A New Handover Scheme for Providing Security in VANET

Shanmuga Priya.S
PG Scholar
V.P.M.M Engineering College for Women, Krishnankoil, India.
Computer Science and Engineering

ABSTRACT
Vehicular Ad Hoc Network (VANET) is the subgroup of the Mobile Ad Hoc Network (MANET). VANET interconnects the nodes for transferring secure information between nodes, here vehicle acts as a node. VANET is used to provide safety and efficiency in transportation system. Many traffic signals are used to reduce accidents in the roads, but since it is not much effective. Hence VANET is used; it uses Road Side Unit (RSU). This RSU connects to the internet, and provides information to the Vehicular Ad Hoc Network users. Each and every vehicle is interconnected to each other hence it can send alert message to another vehicle to reduce the speed or increase the speed to avoid accidents. Each and every vehicle can use internet facility while traveling. Since mobile internet is used nowadays but this road side unit internet connection is more speed. The information transferred between vehicle and RSU is more secure, because the road side unit provides unique key for each and every user connected to it. When the vehicle is moved out of the particular range, handover scheme occurs. The bending information will be transferred from old RSU to the new RSU. The service provided by the road side unit is called *Service-Oriented Vehicular Ad Hoc Network*.

Keywords
Service-Oriented Vehicular ad hoc networks, Road Side Units, hierarchical password-based key derivation, anonymity.

1 INTRODUCTION
The nodes in the Vehicular Ad Hoc Network (VANET) is different from Mobile Ad Hoc Network(MANET) that in VANET the vehicles moving randomly. Here the vehicles acts as nodes, such as car, bus, truck. VANET is used for information sharing, co-operative driving, and internet access. The vehicles are communicated with each other within 100 to 300 meters VANET and it is used for safety, information sharing and internet access. Vehicle communication system is classified into two categories vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The communication between V2V and V2I are ad hoc connection. Ad Hoc Network is a method for wireless devices for directly communicating with each other. It controls in which way nodes decides to move. V2V provides the short range of vehicular network, whereas V2I provides long range of vehicular network. The VANETs are supported by fixed infrastructure, which deploys at critical situation such as slip roads, dangerous intersection, and weather conditions. The information provided by VANET to the vehicles are current speed, location and also services like email, audio/video sharing. These types of services are called Service-Oriented VANET. The goal of VANET is to provide safety in roads. To achieve this, the vehicles act as sensors and exchange warnings. If any vehicle is out of the speed limit then other vehicles can send a warning message to that particular vehicle, by receiving the information the driver get alert and controls speed and avoid accidents. VANET security provides confidentiality, integrity, availability. All this security is done by using the public key infrastructure to protect integrity. This can create own maps to control the traffic data.

The nodes in VANET moves in well-defined path. Unlike MANET, nodes in vehicle do not move randomly. The routing used in VANET are proactive routing, reactive routing, position based routing. The vehicle with VANET application contains positioning system, communication facility, and human-machine interface in the vehicle. If a vehicle contains all these facilities then the number of accidents can be reduced and the data sharing will be more confidentiality, integrity, and availability. All this are done by using the fixed infrastructure called Road Side Unit (RSU). It connects to internet and produces the needed information for the user, when the vehicle is connected to particular nearby RSU. The vehicle identifies the nearby RSU by using the digital positioning system which is attached in the vehicle. Once the vehicle identifies the nearby RSU, it sends the hello packet to get the conformation. All information will be provided to user when they are registered in RSU. But for sending the warning information between two vehicles there is no need for registration. The authentication done through digital signature algorithm. This provides the unique key for all users who had register in the RSU. The RSU is placed in each and every end of the corner of the road. The road can be either 4 way road or any other. If any vehicles are out of the range then it will be connected to another nearby RSU, which performs the handover scheme to do this connection. Service-oriented VANET is used for real time management system. This information sharing to the user is called Service-Oriented VANET. The RSU and vehicles are communicated using DSRC wireless protocol.

The wireless communication technologies make the human lives most convenience and flexibility in accessing internet services and many applications. Then for making wireless communication among vehicles many researches are undergone and then introduced the concept of Vehicular Ad Hoc Networks (VANET). In VANET the cars are the nodes and make a safety and comfort travel through this wireless communication. VANET makes the vehicles to communicate with the Road Side Unit (RSU) and also interconnected to the vehicles.

The connection is made through mesh network. To make this type of services to the user the vehicles and RSU are connected through the wireless communication modules. The connection will be stable even though the vehicle to infrastructure communication is out of range. The information's provided from RSU to the user are internet access, checking mails, downloading maps and news. This type of providing information to the user is called Service-Oriented VANET.

