Key Management of Vehicular Ad-Hoc Network with Eliminating Scheme

S. Suganya[1]
II M.E. Department of Computer Science & Engineering,
St.Peter's College of Engineering & Technology,
Chennai, 600054, India

C. Shanmuganathan[2],
Assistant Professor, Department of Computer Science & Engineering,
St.Peter's College of Engineering & Technology,
Chennai, 600054, India

***Abstract* - In Vehicular Ad-hoc Network is mainly for the safety of the road users, which also improves the wireless applications for all road users. RFID tags are used in VANET which improves the vehicle to vehicle communication. It is also used for identification purpose, reduces the power and the cost of the network. Key management is used for improving the security of the VANET. Clustering is used for generating Digital Certificates (DC) with the help of Internet of Things (IoT) and evaluating the truthiness of the Certificate. Symmetric key management scheme is used in most of the VANET. In this paper we propose an Elimination scheme along with key management of RFID tags, that avoid malicious or suspected nodes due to which a trustiness group can be formed and the security and privacy of the network can be increased. It also helps in better and faster communication between vehicles. Certificate revocation scheme is used for maintaining the revocation list. Effective K-Means Authentication-2 (EKA2) and K-means clustering is used respectively for revocation and clustering of certificates**.

Keywords* *– VANET, RFID, Elimination scheme and IoT.

I. INTRODUCTION

Vehicular Ad-hoc Network is used for increasing vehicle to vehicle communication. VANET improves the safety of the road users by broadcasting emergency messages. Radio frequency identification tags (RFID) is used in VANET for tracking (identification) of the vehicle and message broadcasting with the help of INTERNET of THINGS (IoT). Road side unit (RSUs) are used; The Road side administrator monitors the messages broadcasted. Security and privacy are maintained by using authentication scheme, symmetric key management scheme. Clustering concept is used for generating digital certificates. Certificate revocation scheme called EKA2 (Effective k-Means Authentication-2). Eliminating scheme is used to avoid malicious and suspected nodes for enhancing security.

A. Vehicular Ad-Hoc Network

A vehicular ad-hoc network (VANET) uses vehicles as mobile nodes in a Mobile Ad-hoc Network (MANET) to create a mobile ad hoc network. In the VANET every vehicle acts as a wireless router or node. Vehicles of range 100 metres to 300 metres can connect with each other to create a wireless or mobile network. As vehicles fall out of the signal range they drop out of the network, vehicle that enters a network can join the network by registering their details. Connection of vehicles to one another leads to the formation or creation of a mobile internet. This system was mainly developed for police and fire vehicle for communicating with each other so that they can work fast and in a different way. Few Automotive companies that provide these terms are Toyota, Nissan, BMW and Ford, etc.

Automotive vehicular information can be viewed on electronic maps using the Internet or with the help of some specialized softwares. We can locate a vehicle which is inside big campuses such as universities, airports, tunnel , etc this is the main feature, function or advantage of Wi-Fi based navigation system .we can used VANET as part of automotive electronics, which helps in identifying the optimal minimal path for navigation with minimal traffic intensity (less traffic). It is also been used as a city guide to locate and identify landmarks in a new city.

Communication capabilities in vehicles are the basis of an envisioned in VANET. Vehicles are enabled to communicate among them and via roadside access points also called as Road Side Units (RSUs). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely and important information to drivers, police, and to make travel more convenient, simple, easy and secure.

B. Radio Frequency Identification

Radio-frequency identification (RFID) is uses a small radio frequency which uses an electromagnetic field that is used for identification and tracking and for transferring data. An RFID tagging system includes the tag a read/write device and a memory or data collection where data about the device and the user will be saved. Processing and transmission can also be done with these tags. RFID contains its own power source or it consumes a very less power to operate. RFID systems usually contain three part they are Tag – a microchip that can send and receive data (messages), Verifier the data received – interfacing with the Tag, the Verifier can read the data, write the data and sends messages to access the Tags data and Database – a small amount of memory that used as a database, the data in the database can be changed. The information is stored electrically. Some tags are powered by and read at short ranges. Others Tags use a local power source like battery else have no battery but collect energy from the interrogating EM field (electromagnetic), and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at 100 of meters or in a short range. The tag does not necessarily need to be within line of sight of the reader like bar code reader and bar code, but the tag may be embedded in the tracked object.

