Review on Privacy Preserving in VANET

Bhagyashree Vaze[1], Miss Ranjana Shende[2], Mrs.Vaishali Sahare[3]

[1]M.Tech Student,[2,3] Assistant Professor,
Department of Computer Science Engineering,
G.H.Raisoni Institute of Engineering and Technology,Nagpur, India.

Abstract--*Due to increase in traffic it is very necessary to enhance the efficiency and safety of road traffic. Vehicular ad-hoc networks which are created by applying the principles of mobile ad hoc networks (MANETs),whichallow vehicles to broadcast ad hoc messages to other vehicles and remind drivers to slow down their speed to avoid accidents or to change their routes. For securing vehicular networks, an authentication scheme is very important to ensure that messages are sent by authorized vehicles and not corrupted during transmissions.. An attacker can easily disrupt the function of VANETs by sending fake messages to gain unfair advantage on the road or to cause serious accidents. Hence the sender vehicles should be authenticated by the receiver before taking any action based on the received safety message. Also there is a need to encrypt these messages. When it is about the security of the very important persons like the Prime minister, scientists, army Personals and many more travelling on road. Their safety is of utmost importance. Most of the previously proposed schemes cannot support privacy preservation between roadside units (RSUs) and vehicles. In this paper generation of token by a base station which is a Trusted Authority, is proposed for short communication .This trusted authority provides unique ids to special groups and registers the vehicles. for short communications it provides a temporary token to a nearest user and discards the generated token after the communication.*

Keywords—Navigation, secure vehicular ad hoc network, Trusted Authority , token generation, encryption

I-INTRODUCTION

The vehicular ad-hoc network (VANET) is a type of wireless ad-hoc network. This concept is based on continuously moving vehicles with varying vehicular motion . These moving vehicles act as nodes. It is an active research area now a days and emerging as a type of network aimed at improving traffic optimization, safe driving and some other services through Vehicle to Vehicle communication –V2V or Vehicle to Infrastructure communication - V2I. It plays a vital role in intelligent transportation systems (ITS). Communication in each vehicle is carried out by sending and receiving messages through the On Board Unit (OBU) and are well equipped with GPS,Event Data Recorders, Trusted components etc. The Roadside Units (RSU) broadcast safety messages periodically. The development of Wireless communications protocols and the automobile industry's desire to increase in road safety and also gain competitive edge in the global market ,Vehicles are equipped with GPS, latest communication hardwares etc. hence becoming Computer networks on Wheels. As wireless communication is susceptible to various attacks, the security of VANET is very important. Some vehicle may send false information into the network intentionally to gain unfair advantage to get some confidential information or to cause serious accidents. Hence the receiver needs to authenticate sender vehicles before taking any action based on the received safety message. Hence generation of token is proposed for short communication . In VANET, a Trusted Authority -TA registers the vehicles and allots unique ids . RSUs are fixed infrastructures along the road, which periodically broadcast safety related information. Typically RSUs are placed over every 300m to 1 km for broadcasting at the interval of every 300ms. Hence placing RSUs along a long distance is not feasible economically. Hence to authenticate others with help from TA or a Base station is needed. We need to protect the privacy as well.