Powerful tools are available in the intervehicular communication (IVC) and also number of attacks occurs. The user privacy and data confidentiality are provided in the old techniques, but the security of data and location privacy is provided in the Service-oriented VANETs which gain the high throughput and latency.

Different types of security requirement are available in the service-oriented VANETs. The data exchanged in safety messages are no need to encrypt whereas the data from the infotainment application are needed to be encrypted. The asymmetric encryption systems are used to provide the location privacy between the user and RSU. To increase the security level among the users symmetric encryption system is used. Many security systems are used for the transportation work such as pseudonym, mix zones. For reducing the congestion detection VANET is used.

2. BACKGROUND

Existing systems used some techniques in order to increase the security between vehicles to reduce the accident in transportation system. Some problems occurs in each techniques. Hence to reduce this problems Road Side Unit is used, which increases security in transportation system. Road Side Unit connects to the internet and provides the security information to the user and hence accidents can be prevented. The authenticated user can only access to get the information.

2.1 Pseudonyms

If the user uses the same ID for sending a safety message then the attackers can easily detect the ID and creates a duplicate profile and hacks the safety message of the user. Hence to reduce this problem pseudonym is used [9]. The mail goal of pseudonym is to hide the identity of vehicles location from the attackers. Changing the pseudonym often reduces the identification of the same pseudonym. Certificate Authority (CA) is responsible for issuing the private key for each registered user. This scheme reduces the link between vehicles and pseudonym [12]. But the drawback here is still the safety message can be easily tracked by the attackers when the vehicle is out of range. Hence this scheme is useful when the vehicle is within the range.

2.2 Mix Zones

This pseudonym breaks the link between old and new pseudonym by monitoring the temporal and spatial relations between them. To reduce this identification, the vehicles change their pseudonyms together. A Mix zone is used for providing location privacy in Vehicular Ad Hoc Network. This scheme is done by creating a protocol called CMIX protocol to get the key for each vehicle instead of frequently changing pseudonym [6]. And then analyses the location privacy. Here there is no uniform in the traffic hence the attackers can easily find the location of the vehicles.

2.3 Silent Period

This scheme makes the mobile users to change the pseudonyms with another user [9]. This the first scheme which uses the random address approaches. This scheme identifies the duplicate address by monitoring the station and finds the history of addresses used by the other user and avoids same address used by multiple nodes [15]. If the address is used in the base station then the request from that address of the station will be rejected by the access point. This random approach creates a security problem by blocking the handover to the management.

2.4 AD HOC ANONYMITY

Road Authority (RA) is responsible for the road network. RA uses RSUs to communicate with the vehicle. Some users generate false (dummy) address to prevent their location [16]. The false address and original location sends to the service provider. Because the original location cannot be found by service provider. If attackers intercept to find the location they cannot easily find the true location. In this scheme the communication cost is reduced. But still the dummy location is so far to the user of the vehicle.

3. SERVICE-ORIENTED VANET

The service oriented VANET is introduced to overcome all the problems in the above methods and also to provide efficient security. This approach produces internet facilities to the users who are connected to Road Side unit (RSU). To provide confidentiality the cryptographic algorithm is used which provides unique private key for all users who are registered in RSU. The algorithm used in service-oriented VANET is HARDY function. The cryptographic algorithm can either be symmetric and asymmetric approach. RSA and ECC mechanism for symmetric approach and AES mechanism for asymmetric approach

3.1 Average overhead traffic

Average overhead traffic (AOT) is the overall traffic delay between the time taken for sending and receiving information packet from and to the user. If a user A sending a large packet then time increases for sending this packet. Another user B sending a packet which is also large then here occurs traffic.

3.2 Initialization phase time

It is the security time taken at initial, it is time taken between the vehicle start time and initial packet sending time. In ABAKA each and every request is sent to the Service Provider (SP) hence there occurs delay, but in REACT no need of sending each request to service provider. Hence this reduces time delay at initial.

3.1 Registration in RSU

RSU is placed at each corner of the road. When the user of the vehicle needs to connect to RSU, first user must register to RSU. This registration is done through web; it is done only once to create an account. For registration the user must specifies the name, address, username, password and the current location. Each user selects the default RSU by sending the hello packet to the nearest RSU which sends back the needed information to the user. RSU connects to internet and provides the information such as traffic data, map, email, internet access.

3.2 Providing master key to the user

After the account is created for user, the RSU contacts the TA to obtain key. The user receives the master key once they connected to RSU. To provide this key the encryption function is used in the Iteration Count(IC). The secret key is provided for each user to encrypt the authenticated data from the user. Using this private key the user information is transformed very secure and confidential manner. This master key is unique for all user registered in RSU.