Radio frequency identification (RFID) is part of the family of Automatic Identification and Data Capture (AIDC) technologies that includes 1D bar codes and 2D bar codes. RFID uses an electronic chip that is applied to a substrate to form a label that can be affixed or attached to a product, device, animals or other packages. The information that the tag contains may be read, recorded, or rewritten it depends on the type of tag.

RFID tags are used in many industries that to mainly in automobile manufacturing industry. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line, etc.

C. *Internet of Things*

The Internet of Things (IoT) it is also Cloud of Things or CoT refers to the interconnection of uniquely identifiable embedded computing like devices within the existing Internet structure. Typically, IoT is may offer advanced connection of devices, systems, and new services that are beyond machine-to-machine communications (M2M) and covers many different protocols, domains, and applications that don’t match each other. The connection of these embedded devices (including smart objects) is expected to be used in automation and all other fields, which also enable advanced Smart Grid applications.

Things, in the IoT, can refer to a wide variety of devices such as heart monitoring device, biochip on farm animals, automobiles with built-in sensors for message sharing, or field operation devices that assist fire-fighters. Current market examples include smart thermostat systems such as Heat Genius and washer or dryers that utilize Wi-Fi for remote monitoring.

II. LITERATURE REVIEW

A. *Safety Message Broadcasting*

Vehicular Ad-Hoc Networks which is used for Safety messages broadcast by mobile users periodically. Protocol sequences are used. Protocol sequences are deterministic 0 –1 sequences. Each user reads out the 0’s and 1’s of the assigned protocol sequence periodically and transmits a packet in a time slot if and only if the sequence value is equal to 1. ALOHA-type random access scheme is used to reduce the delay. Safety messages can be divided into two types. The first type is periodic information also called heartbeat messages, Such as the speed and location of an automobile. The second type of messages relates to emergency events such as lane-change warning or pre-crash warning. These are the safety messages broadcasted. The Drawback of this paper is there are no base stations which many lead to delay in broadcasting the safety message. Collision may occur if two or more transmit packet in a same time slot since we use protocol sequence which allow only one vehicle to send message in a time slot [1].

B. *RFID Tags*

Radio Frequency Identification tags are used in e-Health. RFID in health care are mainly for efficient and constant health monitoring system. RFID is fitted in patient’s body, which are either wearable or implantable. Wearable like watch, bracelet etc. With the help of RFID tags we can forms Body Area Networks (BANs) or Body Sensor Networks (BSNs). This RFID tags helps in monitoring the blood pressure, blood sugar and heart rate of the patients. This RFID tags plays a main role in emergency situations where a sudden change in a person's vital statistics might require immediate medical attention and instant communication to the hospital. Even the details of the patients are stored in Electronic Patient Record (EPR) or Patient Information Record (PIR) [2].

C. *VANET Formation*

In Vehicles sensors are present that monitor the velocity, fuel level, weather etc of the vehicle. Road side unit is used for message sharing or for broadcasting some emergency messages like warning about the road traffic, informing about the accident to the police, hospital in need of some emergency help, even pre-crash warning are broadcasted to all the vehicles using this road side unit. In VANET the network, clustering and group formation is very difficult process since it has high mobility. Even if the group are formed maintain the group for a longer time will not be possible since the vehicles keep on moving. Frequent radio obstacles and complete multi-hop path between the source and the destination is used to transfer the packets or messages from source to destination. Map-based sensor-data delivery protocol (MSDP) is also used to combine information and map the nodes to improve data delivery. The drawbacks of this paper are it becomes very difficult to combine the information gather from different vehicles since the vehicles move in different direction and in different speed. Due to high mobility in VANET high delay may occur during heavy traffic even message drop take place. Since dropping of message are not identified we are not able to resending or retransmission the messages [3].