II-LITERATURE REVIEW

T.W. Chim, S.M. Yiu, Lucas C.K. Hui,[1] presented a scheme utilizing the real time road information collected bya vehicular ad hoc network (VANET) guides the driver to reach their destinations distributed manner and in real-time.A navigation scheme that utilizes the realtime road information collected by a VANET-vehicular ad hoc network to guide the drivers to their destinations in distributed manner and in real-time . In this paper the privacy is achieved by the idea of anonymous credential to achieve this goal. Chen Lyu, DawuGu, YunzeZeng, PrasantMohapatra,[2] proposed Prediction-based Authentication (PBA) scheme to defend against computation-based DoS attacks which is an efficient broadcast authentication scheme, and prevent packet losses caused due to high mobility of vehicles. This scheme uses symmetric cryptography which makes it an efficient lightweight scheme . The memory-based Denial of Service attacks are prevented using shortened re-keyed Message Authentication Codes of signatures.Chun-I Fan, Wei-Zhe Sun and Shih-Wei Huang proposed a scheme in [3] which allows arbitrary vehicles to broadcast ad hoc messages to other vehicles notifying them about accidents.So that the drivers can change their routes immediately and slow down the speed of the vehicles.A strong and secure protocol using the blind signature technique which ensures privacy with other essential security requirements is suggested. Xiaodong Lin, Pin-Han HoandXuemin (Sherman) Shen [4] presented an efficient verification scheme using batch signature for communication between RSUs and vehicles which can reduce total verification time where RSUs verify multiple received signatures. Conditional privacy is preserved by mapping every message to a distinct pseudo identity. Xiaodong Lin et al.proposed in [5][6] delay and eliminating redundant authentication efforts by different vehicles on same message. An an efficient cooperative scheme which reduces authentication overhead on vehicles by shortening the authentication evidence token approach is used to control the authentication workload without directly involving a trusted authority and resist various attacks.In [7] RajkumarWaghmode et al. suggested a group based vehicle to vehicle communication scheme which prevents the vehicles from threat. One time authentication for communication and use of group symmetric key for vehicle to vehicle communication is proposed to achieve privacy and security is proposed. Malicious vehicles can be traced which generate a false message.In VANETs, to avoid accidents vehicles communicate with the road side units i.e. RSUs and with each other. To exchange information vehicles in VANET need a routing protocol. Position based routing protocols are more effective as they support geographical position of vehicles. Here they present different effective position based routing based protocols [8].In VANET security is a major issue as it provides safety and non-safety applications. But messaging between the vehicles is still considered as a big issue. In [9] Rajeev Singh and SumitMiglani proposed a model in which RSUs act as a certifying authority which generate the key by using ECC i.e. Elliptic Curve Cryptography for vehicles after which communication between vehicles is carried out by ECDH i.e Elliptic curve DiffieHellman.VANETprovide security to the vehicles by sending different types of warning messages to avoid accidents.But these messages would be attacked and interrupted to change the contents of the message.In [10] AditiSelokar and VaishaliSahare discussed various types of attacks in VANET and its prevention techniques.Sok-Ian Sou proposed an analytical model for evaluation of performance in sending emergency messages through wireless collision avoidance systems in [11]. Different models are used to generate traces of vehicular mobility for analysing them and derived the probability of a rear-end collision between two vehicles.VaishaliKatkar and YogitaRaut [12] suggested the use of RSUs to assist the traffic safety messaging which deliver safety messages alert earlier to vehicles using relative positions. These aiert messages are multicasted to the vehicles which are affected by any event. This is done with lower delay, few hop counts and higher reliability which can improve the VANET connectivity.Brijesh Kumar Chaurasia ,ShekharVerma , S. M. Bhasker [13] studied the various group signature schemes for the verification of their overheads and effectiveness. They proposed a scheme which combines pseudonyms and group signature schemes enhancing the efficiency and the effectiveness of group signatures.Ren-Junn Hwang, Yu-Kai Hsiao and Yen-Fu Liu [14]proposed an Identity based Encryption scheme which provides privacy preservation , confidentiality , anonymity based on efficient pseudonym based mechanism for VANET communications. For ensuring the secure exchange of messages trustworthy and protect user privacy are important issues.

The existing technologies are using different protocols and perform encryption to preserve the privacy during communication. But in case we want to provide privacy preserving to some very important persons their communication with anyone while travelling also needs to be encrypted. Therefore to meet the requirement there should be temporary communication between the commuters and the drivers.

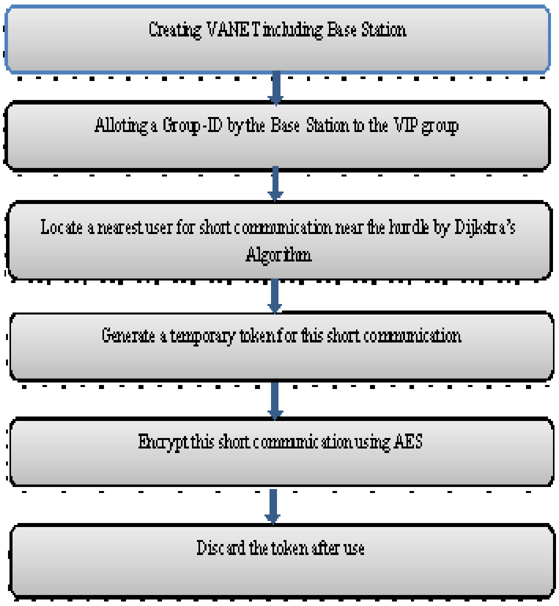
III. PROPOSED RESEARCH

The proposed research mainly focuses on the safety measures of some very important persons. The person can be a Prime Minister, a patient or a Criminal. Whenever the VIP travelling with the group of cars wants to commute through a road where there are hurdles, one of the vehicles has to contact the Base Station which will find out a nearest vehicle near the hurdle. The Base Station will provide the temporary token to these two vehicles after which the communication in encrypted form will take place.

A. Allotting the unique –ids for a special group for communication.
B. Locating nearest user , generating a token for communication and discarding the token after use immediately. The token is generated by a Base station, a trusted authority.

