs
- VANET is a cooperative technology and potential customers may not see the immediate value. This poses a business challenge for VANET especially in creation of new market for the technology. Newer cars could all be equipped with VANET, but would not be able to communicate with the older automobile s.
- New protocols and wireless transmission schemes for VANETs cannot be implemented in large test bed systems due to complexity and costs. Therefore, simulation of VANETs is a crucial method to evaluate new approaches. However, the specific characteristics of vehicular networks also require specific simulation models. New road-based mobility models including the behaviour of potential drivers are one example for a specific simulation model.
- One of the biggest hurdles for any new technology today is security. VANET promises to provide safety and entertainment to its users, however there are risks to using it. On-board Unit's provide communication to other cars in the area, without a proper security they are threats to the system.
- Technologies like the cell phones are already acting as portable computers in cars, GPS units are being used to route alternate directions, and safety systems such as On-Star can notify authorities in the happening of an emergency. With technology increasing data rate in cellular phones, there may not be a need to use cars as nodes on a network.

© 2016, IJCSE All Rights Reserved

IV. ACPN METHOD

A novel verification framework with provisional privacy-preservation and non-repudiation for VANETs, counting initialization, the pseudonym group, and the process of ACPN. The ACPN for VANETs, consider the UVC structure for VANETs, which consists of an RTA, finite numbered registered RSUs along roadsides, and a large number of automobile's on or by the roads. An RTA serves in one region, e.g., a city, a province or a country. An ID pool of RSUs in a region is preloaded in each automobile, in which the number of RSUs is usually fixed that does not change frequently. The automobile registration is required before an automobile starts off to hit the road in a region. If the automobile is newly manufactured, it can be registered to the RTA at the car dealer via a secure network infrastructure. If an automobile is driven into a new region, it can be registered to the RTA at the entry-exit administration or the border immigration office via the secure network infrastructure. Through the automobile registration of each automobile, the RTA registers the automobile ID and profile, then publishes and distributes the RSU ID pool and the certified domain parameters for authentication to the automobile.

In ACPN for privacy preservation, the PKC-based pseudonym of an automobile is generated instead of the real-world ID in the authentication process. Since the RTA is periodically broadcasting the current public key via RSUs for the PKC in the pseudonym group, the automobile can use it for the PKC-based pseudonym generation, when it wants to update its current pseudonym or generate a new pseudonym.

Define the self-generated PKC-based pseudonym of an automobile as follows:

$$PS_v \stackrel{def}{=} Time||E_{pk}(ID_v)||HR||RSU$$

Where Time is the current time, when the pseudonym is generated. E_{pk} (ID_v) is the encrypted value generated from the automobile's real ID, by using the current PKC's public key ${}_pk_c$ obtained from the RSU broadcasts. HR denotes the code name of the automobile's home region. RSU denotes the ID of the current corresponding RSU, where the automobile updates or generates its new pseudonym for secure authentication and communication. The authentication in VANETs can be divided into three categories, namely automobile -to-roadside authentication, roadside- to-automobile authentication and automobile -to-automobile authentication. In the projected ACPN, RSUs are broadcasting their information periodically, and all the operations at RTAs and RSUs are tamper-proof and being performed trustfully. The projected ACPN operates adaptively, whenever an automobile wants to newly authenticate itself to others, or update its current pseudonym.

A. V2R and R2V Authentication

Step 1:

The RSU is broadcasting its information periodically, which is used for the V2R and R2V authentication. Therefore, the automobile s in the transmission range can get the RSU's information <ID_r, T, pkc, adv, nonce, SIGr (ID_r||T)>, where ID_r is the ID of the broadcasting RSU, T is the time stamp for the current time interval. Pk_c is the public key of PKC issued by the RTA, which is used during the current time interval. The advertisement message adv is the invitation of V2R authentication in the next step and the nonce is for freshness. SIG_r (ID_r||T) is the IBS for R2V authentication, which is generated from the RSU's ID ID_r and the time stamp T.

Step 2:

An automobile replies a message to the corresponding RSU in either of the following two cases, by using IBS for V2R authentication:

- An automobile wants to newly generate or update its pseudonym for authentication and communication in the VANET system.
- An automobile receives a new RSU ID from an RSU's broadcast.

The automobile unicasts its new pseudonym to the RSU in the message ID_r,PS_v,T,join,$SIG_v(PS_v||T)$, where ID_r indicates the destination RSU_r, PS_v is the newly generated pseudonym, join is the join request message, and $SIG_v(PS_v||T)$ is the digital signature generated from the automobile 's pseudonym PS_v and the time stamp T.

