Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 1– No.3, February 2015 – www.caeaccess.org

Secure Cluster based Self Organized Authentication with Key Management Scheme in Vehicular Adhoc Network

A.Deepika
Dept of Computer Science and Engineering
K.L.N College of Information Technology
Madurai

G.Ganesan
Associate Professor
Dept of Computer Science and Engineering
K.L.N College of Information Technology
Madurai

Abstract
Vehicular Ad hoc Networks (VANETs) are the promising approach and also a key component of intelligent transport system. Its main aim is to provide driver convenience and safety. To improve security and balance the message overload the cluster approach and the key distribution technique is used. In this model first the network is analyzed based on its parameters and develop three models based on road condition and clusters are formed with every node in the network. The group key management scheme improves scalability, reliability, and security of the VANET. Group key management in VANET solves the issues associated with membership changes. In this phase a model for sending a file from the source to the destination using the mesh network is implemented and the core resolution algorithm for finding the core node in that and the expanded ring search algorithm for identifying the next mesh address in the path to reach the destination. Through this the scalability and the efficiency of network is improved.

Keywords
VANET, cluster formation, ring search algorithm, key Management

1. INTRODUCTION
A Vehicular Ad-Hoc Network or VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network.VANET is a subgroup of MANET where the nodes refer to vehicles. Since the movement of Vehicles is restricted by roads, traffic regulations can deploy fixed infrastructure at critical locations. The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. It is a spontaneous ad hoc network formed over vehicles moving on the road. Such a network can be formed between vehicles with V2V communication or between vehicles and infrastructure with vehicle-to infrastructure (V2I) communication. Such VANETs in which vehicles can communicate with each other and also with roadside infrastructure provide a means to improve road safety by enabling a number of potential applications for driver assistance, collision warning, traffic information, and monitoring the availability of various applications will improve road safety and vehicular environment. Most of the concerns of interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. Providing security to VANET is important in terms of providing user anonymity, authentication, integrity and privacy of data. Most vehicles are restricted in their range of motion. It has rapid dynamic topology and unlimited battery power and storage but in every communications anonymity must be preserved. Any communication in the network is done through VCS.

2. EXISTING SYSTEM
Existing scheme uses the online road information collected by vehicular adhoc network to guide the drivers to desired destinations in a real-time and distributed manner also it has the process of using real-time road conditions to compute a better route and at the same time, the information source can be properly authenticated. To protect the privacy of the drivers, the query for the destination and the driver who issues the query are guaranteed to be unlinkable to any party including the trusted authority. This scheme uses anonymous credentials to achieve this property. Messages sent in the system must be authenticated and signed to make sure that they were not modified by anyone. And it also uses pseudo identity to protect the users real identity from the others users of the network. Secondly Navigation queries and results are protected to preserve user's confidentiality and operator's profit. On the other hand, one's real identity and navigation query are completely delinked using the idea of anonymous credential. Information provided by RSUs can be properly authenticated in an efficient way.

2.1 Limitations on Existing System
In this scheme the route searching process is done by the central server so this approach is not scalable especially for the large cities .It uses anonymous credential for authenticate the transaction but it needs the trusted credential issuer which is a challenge in case of the adhoc network where no single party can be trusted

Then it also leads to a single point of failure and sometimes it is an easy target for compromise

3. PROPOSED SYSTEM
In the proposed work various models are developed in the network and make it work in a distributed manner. This method intends to improve the network performance and reduce the message overhead in the existing system. The network and all the vehicles in the network will be examined then based on its position in the network, three models for Highway, city entrance and inside city/town will be formed. Then to overcome the limitations of the existing system this method will form the cluster in the network. Those are formed by analyzing the position and the direction of every vehicle in the network. After that if have to send the warning message or the navigation information to the users in the network it will be send by using the key management technique. Through

every transformation of message it will generate key and send the message to the appropriate user in the network. This proposed method is effective in terms of processing delay and improve the performance of the network.

4. MODULES DESCRIPTION CLUSTER FORMATION

Usually in the vehicular adhoc network vehicles are separated by the certain distance. So for forming the clusters the parameters like vehicle speed, direction and its connectivity degree with the others are considered. Based on these small-small group of dynamic clusters will be formed. After grouping the vehicles in all three models into the clusters then decision about who are all be the members of the cluster and who will be the cluster head have to be defined. Speed difference among the vehicles is the prime parameter for identify the members. Members are formed by examining their activities and their distance between each other.