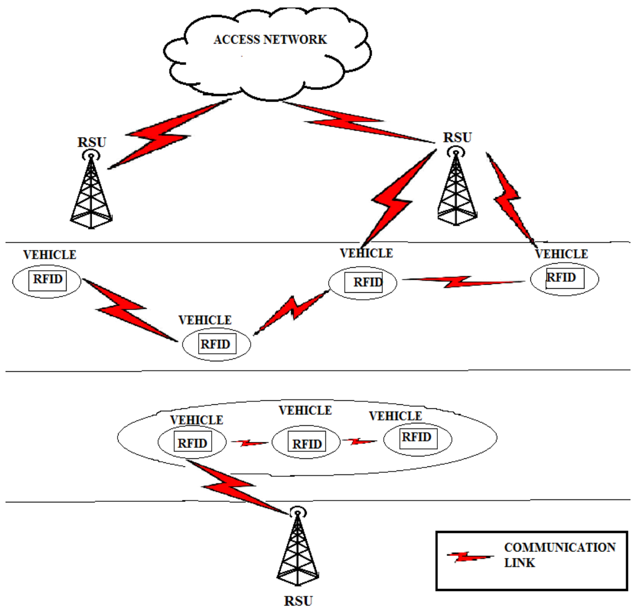


Figure 1: Communication in VANET with RFID tags

III. CLUSTERING

Clustering or group formation is a process in which the network is sub divided in two small groups called clusters. Clustering helps is solving the key management and routing problem in Mobile Ad-Hoc Networks (MANET). Each cluster has a group leader who coordinates the group .the leader is also called as the central server.

The leader acts as a base station with in a group and communicate with other group. The nodes are divided in two groups so that the node comes in some group and the group does not overlap each other. Some nodes are selected as group leader for the key management and other functions. When the nodes move the topology of the network keeps on changing and the nodes which go out of one cluster gets connected to the other.

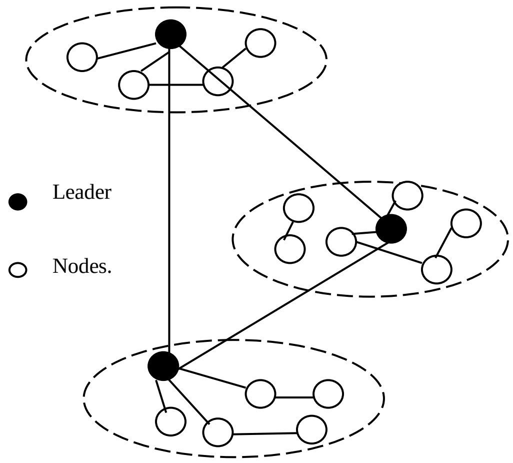


Figure 2: Sample of Cluster Group Communication.

Grouping also helps in reducing the number of keys required in a network. when the node keeps on moving and if it losses it connection with the group leader then it send a request to any group leader whose signal is very close to it, so that it can join in that group [4].

IV BROADCASTING

Broadcasting is the process of sending data to all the nodes within a range or within a limited area. We can even broadcast for a cluster or a group. Broadcasting is mainly used for sending the keys to all the nodes in a group and in a cluster. The broadcasting is done by the cluster head to the cluster and by the group leader to all the group members (nodes). When a node enters a group or a cluster newly den it has to send request for the key, once the request is received then the node will be checked for its trustiness if it is trustable then the key will be sent to that node alone. The next time when the key is changes (rekeying) then the key will be sent to all the nodes even to the new node that has entered the group. The broadcast of the key takes place after certain time interval or sometimes based on the number of data sent. The data or the key that are broadcasted will be saved in the database [1].

