IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 31-44
www.iosrjournals.org

Secure Data Access through Multiuser So-VANET

Anju John,Deepu S
PG Scholar,Department of ECE,University College of Engineering,Muttom,India
Lecturer,Department of ECE,University College of Engineering,Muttom,India

Abstract: *The development and wide utilization of wireless communication system have transformed the human trends by providing the most convenient way of accessing internet whenever wherever its necessity comes. VANET Network supporting Service oriented facilities would have been an revolution in communication era if it could be deployed in real time by the introduction of an Efficient Frame work for So-VANET. Here, proposing a Service oriented media access technique for cluster- based vehicular networks for developing an efficient and uncompromising backbone network which is capable of nullifying the issues related. This technique integrates the centralization approach of cluster management and the universal way of forwarding data, where the farthest vehicle forwards data in an effort to maximize the opportunity of advanced notification. The proposed algorithm intends to create stable clusters by reducing reclustering overhead, prolonging cluster lifetime, and shortening the average distance between cluster heads and their cluster members*.

Keywords: *VANET,HARDY,road side unit, key derivation*

I. Introduction

Vehicular mesh networks aim at enhancing security and provide various types of services to the VANET users. Service oriented VANETs are type of Vehicular ad hoc networks that support various services including traffic data management, access to multimedia files, email and news. Various types of attacks have emerged that threaten the security of service oriented vehicular ad hoc networks. Security and privacy in service oriented VANETs depends on the ability to defend against various types of attacks that exist in VANET. This work deals with the design of secure roadside infrastructures that is connected to the internet and provides various types of information to VANET users.

Vehicular Ad Hoc Network 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. 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 travelling. 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..

The previous work of service oriented VANET have done with various aspects such as user privacy or data confidentiality, location privacy. None of the previous work proved to provide security of data and location privacy of users in service-oriented VANETs while ensuring efficient throughput and acceptable end-to end latency even at the multi user environment. This work deals with the study of secure data exchange between users and RSU and location privacy of users who exchange the data messages in multi user Vehicular Ad-hoc network.

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. The main contributions can be summarized as follows.

(i) A new handover scheme that is particularly suitable for VANETs.
(ii) Novel approach for users to start their connections in the VANET in a secure way
(iii) A new cryptographic approach that provides much higher security measures.

(iv) Two novel mechanisms for data confidentiality and users' location privacy in VANETs.
(v) A new clustering algorithm that considers both node position and node mobility in multi user vehicular ad hoc environments.

II. Related Work

Many researches and studies had been conducted regarding the security challenges related to VANETs. In this section we will do a brief analysis of these studies. The paper with title "security of vehicular ad hoc network" describes security vulnerabilities and challenges in vehicular networks. Here a detailed threat analysis, a basic attacker model, and appropriate security architecture are provided. In addition, there have been several proposals for privacy preservation in VANETs [1]. If VANET users use the same ID whenever they send a packet, an attacker could listen to their packets and build a profile of their locations, which harm their privacy. This is a serious security issue. Hence, pseudonyms were proposed to deceive attackers. It preserves the location privacy of a user by breaking linkability between two locations. Considering that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations. Secure and efficient data acquisition in VANETs is one of the recent existing routing method disscuss single user scenario. No multi user techniques are identified or discussed. The main advantage of multi user technique is that, at a time many users can use this at the same time. There is no proper requesting scheduling algorithm. So if there are many users are online at the time then the RSU routing will be overhead.

If VANET users use the same ID whenever they send a packet, an attacker could listen to their packets and build a profile of their locations, which jeopardizes their privacy. Pseudonyms preserves the location privacy of a user by breaking the linkability between two locations. A vehicle can periodically update its pseudonym. Considering that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations, the techniques of mix zones [2], silent period , and ad hoc anonymity[3] were proposed. A mix zone is an area in which several vehicles change their pseudonyms together so that an attacker will not distinguish the new pseudonym of each vehicle. The silent period approach enables mobile users to jointly change their pseudonym with other approaching users by simultaneously entering a silent period, in which all nearby users suppress their location updates and wield new pseudonyms. Ad hoc anonymity extends mix zones by using dummies, which are virtual users that are created before the pseudonym change starts and disappear after it ends. The dummies link several pseudonym change sets together and mix up all the users who have participated in pseudonym changes at different times.

One major disadvantage in the mix-zone approach is the process of pseudonyms refill. For example, the authors in assume that each vehicle acquires a new set of pseudonyms from the central authority when their stored pseudonyms are used. Another disadvantage is that vehicles do not know where the adversary installed its radio receivers, i.e., where the observed zones of the adversary are. Current approaches that use mix zones assume that the observed zones are small and scattered such that users who change their pseudonym every several transmissions will avoid sending multiple packets with the same pseudonym from within an observed zone. This assumption, however, is not viable in case of a global eavesdropper who can hear all messages in the network. Another disadvantage is that a user might not always find other near users that are willing to enter a mix zone.

Pseudonym Scheme: Vehicles form groups, and the messages of all group members are forwarded by the group leader. Hence, the privacy of group members is protected by sacrificing the privacy of the group leader. Moreover, if a malicious vehicle is selected as a group leader, all group members' privacy may be leaked. The group signature is a privacy scheme in [4] which one group public key is associated with multiple group private keys. Although an eavesdropper can know that a message is sent by the group, it cannot identify the sender of the message. A pseudonym is combined with a group signature to avoid storing pseudonyms and certificates in vehicles.