4.1 Data dissemination

After forming the cluster and then any data in the network can be passed. For transferring the message or to ask any query a vehicle needs to authenticate it first but its real identity will be kept anonymous. Then by using Road side unit any information needed for a user or any warning message can be send to the members of the network by using the cluster head and then it will be further transmitted to the other members of the network so by using this technique also perform Congestion notification for drivers about the traffic surrounded by the vehicle and provides secure driving option and reduces accidents on highways. Scalability of the scheme can be evaluated by varying the number of nodes involved in the network.

4.2 Key Management

The secured VANET should ensure that the data packets are not routed through the malicious vehicles. As the vehicles join or leave the network at any time, all the vehicles change their public parameters that lead to security constraints. Group key management in VANET solves the issues associated with membership changes. To provide a new secret key generation scheme to improve the data security. The core objective is to generate a unique key which can provide data confidentiality and improve the strength of extracted key. Secret key generation using Received Request Message (RRM) scheme can be used to achieve the objective. The secret key extracted from this method using request message consists of source and destination IP, port and user request along with random number will provide high entropy data bits to ensure strength of the key and can attain data confidentiality. The group key management scheme improves scalability, reliability, and security of the VANET.

4.3 Security

This model also focuses on the security features of the network.Because of the dynamic nature there is more possibility of attacks in the network. So it includes the scenario in which the network is checked under the occurrence of some attacks and then it performance is identified in that case to easily understand the efficiency of the network in all the possible scenarios. Performance is measured by considering the network with different number of nodes and then complexity for time based on the key generation time, certificate generation time and also the message routing time is measured and for the key and certificate repository space is measured for calculating the space complexity

5. TECHNIQUES AND ALGORITHMS USED

5.1 Mesh based Routing

Mesh-based multicast routing protocols are more than one path may exist between a source destination pair, Mesh-based schemes set up a single path connecting any two nodes in the multicast group and as mobility increases, link failures start the reconfiguration of the complete mesh. While forwarding the information from source to destination, we have many forward nodes, so there is many hop count, and to reduce we are using AMROUTE protocol. Group member means it identifies path and data transmission to node it reduce the number of transmission. It can change the path quickly to one leader to other leader. Packet delay and time delay has been reduced.

5.2 Core Resolution Algorithm

Tree Initialization Phase

When either a source or receiver wants to join the multicast group they declare themselves as logical core of a one mesh node and flood JoinReq control packets with increasing TTL to discover other members. It should have only one logical core by using core resolution algorithm only one node should remain as a logical core node in the segment.

Tree Maintainence

Due to the movements of the nodes or because of the node failures the modes may split into the parts, nodes in the fragmented parts needs a Tree Create message from the logical core after waiting for the random time period one of the members become the core node and initiate the process of discovering the other disjoint mesh as well as the tree creation..

5.3 Expanded Ring Search Algorithm

In the ERS scheme, the source node will broadcast the RREQ to its neighbors to find route. If the neighbor nodes receive it for first time, it will further forward the RREQ otherwise it will just drop the packet. Hence, much useful information gets lost due to dropping of the packet. Therefore we process a design which helps in utilizing the information before dropping the duplicate RREQ packets to make decision about node's relay value. This helps in making some nodes silent without forwarding the redundant rebroadcast of the RREQ and thus reduces energy consumption

6. IMPLEMENTATION RESULTS

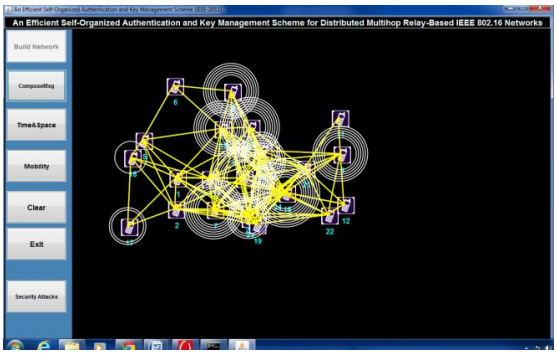


Fig 1 Network Formation

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 1– No.3, February 2015 – www.caeaccess.org

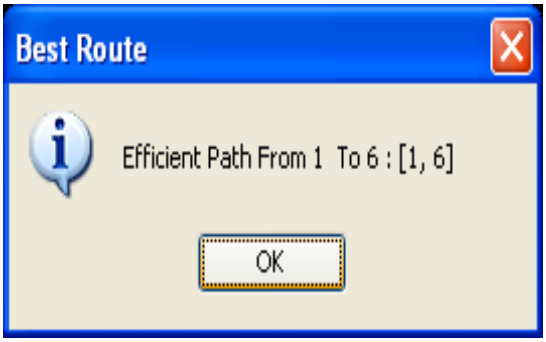


Fig 2.Route Calculation

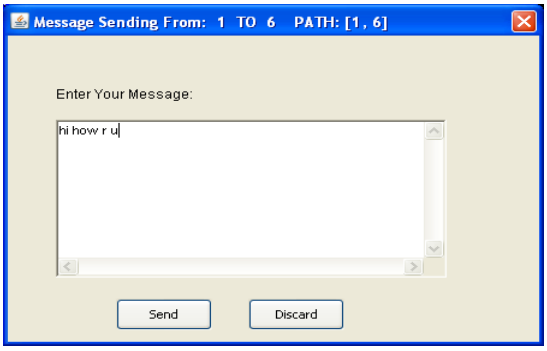


Fig 3.Message Specification

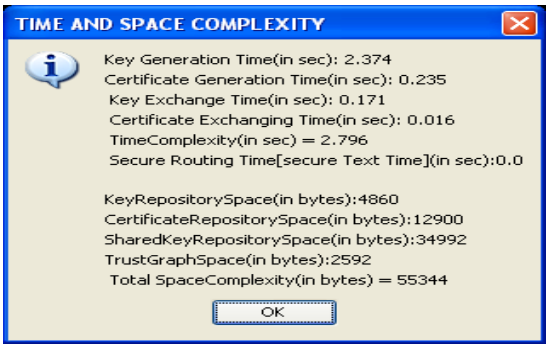


Fig 4.Complexity

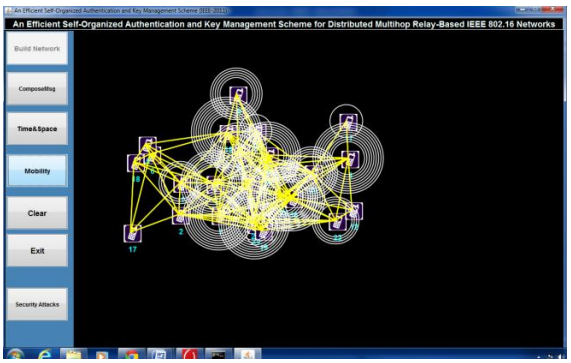
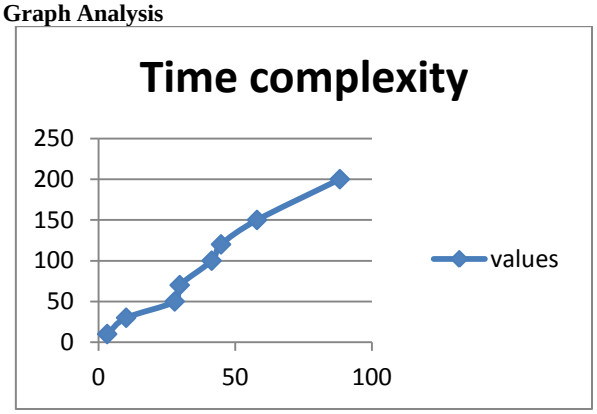