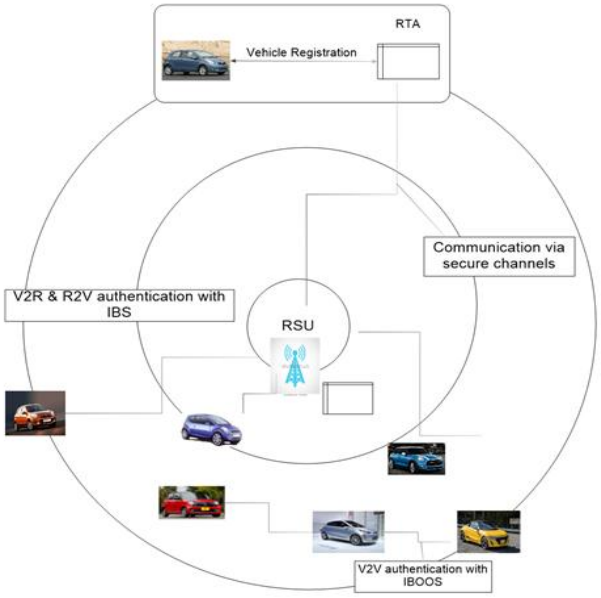

Fig.1: ACPN Architecture

© 2016, IJCSE All Rights Reserved

B. V2V authentication

Step 3:

After receiving the join request message from an automobile, the RSU verifies the signature, and accepts it if the message is authenticated. The RSU first updates the pseudonym PS in its memory, as well as reports it to the RTA. Afterwards, the RSU generates the offline signatures $SIG_v^{offline}(PS_v$ from the pseudonym PS_v for the automobile V_v. The RSU then broadcasts an allocation set message to all the automobile s in its transmission range for the V2V authentication, by using IBS for R2V authentication. The allocation message includes a pseudonym/offline signature/RSU ID (POI) set in the form of $(PS_v| SIG_v^{offline} (PS_v|ID_r)$, attached with a nonce, yet to be concatenated with the digital signature $SIG_r (ID_r||t)$. Here ID_r denotes the corresponding RSU, where the POI set is generated. All the automobile s in the cur- rent RSU's transmission range receive the message, and accept it if the signature verification is valid. Then, regarding the acceptable POI set according to verification, the automobile stores and updates the POI sets in its memory if its storage is possible, otherwise, drops it.

Step 4:

The V2V authentication, which is also called inner-RSU V2V authentication, is used for secure vehicular communication among automobile s. During the V2V authentication, automobile s use the received POI sets for verification for authentication. As a sender, the automobile first computes the online signature SIG^{online} from the offline signature $SIG_{offline}$, by using the IBOOS scheme for authentication. Then, the receiver automobile s can use the online signature for the V2V authentication.

C. Cross-RSU V2V authentication

Step 5:

Assume that automobile w is aiming to authenticate itself to the nearby automobile s. Thus, automobile w broadcasts the authentication message with its online signature SIG_w^{online} in the form of $<PS_w, t, nonce, SIG_w^{online} (SIG_w^{offline} (PS_w||t))>$.

Step 6:

Once the authentication message is received from automobile w, automobile u checks its storage for the pseudonym and the POI set of automobile w. If the information does not appear in automobile u's storage, automobile u transmits its query message q.y. of authenticity to the nearest RSU, which includes the POI set of automobile w in the form of $(PS_w| SIG_w^{offline}(PS_w|ID_r))$, signed with the IBS SIG_u.

Step 7:

After receiving the queried message, the current RSU queries other RSUs or the RTA via secure channels to check if the POI set is authenticated. Afterwards, the cur- rent RSU replies the query result q.r. signed with SIG_r back to the querying automobile u, whether or not the POI set is authenticated.