Security Issues: With regard to actual experimentation on VANET security that was done by several projects such as SeVeCom and Safe Spot, notice that most projects focused on the security of safety beacons or traffic messages. In [4] it describes the types of applications whose security requirements were considered by SeVeCom. These applications vary from collisions to cruise control, including obstacles and work zone warnings. Hence, the security of data messages from SPs or web servers is not considered. In addition, ITSSv6 [4] in focuses on its security aspects on the security and privacy of messages and users only in safety and traffic applications. According to such applications require tight deadlines for message delivery (less than 100 ms). Furthermore, the data exchanged in these applications are usually not confidential. Hence, all proposed security systems rely on elliptical curve cryptography or ECC, because it produces less delay overhead than other

schemes, particularly symmetric ones. However, the secrecy level of the exchanged data is sacrificed. According to ECC keys should be twice the length of equivalent symmetric key algorithms to provide the same security level. Hence, it is better to use a symmetric scheme as to encrypt data messages, because these messages do not have a delay restriction. Rather, a high security level is required, because very sensitive data could be exchanged between users and Internet servers through the RSUs (such as e-mails, money transfers, and criminal records).

III. System Methodology

The platform used for making codes in this thesis work is NS2. NS2 differs from most of the others by being an open source software, supplying the source code for free to anyone that wants it.. The implementation of the proposed project can be done in NS2 so that all the simulations can be done easily and helps to show the enhancements compared to the existing systems.

A. System Architecture

Primary purpose of VANET standards is to enable communication-based automotive safety applications, they allow for a range of comfort applications. In REACT, users register once with the RSUs online (through the Internet) before they start connecting to the RSUs from their vehicle. After registration, the RSUs obtain from a trusted authority a master key for the user. The users get their Km the first time they connect to an RSU from their vehicle. Here describes a novel algorithm that uses the users' password from their account to securely transfer their Km to them. Km will be used to encrypt the initial packet key, which is assigned to the user at the beginning of each session. Then, each packet will be encrypted by a set of derived keys. Here also assume a hybrid RSU architecture in which some RSUs are directly wired to each other, others connect to the RSU network through the Internet (using gateways),whereas a third group is both wired to other RSUs and has an Internet connection. In all cases, however, each RSU has a way of connecting to any other RSU. In addition, several TAs are connected to the RSUs through secure wired links. It assume that TAs have powerful firewalls and other protections that prevent them from being compromised. In addition, the RSUs are supposedly equipped with trusted platform modules, intrusion detection systems, and firewalls that enable them to resist software attacks. With respect to hardware attacks, RSUs can be monitored using hidden surveillance cameras such as digital video or analog CCTV cameras that report to a central station, in which observers can immediately notice a hardware attack and take the appropriate actions. The RSUs do not store sensitive data, but each RSU has a secure connection to a database server that stores the RSUs' private information. Each RSU will have its own database to avoid the effect of failures. In addition,here assume that each RSU will be monitored by a TA, which, upon detecting a malicious behaviour from the RSU, will isolate it from the network by informing other RSUs, which inform vehicles that are connecting to them

Registration: The registration is done by the user only once to create an account with the RSUs. RSU stores the personal details i.e., Name, Address, Phone number plus a username and password. Users also choose a default RSU, which will save their account in its database. Examples of users' interests are web pages, certain news, and email messages. When they later connect to the VANET, they send a Hello packet to the nearest RSU, which will notify their default RSU, which in turn, retrieves their interests from its database and collects the required data for them. Kc is used by the RSU to encrypt their authentication data and save them. Some user interests may require authentication, which means that the RSU needs to obtain from the users their credentials with the corresponding SPs so that it can connect to these SPs(Service Providers) on the users' behalf. In REACT, we require users to provide during registration their authentication data with these SPs in addition to a secret key Kc that is used by the RSU to encrypt their authentication data and save them When the users connect to the VANET from their vehicle, they send Kc to the RSU.

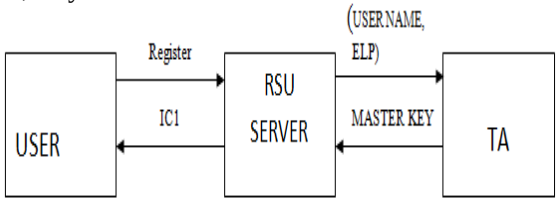

Fig 3.1: block diagram for online registration scenario

Once registration is completed default RSU saves account and contact TA to serve Km. After registration they connect from their vehicle to one of the RSUs. To achieve this, we propose a technique that

depends on deriving a group of encryption keys from the users' password (of their account with the RSUs) and using these key to securely transfer Km to them. To generate these keys, we propose a new key derivation and encryption function. One of the inputs to this function is an initial iteration count (IC1), which an integer is kept as a secret between the user and the RSU. After registration, the RSU generates IC1 and sends it to the user, who saves it and uses it as an input to the hierarchal password-based key derivation (HARDY) function when he/she obtains and decrypts Km .

Participating in a Session: Each time a user connects to an RSU, he/she starts a new session. A user starts by sending a Hello packet that contains his/her username to the nearest RSU. As receiving Hello packet, it starts preparing the user's data regarding their interests. Interests that require authentication with other systems will be delayed until the RSU gets Kc from the user. Although the RSU prepares users' data, it assigns them a pseudonym and sends it to them in an ID packet. The user replies with an "Identify" packet that contains his/her username, password, and Kc . Both packets will be encrypted using Km. The RSU authenticates users using their password, and if successful, it retrieves from its database the user's encrypted credentials with other SPs and uses Kc to decrypt them and sends them to the corresponding SPs on behalf of the user and obtains their data.