C. Provide ease in communication with security by encrypting the messages.

The flow diagram for the proposed approach is as follows;


Creating VANET including Base Station
Alloting a Group-ID by the Base Station to the VIP group
Locate a nearest user for short communication near the hurdle by Dijkstra's Algorithm
Generate a temporary token for this short communication
Encrypt this short communication using AES
Discard the token after use

A) Allotting unique ids for a special group by using SHA1 algorithm

All the vehicles moving on road have their own unique ids for their identity. But if a very important person like the President or The prime Minister of country is travelling by road the security officials also travel with them. The vehicles of these security officials along with the VIP's are allotted a group key through which only this group can communicate with each other. This is done by SHA1 algorithm. Secure hash algorithm SHA-1 is a hash function that takes a variable length input message and produces a fixed length output message called the hash or the message digest of the original message. The SHA-1 algorithm is of particular importance because of its use with the Digital Signature Algorithm (DSA) for digital signatures.

A hash function takes a variable length message and produces a fixed length message as its output. This output message is called the hash or message digest of the original input message.

The way this algorithm works is that for a message of size < 2^{64} bits it computes a 160-bit condensed output called a message digest . The SHA-1 algorithm is designed so that it is practically infeasible to find two input messages that hash to the same output message. It is also practically impossible to deduce the original input message given only the output hash message.

B)Locating nearest user

This is done by the base station in VANET.When a very important person is travelling by road with the security personnel's and wants to know about some route ,Or about the blockage of roads due to accidents or bad condition of the road, this group can directly approach the nearest base station. This base station locates a nearest user using the GPS and Dijkstra's Algorithm.

Dijkstra's Algorithm

Dijkstra's algorithm solves the single-source shortest-path problem when all edges have non-negative weights. It is a greedy algorithm. Algorithm starts at the source vertex, s, it grows a tree, T, that ultimately spans all vertices reachable from S. Vertices are added to T in order of distance i.e., first S, then the vertex closest to S, then the next closest, and so on. Following implementation assumes that graph G is represented by adjacency lists.This algorithm finds a nearest user to one of the vehicles in the group by using shortest path. The base station now allots temporary tokens to these vehicles for communication.

C) Encryption of messages.

The messages in this short communication are encrypted using algorithm AES.

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure where, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

IV-EXPECTED OUTCOME

This paper helps in proposing a new methodology for designing a system for a special scenario where the commuters can be some very important person. In future we will work to communicate through audio messages for communicating with the vehicles present near the hurdle. This paper concentrates on privacy preserving and secured communication in VANET and also covers the literature survey of some technologies which are involved in the system.

REFERENCES

[1] *T.W. Chim, S.M. Yiu, Lucas C.K. Hui,"VSPN: VANET-Based Secure and Privacy-Preserving Navigation" , IEEE Transactions on computers, Vol. 63, No. 2, February 2014*

[2] Chen Lyu, DawuGu, YunzeZeng, PrasantMohapatra," PBA:Prediction-based authentication for Vehicle-to-Vehicle Communications", IEEE Transactions on Dependable and Secure Computing, 2015

[3] Chun-I Fan, Wei-Zhe Sun and Shih-Wei Huang"Strongly Privacy-Preserving Communication Protocol for VANET", 2014 Ninth Asia Joint Conference on Information Security

[4] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin ," An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks", IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008

[5] Xiaodong Lin, Senior Member, IEEE, and Xu Li," Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks",IEEE Transactions on vehicular technology Vol. 62, No. 7, September 2013

[6] Kyung-Ah Shim,"CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks" ,IEEE Transactions on vehicular technology,Vol. 61, No. 4, May 2012

[7]RajkumarWaghmode, RupaliGonsalves, DayanandAmbawade,"Security Enhancement In Group Based Authentication for VANET", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016 India

[8] NehaGoel, IshaDhyani, Gaurav Sharma, "A Study of Position Based VANET Routing Protocols",International Conference on Computing, Communication and Automation(ICCCA2016)

[9] Rajeev Singh, SumitMiglani, "Efficient and Secure Message Transfer in VANET",International Conference on Inventive Computation Technologies (ICICT) 2016

[10] AditiSelokar, VaishaliSahare, "Various Types of Vehicular Attacks and Its Prevention Techniques in VANET",International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) August 2016

[11]Sok-Ian Sou,"Modeling Emergency Messaging for Car Accident over Dichotomized Headway Model in Vehicular Ad-Hoc Networks", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL 61, FEBRUARY 2013

[12] YogitaRaut, VaishaliKatkar, "Emergency Messaging for Car Accident in Vehicular Ad-hoc Network" , IJCSN International Journal of Computer Science and Network, Volume 3, Issue 1, February 2014

[13] Brijesh Kumar Chaurasia, ShekharVerma, S.M.Bhasker, "Message broadcast in VANETs using Group Signature", Fourth International Conference on Wireless Communication and Sensor Networks

[14] Ren-Junn Hwang, Yu-Kai Hasio and Yen-Fu Liu,"Secure Communication Scheme of VANET with Privacy Preserving",IEEE 17th International Conference on Parallel and Distributed Systems