3.3 Participating in session

The user sends the hello packet to the RSU and starts the session. Each packet has a timestamp to reduce the attacks.

The transformation of delay is occurred until the user sends the master key to verify whether the user is authenticated. The pseudonym is used to reduce the attacks. If the username and password matches then the RSU sends the needed information to the user.

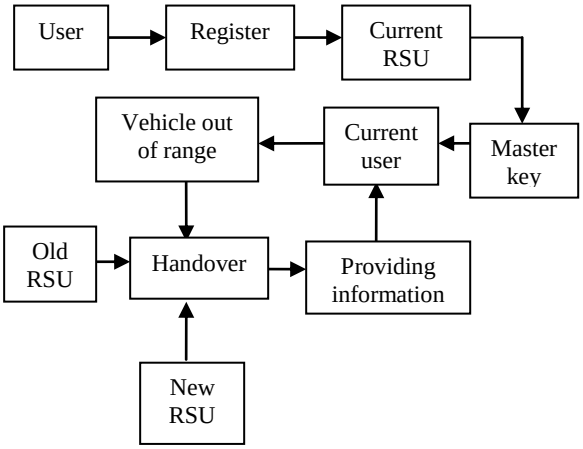


Fig-1: Block diagram of Proposed Technique.

3.4 Switching connection between RSU (handover)

A vehicle observes its current location and calculates the distance from all nearby RSUs using digital map. If any RSU is closer than the current RSU then the vehicle switches to new RSU. This is done by sending the handover request to old RSU; the old RSU sends the handover packet to the new RSU with the username, master key, and pseudonym. After receiving the particular request the new RSU sends back the handover confirm message to the user connected to the new RSU. This process is called handover scheme. Then the user sends a hello packet to new RSU, new RSU decrypts the packet and checks whether the username is valid. This encryption and decryption is done by using the symmetric and asymmetric approach. If so then the new pseudonym and ID packet is send to the user from new RSU. If there is any pending data to the user from old RSU, then the old RSU forwards it to new RSU, then all the needed information for the user will be send from the new RSU. The communication between mobile user and the access point is a single-hop connection. But the communication between vehicle and RSU are multi-hop connection. Old RSU sends all the pending request of the user to the new RSU. Once all the details about the user are received by RSU then the acknowledgement will be sent from the new RSU to the old user. After sending acknowledgment a new pseudonym will be assigned by the new RSU to the old user.

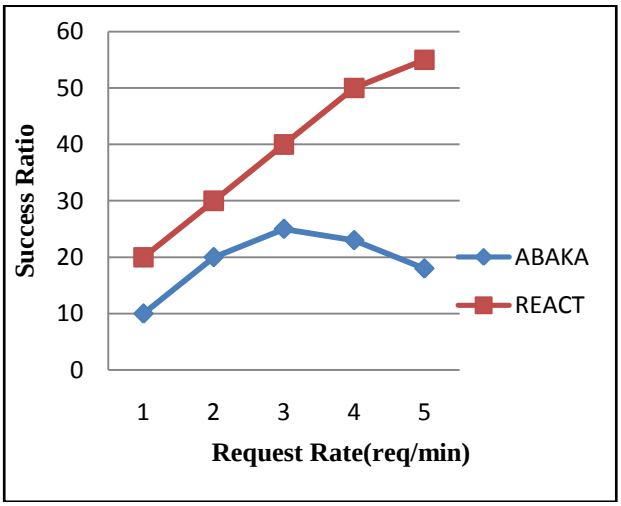
The new RSU verifies all the details of the user to check whether there is any illegal information. The packets send between vehicle and RSU is done through the multi-hop connection. This packet is smaller in size hence it can be sent easily in a small duration of time. The handover scheme done in REACT is reduce to 20m/s compared to ABAKA. The protocol used for transmitting the information from user to RSU and from RSU to user is ROAMER. In many systems only one key is used to encrypt all message which may allow for eavesdropper hence to reduce this service-oriented VANET uses single key to encrypt single message.

For each and every request a pseudonym is assigned to enhance the location privacy. For each user a pseudonym is created by RSU, when a request is sent from the user the reply from the RSU sent along with that pseudonym is added and sent to user. Then the user uses that duplicate ID and sends for another request. Then again RSU sends reply with the another duplicate ID. This process continues until there is a connection between RSU and user. If the user uses the old ID then RSU sends the alert message to the user, then the user reassigns the ID and back the previous request to RSU. Then the correct transformation occurs without any error or attacks.

4. SIMULATED RESULTS

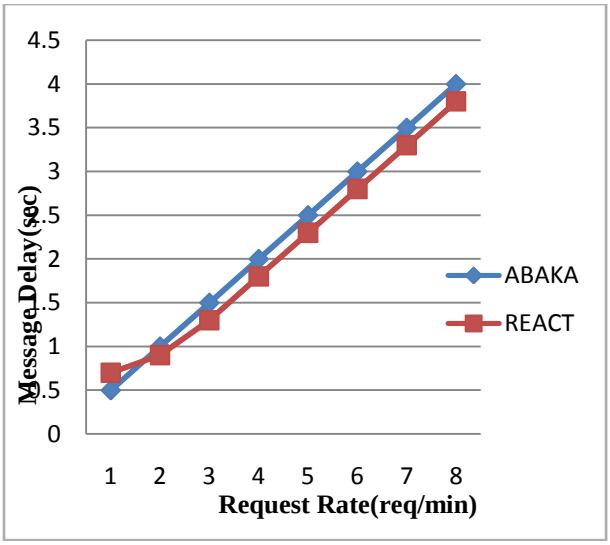
4.1 Message Success Ratio

The message success ratio is calculated based on the number of request sent from the user to RSU and message delivered for that particular request to the user from RSU. The calculation of MSR shows that the percentage of successful messages send to the destination. Comparing to ABAKA, REACT has a high percentage of successful message delivers. For each message request from user ABAKA verifies it using Service Provider. Whereas REACT does not verifies each message using Service Provider. Instead of this REACT encrypts the message, hence here the information needed for the user is sent earlier when compared to the ABAKA. Fig.2 shows the message deliver ration between ABAKA and REACT. The message deliver ration for REACT is higher than the previous method ABAKA.



4.2 Message Response Time

The message delay is calculated based on the ratio between request send from a user to RSU and response received from the RSU. The delay occurs when the request packet is not send from the user at correct time and delay in sending the needed information for the user. Due to this there will be delay in issuing the key for each vehicle connected to RSU. The delay rate for REACT and ABAKA are almost similar. The authentication is done for each and every request in ABAKA and hence there will be more number of delay rates.



5. CONCLUSION

A service-oriented VANET is proposed to enhance the security and location privacy between the vehicles. Privacy preservation mechanism is used to make the location privacy. Symmetric and asymmetric algorithm is used for generating key for each and every user who had registered in RSU. The effectiveness and deliver ratio are compared with the proposed system. More number of users can connect to the RSU. The Time Slots (TS) are introduced to connect many users to the single RSU. If a user finishes retrieving information from RSU, then the time slot will be free hence another user can get connected to RSU. Equal amount of load will be distributed to all a user who are connected to the RSUs.

6. ACKNOWLEDGMENT

I would like to thank our respective head of the department Prof. Mrs. Anitha M.Sc., M.Tech. (Ph.D) and our respective guide Mr.S.Erana Veerappa Dinesh M.E, Assistant professor and all who help us to complete the project successfully.

7. REFERENCES

[1] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

[2] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, "EP2DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 580–591, Feb. 2011.

[3] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[4] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in *Proc. ITST*, St. Petersburg, Russia, Aug. 2011, pp. 613–618.

[5] N. V. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad hoc networks," in *Proc. IEEE ISWTA*, Langkawi, Malaysia, Sep. 2011, pp. 96–101.

[6] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside unit's deployment for efficient short-time certificate updating in VANETs," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010, pp. 1–5.

[7] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 16–22, Aug. 2009.

[8] E. Coronado and S. Cherkaoui, "Service discovery and service access in wireless vehicular networks," in *Proc. IEEE GLOBECOM Workshops*, 2008, pp. 1–6.

[9] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: A new pseudonym refill strategy for vehicular communications," in *Proc. IEEE68th Veh. Technol. Conf.*, Calgary, AB, Canada, Sep. 2008, pp. 1–5.

[10] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[11] B. Mohandas, A. Nayak, K. Naik, and N. Goel, "ABSRP—A service discovery approach for vehicular ad hoc networks," in *Proc. IEEE 3rdAPSCC*, Yilan, Taiwan, Dec. 2008, pp. 1590–1594.

[12] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. ESAS*, Cambridge, U.K., Jul. 2007, pp. 129–141.

[13] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in *Proc. ACM Mobicom*, Montreal, QC, Canada, Sep. 2007, pp. 19–28.

[14] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel.Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[15] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE WCNC*, New Orleans, LA, 2005, pp. 1187–1192.

[16] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. ICPS*, Santorini, Greece, Jul. 2005, pp. 88–97.