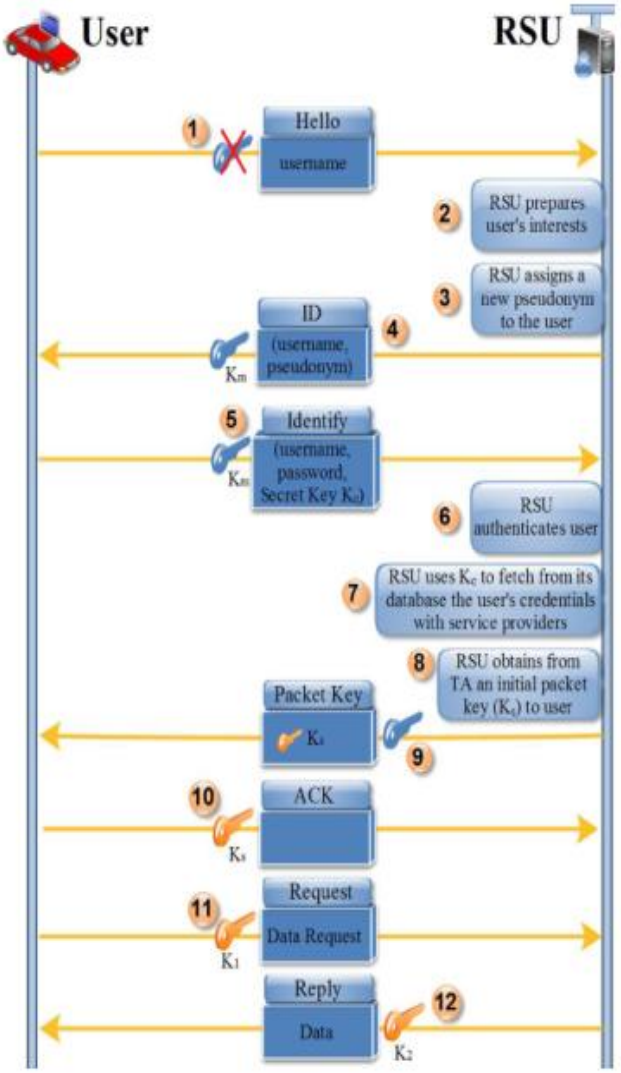

Fig3.2: Sequence Diagram for Participating in a Session

Handoff procedure: A vehicle observes its current location at constant intervals of time and calculates its distance from all nearby RSUs using the digital map. When it finds much closer to another RSU (30%), it switches to it. Contrary to handover in traditional wireless networks ,where the communication between the

mobile user and the access point is always through a single-hop connection, the communication between a vehicle and an RSU could traverse several vehicles (i.e., multihop). Hence, the packets exchanged between the vehicle and the RSU during a handover could be sent in a multihop manner. These packets small in size compared to data packet hence less time to travel(<20ms). This is mainly due to using an efficient routing protocol ROAMER "store-and-forward and location-based routing techniques". Also evaluating, superiority of ROAMER over three recent VANETs routing protocol and its ability to route packets between far locations.

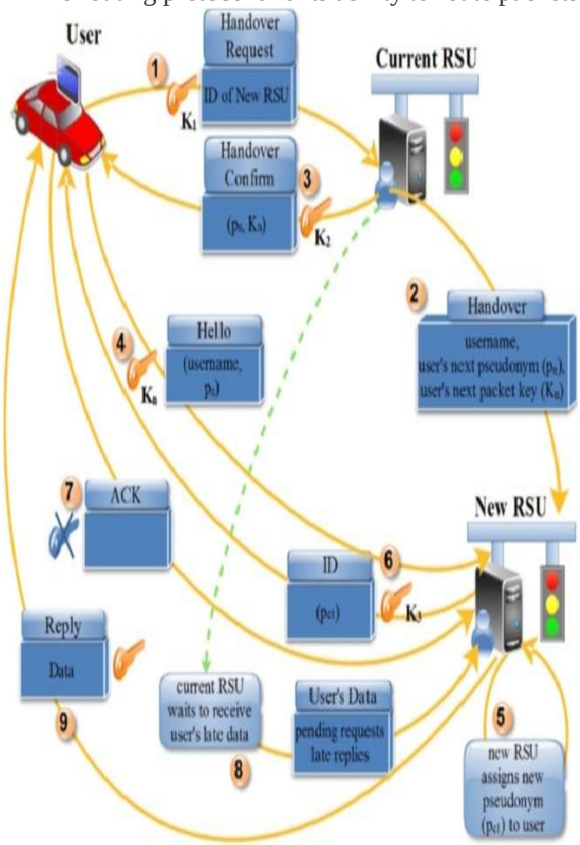

Fig 3.3: Handoff Procedure

B. Security And Privacy

To provide data confidentiality, encryption is used to allow only the legitimate user to read and process the transmitted data. Cryptographic schemes are either symmetric or asymmetric, where symmetric schemes use a single key for both encryption and decryption, whereas asymmetric schemes use a public key for encryption and a private key for decryption. Here designed an algorithm for securing data messages based on using a symmetric scheme for cryptographic operations. The algorithm is used by the source to generate a sequence of keys from a secret input string (S) and uses these keys to encrypt the next packet. The input string (S) is specified as part of the data in the current packet. Here also use this algorithm to transfer the master key of the user to him/her, where the input string (S) to the algorithm will be the user's password.

After the users have registered, they need to obtain their master key Km from the RSUs. However, the RSU needs to authenticate the users to send Km to them. However, the users cannot send their password to the RSU in plain text. To solve this problem, here proposes that the RSU will use HARDY to generate a sequence of encryption keys from the users' password and uses them to safely transfer Km to them. The users use their password to generate the same keys and to decrypt Km. However, we assume that RSUs accept only passwords with high entropy (e.g., above 60).

Users start their initial session after registration by sending an Initiate packet to their nearest RSU. This packet contains the users' username and ELP. The ELP is a unique electronic identifier that is issued by the government to each vehicle. The ELP is cryptographically verifiable by the TA. Hence, when the RSU receives the Initiate packet, it sends the ELP and the username to the TA, which authenticates the user and replies to the RSU. If the RSU receives a positive reply from the TA, it obtains from the user account the password, IC1, and

Km and executes the HARDY function. Here, the user's password (P) will be passed to the HARDY function as the string S, and Km will be passed as the plain-text message Mp. The result of HARDY will be the cipher message Mc, which the,RSU sends to the user in a Master Key packet. The user executes the HARDY, function, passing to it (P) and IC1, to decrypt Mc and obtain Km. Note that, as long as the user's password an IC1 are known only to the user, he/she is the only one who can decrypt Mc. Hence; the security of Km is coupled with the secrecy of the password and IC1. For this reason, the user needs to keep these two in a very safe state and should obtain a new password and IC1 from the RSUs each time he/she changes his/her master key. Note that the process of assigning a new Km to a user should be executed at constant periods of time (for example, yearly or half yearly) such that highly sophisticated attacks will not be able to crack Km.

Ensuring Location Privacy: In REACT, each RSU stores a table Tr .Current ID is the last pseudonym that the RSU sent to the user, whereas next ID is the pseudonym that the RSU will send to the user in the next packet. When the RSU receives a packet from users, it identifies them by looking up their pseudonym in the current ID field in Tr. When the RSU sends the next packet, it includes in it the next ID, which will be used by the users as their new pseudonym. The RSU then generates a new pseudonym Pn and replaces the users' current ID with their next ID and the current value of next ID with Pn.

To account for lost or corrupt packets, the RSU does not delete the old pseudonym but stores it in a temporary table Ttem.In the future, if the RSU receives a packet from the user in which he/she uses his/her old pseudonym, it assumes that the user has not received the new pseudonym.

C. Proposed Scheme

In the previous case we have control over only one vehicle but in this enhanced mode we can control many vehicles in the traffic at a time. The RSU is used to provide control signals to the vehicle when more than one vehicle is arrived. A group of vehicles arrived then select a cluster head and each RSU is connected to the cluster head. The cluster head controls the RSU functions. If a group of vehicles are arriving from the same direction then it merges and select one cluster head. In other case there will be no merging occurs.

In the real time scenario there will be multiple vehicles comes in picture each vehicle may access the RSU for various purpose. This will burdens the RSU performance which leads to the failure of the system. In order to nullify these problem its important to have an efficient cluster based VANET architecture along with a well equipped clustering algorithm [8].

(i)Clustering Overview

Clustering [9] is a technique to group nodes into several clusters. Each node in the cluster structure plays one of three roles: Cluster Head (CH), Cluster Gateway (CG), and Cluster Member (CM). A CH is a leading node of a cluster and is responsible to coordinate all CMs in its cluster. A CG is a border node of a cluster that can communicate nodes belonging to different clusters. In mobile wireless networks, clustering is a practical skill to reduce the complexity of network management. For example, CHs can allocate channel resource (time slots or frequency spectrums) to their CMs to avoid any happenings of transmission collisions and increase resource utilization within a cluster.

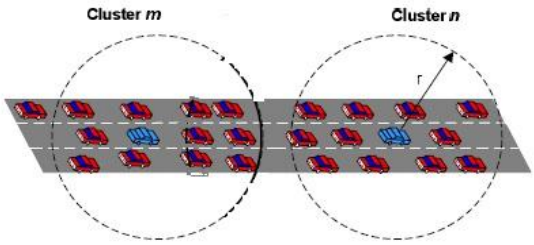

Fig3. 4: Typical Clustering Environment

Clustering has many application domains. However, developing efficient clustering techniques in mobile environments is not an easy job. Node mobility will frequently destroy existing cluster structures. Reclustering overhead becomes an important cost metric. In this work, we consider a data sharing application in a Vehicular Ad hoc Network (VANET). VANET is a specialized Mobile Ad Hoc Network (MANET) that connects vehicles and roadside facilities. The major function of VANET is to provide real-time services and

emergency warnings for drivers and passengers. VANET provides both Roadside-to-Vehicle Communication (RVC) and Inter-Vehicle Communication (IVC).

The data sharing application is motivated by a typical scenario, where a passenger in a car would like to download an interested multimedia file from neighboring cars via IVC. Here, it uses the cluster structure to facilitate the finding, uploading, and downloading of multimedia files. Vehicles that are willing to share data are grouped into clusters. In a cluster, CMs can upload their shared data and query interested data to the CH(s). CMs can also download interested data from the CH(s). To speed up data downloading, a bit-torrent downloading mechanism from multiple seed nodes (CHs) is recommended. Therefore,it is important to construct a cluster with multiple CHs. Several clustering algorithms [8] have been proposed for mobile networks. However, they have some weaknesses when applied to data sharing application. First, these algorithms do not support an arbitrary number of CHs within a cluster. Second, most of them are designed for MANET but VANET. VANET has its own unique features such as highly dynamic topology, sufficient energy and storage, and geographical environment constrains. A mobile node in MANET can move in arbitrary directions but can only move along the street in VANET. Moreover, most vehicles are equipped with GPS (Global Positioning System) devices. The location and mobility information about a vehicle is available, which facilitates the design of a more efficient clustering algorithm.

(ii) Clustering Architecture

At first, the design of single-head clustering algorithm is explained. Then, the multi-head version is introduced. Two assumptions are made: Each mobile node has a unique ID and is equipped with a GPS device.

Election Criterion: In a data sharing application, it is fairer for CMs that a CH is nearer the center of a cluster, because the hop count of a data transmission path from a CM to the CH is similar. Moreover, a CH should have stable relative mobility to its CMs for reducing CH re-election times. Based on these concepts of center position and relative mobility, measure the RPM (Relative Position and Mobility) of each mobile node as the criterion of CH election.

If a node has m entries in its neighbor table, without loss of generality, we assume that the first entry records its own mobility-related data. Three data fields (x_i , y_i , v_i) are recorded in the entry, which indicate the current location (x_i , v_i) and the current moving speed (v_i) of the recorded node. The RPM of a node is computed as the following steps:

(1) Compute the center position from these m entries in the neighbor table.
(2) Compute the relative distance to this center position.
(3) Sort these m moving speeds (scalar values) and find the median.
(4) Compute the relative speed to the median speed.
(5) Compute the RPM (between 0 and 1).

A mobile node declares itself a CH when its RPM is the smallest one in its neighbour table.

Cluster Establishment: In the cluster establishment phase, three node roles are used: UN (Undecided Node), CH, and CM. A UN is a node that is not currently belonging to any cluster. A node will play one of these three roles and may transit from one role to another role if cluster structure is changed.

- BI (Broadcast Interval): Time interval for a node to broadcast a HELLO packet.
- CI (Contention Interval): Time duration after two encounter CHs start competing to be a CH.
- CD (Contention Distance): Distance gap after two encounter CHs start competing to be a CH.
- TI (Timeout Interval): Time duration after an unreachable neighbor is removed from a neighbor table.
- UN-NUM $_i$: Number of UNs in the neighbor table of node.
- UN-BOUND: Threshold value for a node to start the CH election
- CM $_i$: Number of CMs joining to a CH node i.
- Four control packets are used in our clustering algorithm:
- HELLO: Periodically broadcast packet by each node that carries the mobility related data, RPM, node role, and CM values.
- JOIN-INVITE: Broadcast packet issued from a CH to invite any possible CMs.
- JOIN-REPLY: Broadcast packet issued from a CM to acknowledge a join invitation from a CH.
- CH-RESIGN: Broadcast packet issued from a CH when deciding to resign from a CH.

Cluster construction steps are explained below:
(1) Initialize each node to be a UN.
(2) Each node broadcasts a HELLO packet per BI.
(3) A node i starts the CH election as UN-NUM I greater than UN_BOUND. A node declares itself a CH when its RPM is the smallest one in its neighbor table. To break the tie, the smallest Rel_Dist, Rel_Speed, and ID are considered in sequence.
(4) A new CH broadcasts a JOIN-INVITE packet to its neighbors.
(5) A UN joins to a cluster when it receives a JOIN-INVITE packet from a CH that is driving with the same direction as it. This UN replies a JOIN_REPLY packet to the CH
Multi-Head Clustering: The multi-head version [10] is extended from the single-head version. We first construct clusters using the single-head algorithm. The selected CH in each cluster is called a master CH (MCH).

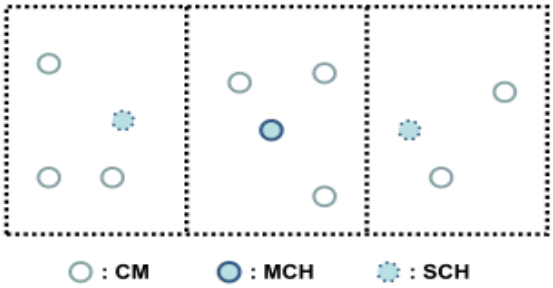

Fig 3.5: Multi-head election

We select some CMs from a cluster to be slave CHs (SCHs). Therefore, each multi-head cluster contains one MCH and several SCHs. In a vehicular environment, a cluster usually has a rectangular shape that captures a certain road segment. Having the positions of all CMs, an MCH can compute the bounded rectangle that encloses all its CMs. Then, this rectangle is divided into some sectors (with the number being specified) as the example shown in Fig. 3.6. The MCH selects one SCH that has the locally smallest RPM in each sector (except for the sector the MCH is located in).

IV. Results And Discussions

Compared Protocol

To compare the system with other security mechanisms that were proposed for service-oriented VANETs. VANETs,ABAKA protocol is used,which has recently been proposed as an authentication and key agreement scheme for VANETs. In addition to ABAKA here it is using REACT where single user scenario is been discussed. More over proposed algorithm abbreviated Cluster oriented Relative Position and Mobility (CORPM) is compared with LID, LCC, and MOBIC. The cost metrics used in the experiments are listed below:

(i) Average number of clusters: average number of clusters by averaging system observations per ten seconds.
(ii) Average number of CMs: average number of CMs in a cluster by averaging system observations per ten seconds.
(iii) Average cluster lifetime: average lifetime of a cluster.
(iv) Average idle time: average time duration for a node remaining as a UN in the system.
(v) Average resident time: average time duration for a CM to stay in the same cluster.
(vi) Message success ratio (MSR), which is the percentage of messages that are successfully received at their destinations;
(vii) Message response time (MRT), which is the total time required to send a request from a vehicle to an SP and to receive the answer;
(viii) Initialization phase time (IPT), which is the system security initialization time, i.e., the average time between the instance a vehicle starts a session to the instance it sends the first packet encrypted with a session key (or packet key)
(ix) Average overhead traffic (AOT), which is the extra traffic (mainly due to security packets and to the increase in the size of packets due to cryptographic operations) sent or received by a vehicle

MSR vs Number of Keys: In Fig 4.1 it is seen that MSR of CORPM achieves more than 85 percentage while REACT limits to 65.

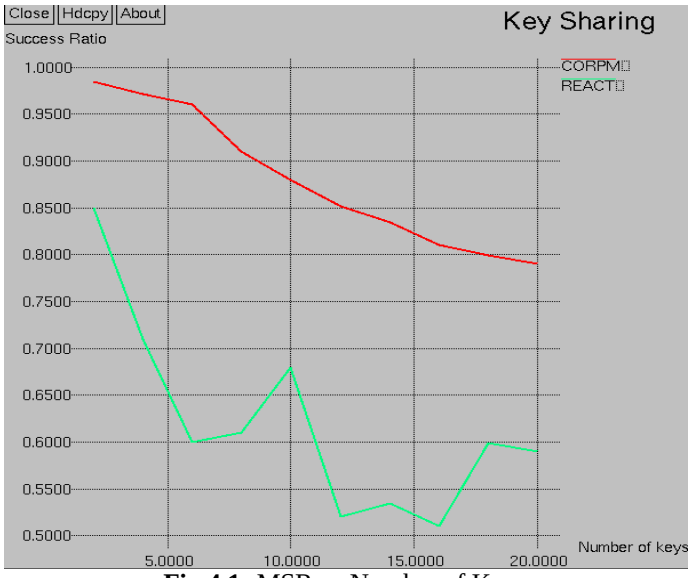

Fig 4.1: MSR vs Number of Keys

Traffic Overhead vs Moving Speed: Traffic overhead is bit too small as compared with the other system such as REACT and ABAKA. Also its clear from Fig 4.2 that both the system has similar performance responsibilities of routing.While in case of EALERT,partial function is carried out by RFs.