V KEY MANAGEMENT

Authentication is mainly for secure communication, it is the process of just checking the sender is a trusted one or not and to check the trustiness of the message received (i.e.) to see if the messages are changed by others outside the network or the group. The messages that are sent can be encrypted with the help of keys; the keys can be symmetric or asymmetric. In symmetric method only one key is used for both encryption and decryption. In asymmetric method there are two different keys are used for encrypted and decryption. Public key cryptography system or public key infrastructure is a set of software, hardware, etc which helps to create, manage he digital certificate. PKI binds public key with the respective user id with the help of certificate authority (CA). We can also use the third party or software to provide the details instead of the CA. Key management systems are susceptible to security attacks as they work contactless, an attacker can work remote and passive attacks will not be noticed. These security risks have to be dealt with in order to gain a broad user acceptance [10].

The different key protocols are centralized group key distribution (CGKD), de-centralized group key management (DGKM) and distributed group key distribution (DGKD). In CGKD there is a central entity controller, this is responsible for key distribution and key managing , updating etc. the main scheme in this is the tree based key where the keys placed in a hierarchical manner this placement is also called Logical Key Hierarchy (LKH). In this tree based structure the user are placed in the leaf node and the leader is in the root node. This method reduces the number of message broadcasted and the storage space. The leaf node and the root node have a set of keys. The function is a one way function.

VI K-MEANS AUTHENTICATION

A. *Digital Certificate*

A digital certificate helps in exchanging information with different computer or organization with the help of Internet using the Public Key Infrastructure (PKI). A digital certificate may also be referred to as a public key certificate. In Public Key Infrastructure (PKI) scheme, the signature will be of a Certificate Authority (CA). Each digital certificate has a certificate ID called digital ID. Certificate is generated or created with the help of keys. We may use a single key to encrypt and decrypt the message or we can use one key to encrypt and another key to decrypt.

B. *Certificate Revocation*

CR is a method to revoke the certificates that have expired in date or the certificates of the problematic vehicles so that problems can be avoided. There are two different states in revocation they are: Revoked and Hold. Certificate revocation is done with the help of Certificate Revocation List (CRL), Distributed Revocation Protocol (DRP) and Certificate Revocation Tree (CRT). An alternate to CRLs is online certificate status protocol (OCSP) that has many benefits like less bandwidth etc. CRL consist of CRL table which has the following field’s serial number, revocation date, issued date, credibility.

C. *Credibility Value*

Credibility refers to the trustiness of the message or the source from with the message has been sent. Certificates may be divided into different levels based on the trustiness, acceptance or the rejection of the certificate. Credibility value is a numerical values, the scale may range from 0 to 100. We can set any value as minimum and any value as maximum. The vehicle with credibility value less than the minimum will be considered as malicious or suspected node. The value is set based on the behaviour of the vehicle in the environment (Road).

D. *K-Means Clustering*

K-means clustering is mainly used because it is very simple and efficient one. In this clustering we can partition the clusters in to any number of n, discrete clusters c. The clusters contain data points. Each clusters have centroids, it is selected at random for the first time from the next time it is selected by

$$L=\sum_{j=1}^{k}\sum_{i=1}^{n}||X_i-\mu_j||^2$$

Where X_i is a vector, X_{i-}th data point, μ_j is the centroid of data points in C_j and L is the distance for each data points to the centroids [4].

VII RFID AUTHENTICATION

RFID Authentication has an important role in many applications for providing security and privacy. RFID tags reducing the cost of manufacturing, Optimizing data networks for storing and delivering larger amounts of data and Developing open standards [9].

A. *Location Tracking*

RFID tags also play a major role in tracking the location of the vehicle. The location can be found when the vehicle communicates with the RSU or when the vehicle broadcast the message. This helps in finding the lost vehicle and the vehicle which had lost the direction [11].