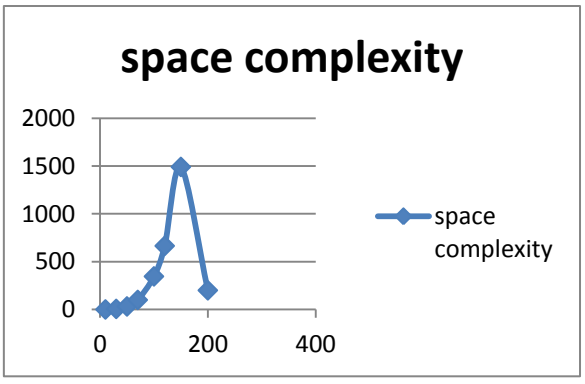
Fig 5 Mobility

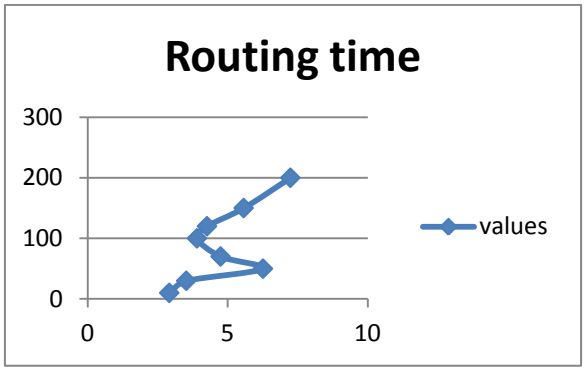
Nodes	Source	Dest	Time complexity (sec)	Routing time (sec)	Space complexity (bytes)
10	1	6	3.167	2.918	234096
30	13	28	10.112	3.525	6169232
50	12	30	27.886	6.265	33279248
70	29	60	29.727	4.75	104574640
100	30	77	41.417	3.906	362680800
120	48	101	44.846	4.265	697323552
150	61	106	58.014	5.577	1563527792
200	70	120	88.336	7.245	210281584

Fig 6 Comparison Table

Graph Analysis







Above table and graph defines the various ranges of the network performance in sending the data from one node to another. Based on the number of hops between the source to destination, time complexity and routing time of the network varies and space complexity includes the space needed for the key repository space and the certificate space and the values in the network changes according to the current number of nodes in the network and the amount of data transfer in the current scenario.

7. CONCLUSION

Vehicular Adhoc Networks has many important features helps to improve the traveler's safety and convenience while travelling. But its high mobility and irregular connectivity needs to provide security. so the approach of creating the models for each road condition rectifies the problem of centralized approach and also the clustering technique helps to maintain the stable cluster and it is better in terms of cluster formation time and the life time since we can assure that it is effective in terms of processing delay, lower route blocking rate and providing routes of much shorter traveling time. Further improvement can be made by creating the three models for Highway, city entrance and inside city/town and apply the key distribution technique in different clusters developed for three models helps in improving the efficiency of the model in the distributed approach.

8. REFERENCES

[1] Kakkasageri M S and Manvi S S, "Connectivity and Mobility Aware Dynamic Clustering in VANETs "International Journal of Future Computer and Communication, Vol. 3, No. 1, February 2014

[2] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K. "VANET based secure and privacy preserving Navigation" ieee transactions on computers, vol. 63, no. 2, February 2014

[3] Mejri Mohammed Nidhal, Jalel Ben-Othman, "VANET security challenges and possible cryptography solutions", journal on vehicular communications, January 2014(Elsevier)

[4] Juan A. Martinez, Daniel Vigueras, Francisco J. Ros, and Pedro M. Ruiz "Evaluation of the Use of Guard Nodes for Securing the Routing in VANETs" Journal of communications and networks, vol. 15, no. 2, april 2013.

[5] Maria Elsa Mathew and Arun Raj Kumar P." Threat Analysis and Defence Mechanisms in VANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013

[6] Ameneh Daeinabi, Akbar Ghaffarpour Rahbar "An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks" 2013.

[7] Christina Garman, Matthew Green, Ian Miers,"Decentralized Anonymous Credentials", The Johns Hopkins University Department of Computer Science, Baltimore, 15,october 2013.

[8] Omar Abdel WahabHadi OtrokAzzam Mourad," VANET Qos-OLSR: Qos-based clustering protocol for Vehicular Ad hoc Networks"journel in computer communications, vol 36, issue 13, July 2013.

[9] Bilel Nefsi,Yi Qiong song,"QoS for Wireless Sensor Networks-Enabling service differentiation by using the CoSens"journel in Adhoc Networks,vol 10,issue 4,june 2012.

[10] Zaydoun Y Rawashdeh, Syed Masud Mahmud"A novel algorithm to form stable clusters in vehicular ad hoc networks on highways", Journal on Wireless Communications and Networking 2012.