Request Rate Vs Message Delay: From the Fig 4.3 it is clear that as compared to the ABAKA and REACT, CORPM has much low delay problem since it has cluster based vehicular system

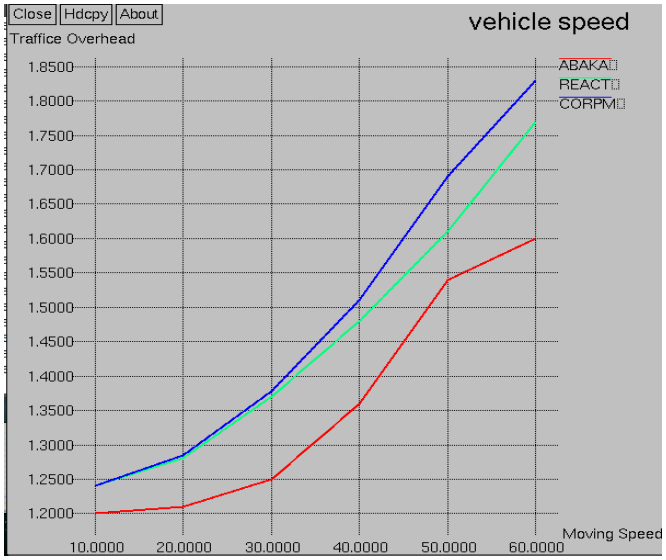

Fig 4.2 Traffic Overhead vs Moving Speed

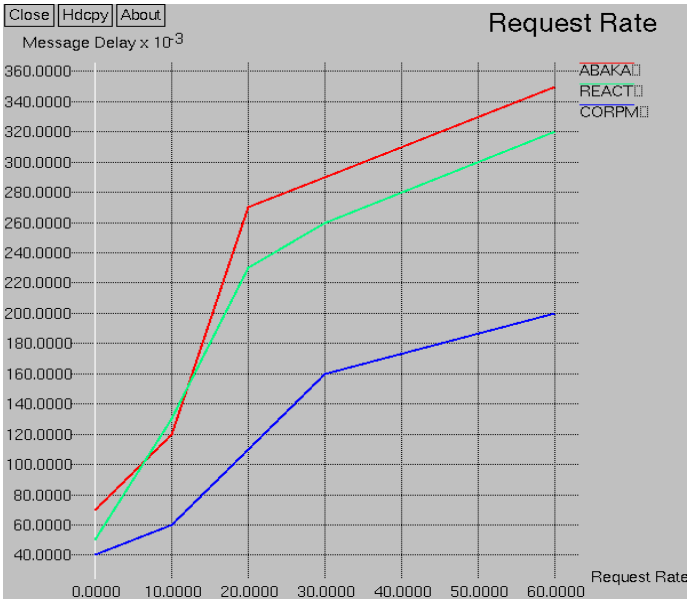

Fig 4.3 Request Rate Vs Message Delay.

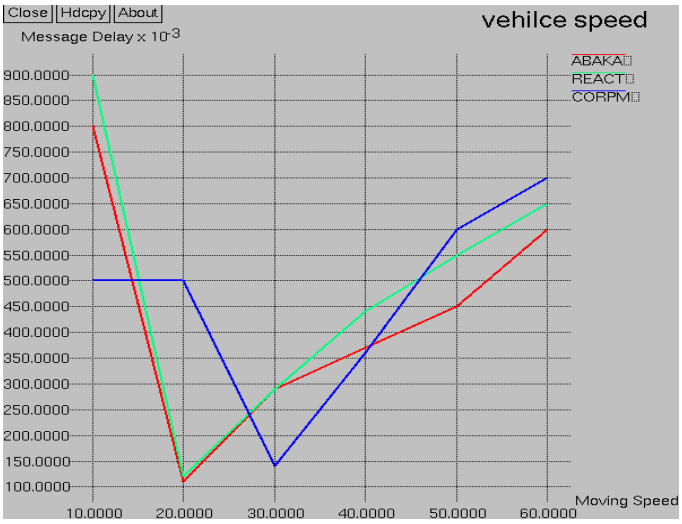

Fig 4.4: Message Delay Vs Moving speed.

Message Delay Vs Moving Speed: In the Fig 4.4 it is seen that for the average speed of vehicle (30- 40km/hr) CORPM performance is very much effective as compared with the other protocol. Moreover for the above average speed of 60 km/hr all the three system has similar

Initialization Delay vs Moving speed: As far as initialization delay is concerned the performance of CORPM is appreciated as compared with the other two system. Unlike the other compared system CORPM has negligibly small initialization delay.

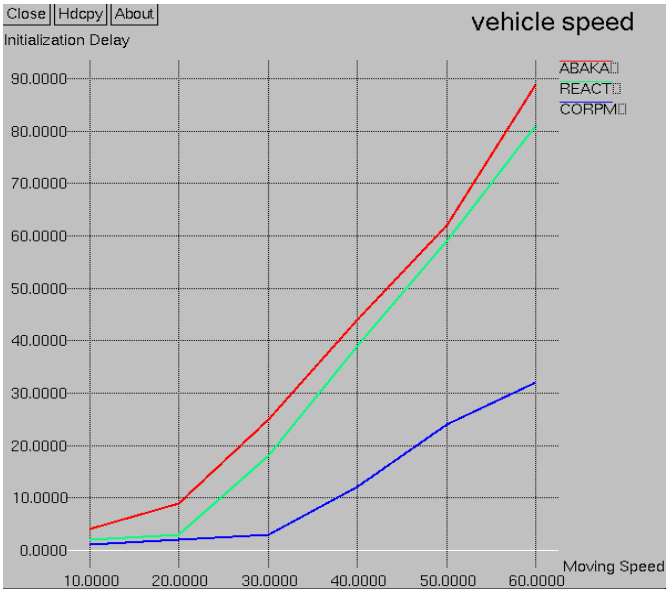

Fig4.5: Initialization delay vs Moving speed.