B. *Communication*

Communication is done by broadcasting in-order to start broadcasting we need to form groups first after that only we can broadcast the message to that group. Grouping is done by using clustering methods. Clustering may involve both similar and dissimilar nodes; it may be done based on certain conditions or certain patters. When a node leaves a cluster it may join another one. The messages for each cluster are broadcasted with the help of Road Side Unit (RSU). Each cluster has a maximum and a minimum limit for the number of nodes. If the count crossed the maximum limit then a new cluster will be formed by dividing the cluster that has the maximum nodes. K-means clustering algorithm will be used to form clusters. Each cluster has communication with one another.

C. Security

RFID systems are susceptible to security attacks as they work contactless, an attacker can work remote and passive attacks will not be noticed. Some of the main concerns are (unwanted) vehicle tracking, tag forgery and the unauthorized access to the tag's memory content. These security risks have to be dealt with in order to gain a broad user acceptance [7], [8].

VIII IMPLEMENTATION

A. Simulation of VANET

Since wireless technology and the protocols used are very complex and costly they can't be tested in a reality. In order to overcome this problem we are using network simulation-2 software (ns2). With the help of this simulation software we can find out the problems in design, we can find out the capacity, few new ideas and different approaches. For VANET design we need two components they are Network and mobility. Traffic flow simulator generates required realistic vehicular mobility traces to be used in network simulator as an input.

In VANET mobility generators are of two main types they are microscopic and macroscopic. The Macroscopic focus mainly on mobility of flow of vehicles and not all the individual vehicle. In this the generations of vehicular traffic such as traffic density or traffic flows are defined. In the other types of the mobility models, microscopic approach, the movement of each individual vehicle and the vehicle behaviour is important. In macroscopic, parameters for the mobility generator can be the roads map, scenario of vehicle travelling and some road and vehicle parameters like maximum vehicle speed, roads limitation, arrivals and departures times of each vehicle's.

Network simulator is usually used for simulation the computer networks. They are used for simulating the VANETs by evaluating the performance of network protocols for mobility of nodes and other required technique. Most currently used network simulators are developed for MANETs and hence require VANET extensions. Scenarios in SUMO simulator consist of two parts: Road Network (maps) including roads, streets, traffic light, junctions etc. Traffic demand which mean details of the vehicle. SUMO's road network can generate by an application named: "VANET gen" that provided with SUMO package, or generate by importing a digital road map.

The shortest path through the road network is calculated using the Dijkstra algorithm. When a vehicle arrives to its destination, it shuts down all interfaces and is removed from the map. We consider that this behaviour is a better approximation to real mobility than other proposed mobility models in which vehicle never stop, following infinite routes. We want to remark that the duration of the routes is unpredictable, and removing a vehicle means that all the packets contained in its buffer will be lost. In a real situation packets could be reintroduced in the network when the node starts a new route, but only under the assumption that the maximum delay is lower than the average stop time; we can also assume that all the packets contained in the buffer when a node stops will never arrive[3] , [5].

B. RSU Placement

RSUs are located by an entity whose objective is to collect as much traffic information as possible. According with this assumption, we placed the RSUs on the avenues of our network with a bigger volume of road traffic every node in our network scenario generates a message with a size of 2500 Bytes every 5 seconds. The size of the fragments is 231 Bytes plus headers, making a total size of 256 Bytes. The traffic generation will be stopped after the first 100 seconds of our simulation. The simulation will last 3600 seconds.

IX EXPERIMENTAL RESULT

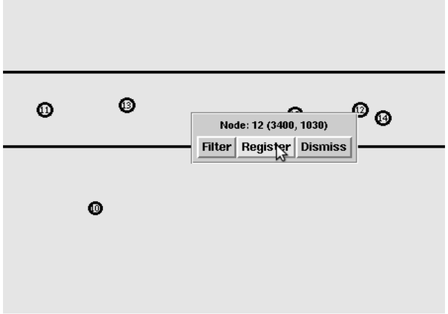
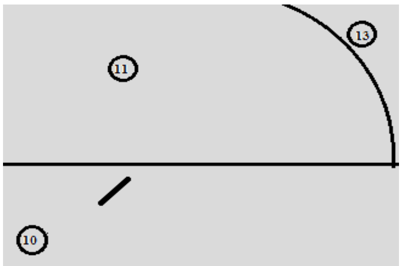