V. EXPERIMENTS & RESULTS

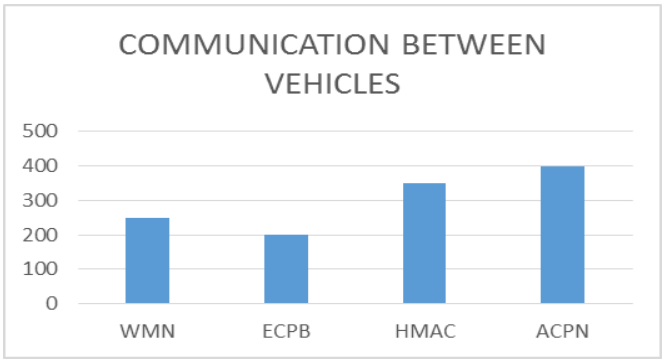

Fig.2: Communication between Vehicles

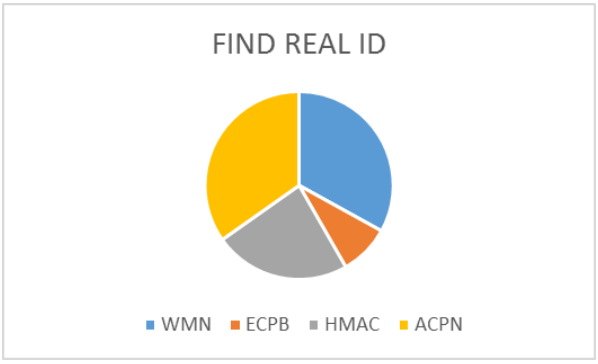

Fig.3: Find Vehicle Real ID

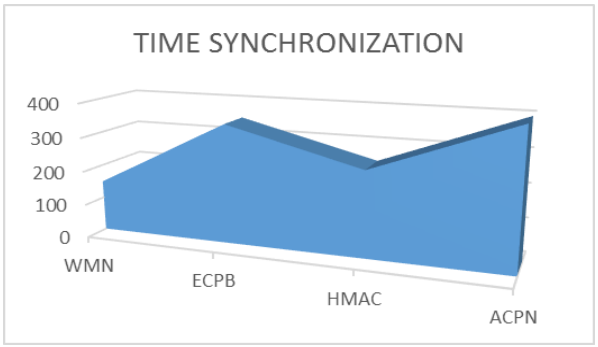

Fig.4: Time Synchronization of Vehicles

© 2016, IJCSE All Rights Reserved

VI. CONCLUSION

A fresh authentication outline with conditional privacy-preservation and non-repudiation for VANETs has been projected, which utilizes the IBS and IBOOS schemes for the authentication, the pseudonym- based scheme for the privacy preservation, and the PKC- based scheme for the pseudonym generation. The public-key cryptography (PKC) to the pseudonym generation, which ensures a legitimate third party to achieve non-repudiation of automobile s by obtaining their real IDs. The IBS scheme for the automobile - to-roadside (V2R) authentication and the roadside-to-automobile (R2V) authentication, which is efficient in communication. To reduce the computation overhead by IBS in authentication. ACPN achieves the desired authentication, privacy preservation, non-repudiation and other security objectives for UVC in VANETs. Another important characteristic of ACPN is its reusability, i.e., it can also be utilized with other new schemes for security and performance improvements. ACPN is feasible such as authentication, privacy preservation, non-repudiation, time constraint, independency, availability and integration. Analysis and performance evaluation show that, the projected ACPN is feasible and adequate to UVC in the VANET environment for efficient privacy-preserving authentication with non-repudiation.

A. Future Work

The future research, there is needed to build a generic architectural framework towards addressing these security and privacy issues/challenges in a holistic manner. Now, in a new era where provided security and privacy issues will help to discover new knowledge that no one has discovered before. So everybody is warmly invited to provide a safe, secure and trusted environment to moving objects.

REFERENCES

[1] Xiaohu Ge, Hui Cheng, Guoqiang Mao, Yang Yang & Song Tu, "Vehicular Communications for 5G Cooperative Small-Cell Networks", in IEEE Vehicular Technology, Vol.65, Issue.10, Oct. 2016.

[2] M.Boban & P.M. d'Orey, "Exploring the Practical Limits of Cooperative Awareness in Vehicular Communications", in IEEE Vehicular Technology, Vol.65, Issue.6, June 2016.

[3] M.Uysal, Z.Ghassemlooy, A.Bekkali, A.Kadri & H.Menouar, "Visible Light Communication for Vehicular Networking: Performance Study of a V2V System Using a Measured Headlamp Beam Pattern Model", in IEEE Vehicular Technology Magazine, Vol.10, Issue.4, Dec.2015.

[4] Li Li, D.Wen & D.Yao, "A Survey of Traffic Control with Vehicular Communications", in IEEE on Intelligent Transportation Systems, Vol.15, Issue.1, Feb.2014.

[5] U.Rajput, F.Abbas & Heekuck Oh, "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET", in IEEE, Vol. 4, October 2016.

[6] Arrate Alonso Gomez & Christoph F. Mecklenbräuker, "Dependability of Decentralized Congestion Control for Varying VANET Density", in IEEE Vehicular Technology, Vol. 65, Issue.11, Nov.2016.

[7] A.Karmokar & A.Anpalagan, "Green Computing and Communication Techniques for Future Wireless Systems and Networks", in IEEE Potentials, Vol.32, Issue.4, July-Aug. 2013.

[8] Qutaiba Ibrahim, "Design, implementation and optimization of an energy harvesting system for vehicular ad hoc networks' road side units", in IET Intelligent Transport Systems, Vol.8, Issue.3, May.2014.

[9] W.Feng, H.Alshaer, J.M.H.Elmirghani, "Green information and communication technology: energy efficiency in a motorway model", in IET Communications, Vol.4, Issue.7, April.2010.

[10] R.Singh & S.Miglani, "Efficient and secure message transfer in VANET", in: Inventive Computation Technologies (ICICT), Aug. 2016

[11] M.Dixit, R.Kumar & Anil Kumar Sagar, "VANET: Architectures, research issues, routing protocols, and its applications", in Computing, Communication and Automation (ICCCA), 2016 International Conference on April 2016.

[12] N.Goel, G.Sharma & I.Dhyani, "A study of position based VANET routing protocols", in Computing, Communication and Automation (ICCCA), 2016 International Conference on April 2016.

[13] Y.Mao, H.Luan, W.Liu, R.Yang, M.Jin, X.Jin & Z.Xu, "Experimental investigation of carrierless amplitude-phase transmission for vehicular visible light communication systems", in Communication Systems (ICCS), 2016 IEEE International Conference on Dec. 2016.

[14] Jamal Toutouh & Enrique Alba, "Green OLSR in VANETs with Differential Evolution", GECCO'12, July 2012.

[15] Maazen Alsabaan, "Greener electric vehicles with VANETs", in: Electrical and Computer Engineering (CCECE), May 2015.

© 2016, IJCSE All Rights Reserved