Initialization Delay vs Request Rate: In the Fig 4.6 as far as initialization delay is concerned against request rate the performance of CORPM is better than the other two system**.**

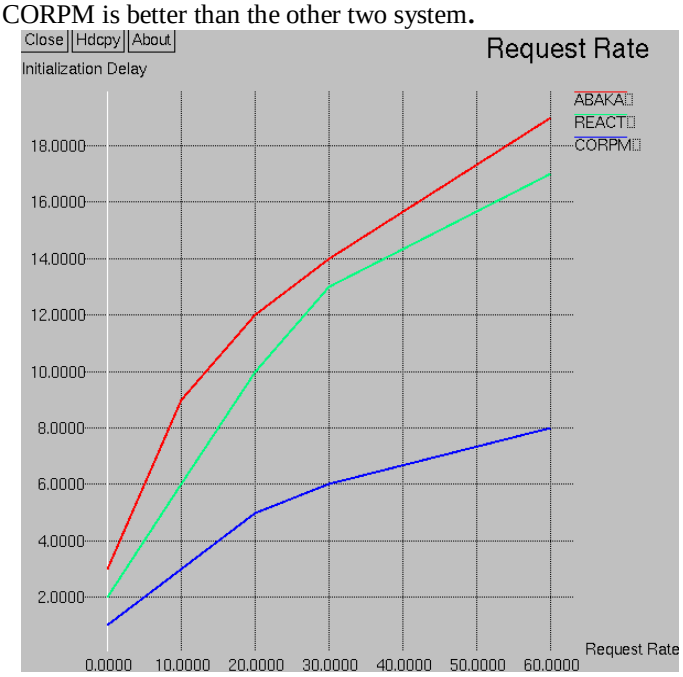

Fig 4.6: Initialization Delay vs Request Rate.

The experimental results are depicted in Figures 4.7-4.11 LCC [9] and LID [9] are ID-based clustering algorithms. They will group vehicles on both forward and reverse lanes, so their constructed clusters tend to be large and hence the average number of clusters is small. These results are more significant if larger transmission ranges are used. However, under high node mobility, these two algorithms are not stable. The average cluster lifetime is short. LCC relaxes certain criteria on reclustering as compared with LID. The cluster lifetime of LCC is a little bit higher than that of LID. Since the CH election is simple for ID-based approaches, a UN can easily join to a surrounding cluster. Therefore, the average idle time is short. However, the cluster is not stable and tends to be reconstructed. A CM frequently joins to a different cluster, so the average resident time is short. This

reduces the opportunity of a CM to successfully download data from CHs.These ID-based clustering algorithms are not suitable for data sharing application in vehicular environments

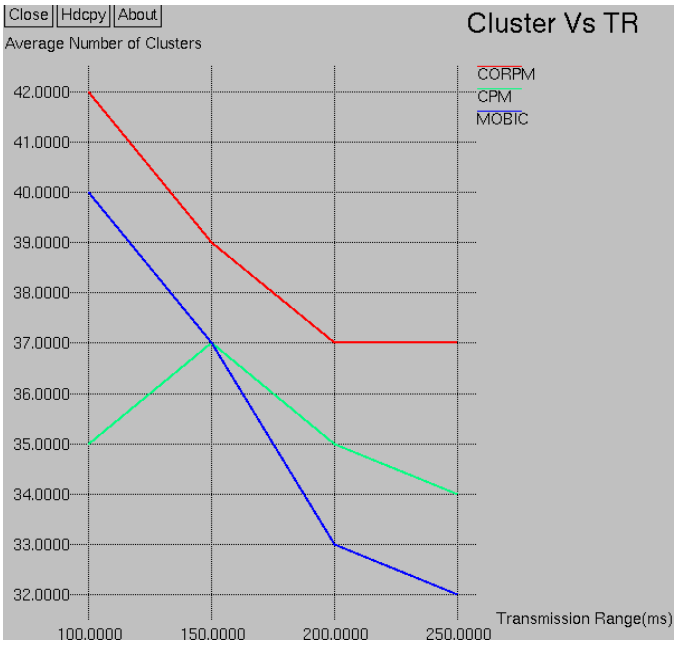

Fig 4.7 Average Number of Clusters vs. TR.

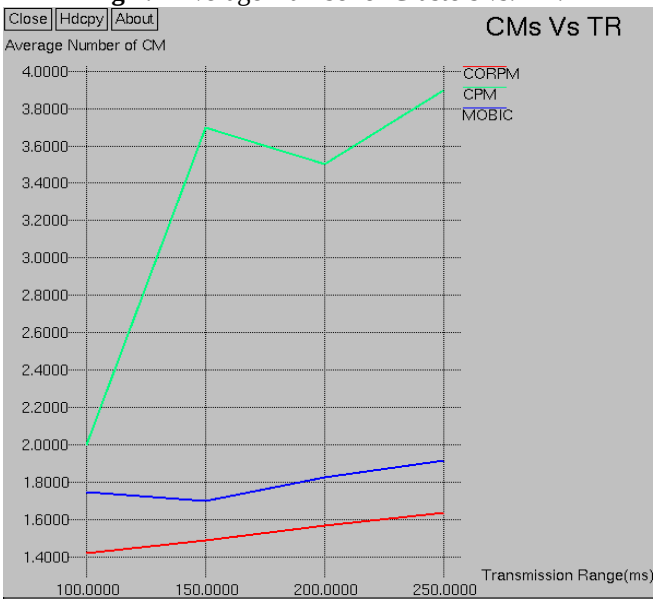

Fig 4.8: Average Number of CMs vs. TR.

Next, compare the performances of MOBIC and CORPM. MOBIC is a mobility-based clustering algorithm while CPM is a multiple-metrics-based one. As seen in the Figures, MOBIC generates smaller clusters than CORPM. Also, vehicles on forward and reverse lanes are not separated in MOBIC, so its cluster lifetime is shorter than CORPM.

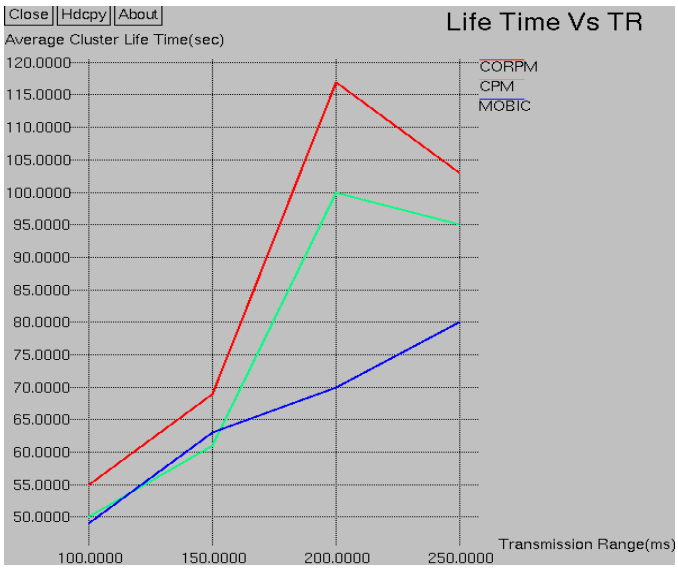

Fig 4.9: Average Cluster Lifetime vs. TR

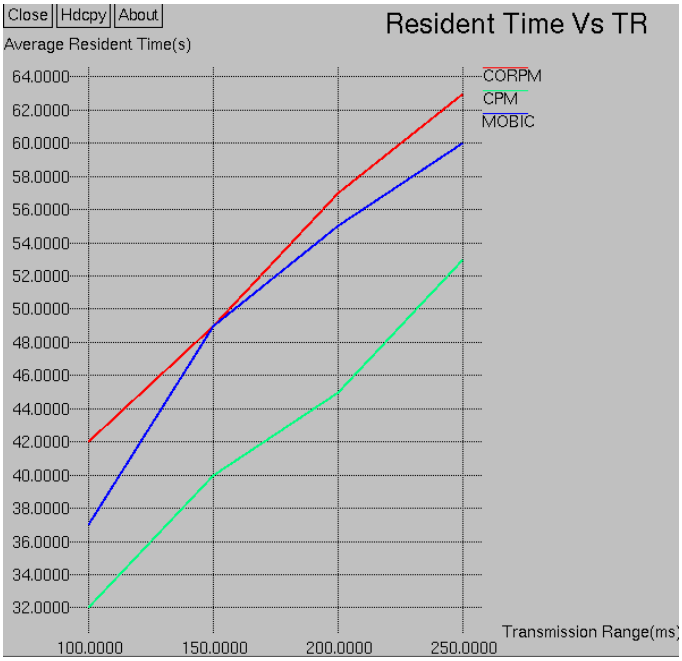

Fig 4.10: Average Resident Time vs. TR

Those vehicles that occasionally join to a CH with a different moving direction as them will frequently become UNs as the CH is leaving. Moreover, the CH election in MOBIC takes the most time among all. To compute the relative mobility of one node against the other node, two successive HELLO packets are required. Therefore, the average idle time in MOBIC is long. However, those vehicles that drive the same direction with the CH will keep joining the same cluster, so the average resident time of MOBIC is long. MOBIC is still not suitable for data sharing application, because small-size clusters and long-idle periods prevent the searching of a veriety of shared data. Compared with other algorithms, CPM provides stable clusters with long lifetime. Moreover, the short idle time and the long resident time qualify CPM for a good clustering algorithm in data sharing. The idle time of CORPM is higher than LID and LCC, because it disallow any clusters with size 1. There may have single UN in our system and these single UNs are useless to data sharing.

V. Conclusion

To ensure security and privacy in service-oriented VANETs represents a challenging issue.These issues are overcome by the proposed privacy-preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption. The evaluation of the proposed scheme confirmed its effectiveness compared to a recent security mechanism. Moreover introduced the importance of clustering to network and application designs. In this work,it considers a data sharing application in a vehicular environment. Vehicles nearby are grouped into a cluster in which some nodes are selected as cluster heads. These cluster heads serve as local file servers that enable surrounding nodes to upload and download shared data.Here proposes a multi-head clustering algorithm.The unique feature in vehicular environments that vehicles drive along the street either with the same or opposite driving direction. The experimental results reveal that the proposed algorithm generates stable clusters with long lifetime. In future it is expected to extend the single headed approach to the multi cluster head approach where first construct clusters using the single-head algorithm. The selected CH in each cluster is called a master CH (MCH). Then, select some CMs from a cluster to be slave CHs (SCHs). Therefore, each multi-head cluster contains one MCH and several SCHs. This kind of architecture can provide much more throughput than the other.

References

[1]. Khaleel Mershad and Hassan Artail"'A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks"' Vehicular Technology,Vol. 62, No. 2, Feb 2013.
[2]. J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J. P. Hubaux, "Mix zones for location privacy in vehicular networks," presented at the Int. Workshop Wireless Netw. Intell. Transp. Syst., Vancouver, BC, Canada, Aug. 2007 LCA-CONF-2007-016
[3]. 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.
[4]. C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Data aggregation and roadside unit placement for a VANET traffic information system," in Proc. 5th ACM Int. Workshop VANET, San Francisco, CA, Sep. 2008, pp. 58–65.
[5]. M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in Proc. SASN, Alexandria, VA, Nov. 2005, pp. 11–21.
[6]. 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.
[7]. "Brute-force attack," Wikipedia. [Online]. Available: http://en.wikipedia. org/wiki/Brute-force_attack
[8]. Shou-Chih Lo, Yi-Jen Lin, and Jhih-Siao Gao "A Multi-Head Clustering Algorithm in Vehicular Ad Hoc Networks" Vol. 5, No. 2, April 2013