Figure 3: Registering of the nodes (vehicle)



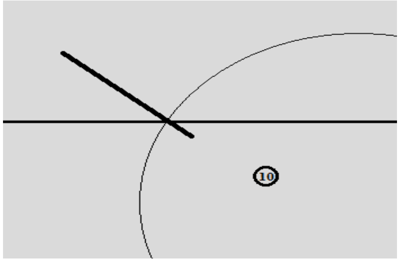


Figure 4: sending request and receiving response from RSU.

A. *Performance Evaluation*

The performance is much better when compared to others which use EKA algorithm since we use EKA2 algorithm which is an enhanced one of EKA. The time taken to send request and response for the authentication is also very less. The response time taken for a dynamic network (network which keep on changing) is very less when we compare with liner and EKA1 algorithm. We can also support large number of nodes and clusters. This also makes the search more efficient and faster one when compared to all other algorithm.

X CONCLUSION

In this paper, EKA2 is used which is reliable, secure and certificate authentication is used over RFID tags in Vehicular Ad-hoc Network so that the trustiness of the vehicle can be know to all others in the network. In terms of future work, we can develop this in offline by using cryptographic scheme for certain nodes that communicate in a short range with in a RSU. We can also bring automatic registration and certificate revocation scheme with the help of the details in RFID tags like name, certificate number, vehicle number, credibility value etc. This automatic registration and revocation scheme will be an efficient one; it may also reduce the work of users. We can also implement automatic elimination scheme along manual eliminating scheme which eliminated the unwanted or suspected nodes based on certain condition or criteria this also reduces the work load and increases the security of the VANET.

REFERENCES

[1] Yi Wu, Kenneth W. Shum, wing Shing Wong and Lianfeng Shen.m "Safety- Message Broadcast in Vehicular Ad-Hoc Networks Based on Protocol Sequences," Vehicular Technology, Vol. 63, No. 3, March 2014.

[2] X. Liang, M. Barua, R. Lu, X. Lin, And X. S. Shen, "Health share: Achieving Secure and Privacy-preserving Health Information Sharing through Health Social Networks," Computer Communications, 2012.

[3] sergio Martinez Tornell, Carlos T. Calafate, Juan-carlos Cano and Y Pietro Manzoni," A Road Topology Aware Protocol for Vehicular Networks" Feb. 2011.

[4] M. Almulla, Q. Zhang, A. Boukerche, And Y. Ren, "An Efficient K-means Authentication Scheme For Digital Certificates Revocation Validation In Vehicular Ad Hoc Networks," Wireless Communications And Mobile Computing, Pp. N/A– N/A, 2012.

[5] Hamed Noori ," Realistic Urban Traffic Simulation As Vehicular Ad-hoc Network (VANET) Via Veins Frame work," tampere University Of Technology Finland, Volume: 01 Publication Year: 2013.

[6] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, CCS '02, (New York, NY, USA), pp. 41–47, ACM, 2002.

[7] Daojing He, Chun Chen, Sammy Chan and Jiajun Bu," Analysis and Improvement of a Secure and Efficient Handover Authentication for Wireless Networks "IEEE COMMUNICATIONS LETTERS, VOL. 16, NO.8, AUGUST 2012

[8] Kamal Kumar Chauhan and Amit Kumar Singh Sanger, "Securing Mobile Ad hoc Networks: Key Management and Routing" International Journal on Ad-Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[9] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, "Strong Authentication for RFID Systems using the AES Algorithm".

[10] Mohammed ERRITALI , Oussama Mohamed Redal, Bouabid E Ouahidi, "A Beaconing Approach With Key Exchange In Vehicular Ad Hoc Networks" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6, November 2012.

[11] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks".