

An Effective Diffie-Hellman Key Based New Rsu Detection Secure Routing In Vanets

^IIndu.I.R , ^{II}Prof.R.G.Sakthivelan

^{I,II}M.E.,CCE, Anna University Chennai,Tamil Nadu,India

Abstract

A Vehicular Ad Hoc network is a collection of vehicles that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. And designed the new Road Side unit act as a base station. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. In our network to using a movable nodes from one place to another, that time the attacker to hack the data on network.

The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys, whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme. In this paper, we propose a new RSU scheduling in which an RSU builds an agenda that is separated into time slots (TSs). In each time slot, all users that are predictable to connect to the RSU are specified. Therefore, an RSU prepares users' data and caches them during a free TS before the users connect. Using this scheme, the RSU distributes its load among the available TSs. The key distribution to nodes is done by means of two layer process. This project implements a key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It is based on high

level security and more energy efficient data transmission on their network.

Keywords

Rsu Scheduling, TSs, Diffie-Hellman Key Exchange

I. INTRODUCTION

The Vehicular ad hoc networks (VANETs) have attracted a lot of attentions due to their interesting and promising functionalities including vehicular safety, traffic congestion avoidance, and location based services. VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET mainly consists of three components vehicles, roadside devices, and base stations. Vehicles should provide functions for accessing to the internet, communicating among themselves, and offering services such as, traffic monitoring, vehicle diagnostics, cooperative driving, and entertainment services. Among the functions provided, security and efficiency are the two most concerned issues. For example, it is essential to assure that life-critical traffic information cannot be modified or forged by an attacker. Also, it may require that the protocol needs possessing the anonymity property. A number of researches have investigated on the two issues, security and efficiency.

Current research trends for VANETs focused on developing two groups of applications. For improving the safety level on

the road and providing commercial and entertainment services. All the vehicles in the network and RSUs will be equipped with onboard processing and wireless communication modules for enabling such applications. Then, vehicle-to-vehicle and vehicle-to-infrastructure (V2I) communications will directly be possible when in range or across multiple hops. RSUs are usually connected to the Internet and allow users to download maps, traffic data, and multimedia files and check emails and news etc.

In VANET, where each vehicle periodically broadcasts messages including its current position, direction and velocity, as well as road information.

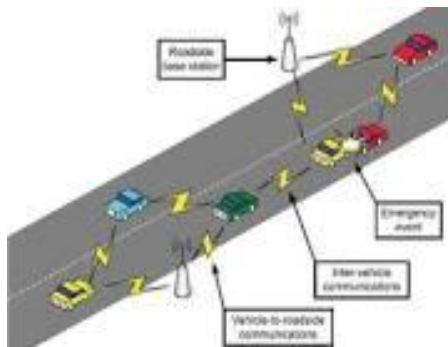


Fig 1. Routing in VANETs

Privacy is an important issue in VANETs. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. VANET basically used to provide various services to its user. In this framework, road side unit (RSU) acts as the key distributor. A new problem encountered is that a RSU may misbehave. A secure key distribution protocol is used to detect such misbehaved RSUs. The protocol guarantees the traceability of compromised RSUs and malicious vehicles. Misbehavior of the system should be defended. VANET system provides the intercommunication between the vehicles by

letting them exchange the traffic information. Such kind of exchanges may create privacy apprehension since the vehicle-generated information can contain much confidential data of the vehicle and its driver. Vehicular networks pose a number of unique challenges.

Security and efficiency are two crucial issues in vehicular ad hoc networks. Many researchers have devoted to these issues. However, we found that most of the proposed protocols in this area are insecure and can't satisfy the anonymous property. Due to this observation, we propose a secure and anonymous method based on bilinear pairings to resolve the problems. After analysis, we conclude that our scheme is the most secure when compared with other protocols proposed so far. For the rapid development in the hardware technology, vehicular networks would be widely deployed in the coming years and become the most important application of ad hoc networks. VANETs are expected to greatly enhance drivers' safety and improve the efficiency with which information on local traffic conditions is disseminated. However, the communication model for these versatile networks is unprecedentedly unique compared with other popular networks.

Advances in mobile networks and positioning technologies have made location information a valuable asset in VANETs. However, the availability of such information must be weighed against the potential for abuse. In safety enhancing applications, each vehicle needs to periodically broadcast an authenticated safety message, which includes its verifiable identity, its current location, speed, and acceleration. Although these safety messages can help to prevent accidents, they may also be used by the adversaries for unauthorized location tracking of vehicles. By using an external WiFi network, an attacker can eavesdrop on all the broadcast messages and determine the locations visited by the vehicles (or users) over a period of time. The location history information (or mobility

traces of the target vehicles) can be exploited for advertisement or surveillance. Thus, protecting the location privacy of vehicles is important because the lack of privacy may hinder the wide acceptance of VANET technology.

VANET are very likely to be emerged in the coming years.

The main contributions of this paper can be summarized as follows,

- 1) We propose a new key exchange method ,Diffie-Hellman key exchange for providing security to the VANET.
- 2) We illustrate a new RSU scheduling mechanism .
- 3) We explain a new cryptographic approach for providing higher security measures compared to existing ones and analyze the performance of our approach using mathematical and simulation means.

II. AIMS & OBJECTIVES

The Main Objective of the proposed research to develop new RSU scheduling instrument in which an RSU builds an agenda that is separated into time slots (TSs). In each time slot, all users that are predictable to connect to the RSU are specified. Therefore, an RSU prepares users' data and caches them during a free TS before the users connect. Using this scheme, the RSU distributes its load among the available TSs. And also the Diffie-Hellman key method. In these key is used to exchange is vulnerable to attacks whereby an intruder intercepts messages between the sender and receiver, and assumes the identity of the other party. Consequently, the Diffie-Hellman algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are established between legitimate parties. In upper layer, rekeying is performed using the secret key between BS and normal node on the basis of time slot. The data send from source to destination on network through a base station. That time have any attacker to attack the data, so implement to avoid

that data loss on network, using the secret key is generated for an each node; it has secure and more flexible on the network. Finally using the Key as well as timeslot the RSU is to allocate the each time slot for each user. We have to take parameters for throughput, delay and level using to better results on the network.

III. MATERIALS & METHODS

Prior work in our existing system to be consider the real time traffic management. The VANET network is depends on the Road Side Units. The achievement of data gaining and delivery systems Based on their capability to protect subsequently to the different types of security and privacy attacks with the aim of exist in service-oriented VANETs. And a system that takes gain of the RSUs that provide various types of information to VANET users. In VANET use the hierarchal password-based key derivation function, in this function to generate the individual secret key in each vehicular user. Using those key the user can travel the data in to correct destination in network. Sometimes our RSU system to give the duplicate key, so the easily attackers access the path as well as data that time the destination doesn't get original data.

IV. Feasibility Study

Feasibility study is the test of a system proposal according to its workability, impact on the organization, ability to meet user needs, and effective use of recourses. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible.

A. Technical Feasibility

The technology used can be developed with the current equipments and has the technical capacity to hold the data required by the new system.

- This technology supports the modern trends of technology.

B. Operational Feasibility

This proposed system can easily implemented, as this is based on ns 2. The resources that are required to implement/install these are available. So the project is operationally feasible.

C. Economical Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system.

V. RESULTS & DISCUSSIONS

An Analytical and simulation study shows that this proposal enhances much security to the VANET. We evaluate the performance of our algorithm using trace driven simulation. In this paper we study the key exchange, security of the data message exchanged between users and RSUs and location privacy of VANET users who exchange these messages.

RSU scheduling

VANET uses the road side units (RSUs) in the roads every 100m so that the information about the vehicles and their position, location, driving speed of other vehicles are transferred between the RSU and the vehicles through the OBU (on board unit). Through the RSU and OBU the messages are transferred and safety prevention of vehicles

RSU scheduling in which an RSU builds an agenda that is separated into time slots (TSs). In each time slot, all users that are predictable to connect to the RSU are specified. Therefore, an RSU prepares users' data and caches them during a free TS before the users connect. Using this scheme, the RSU distributes its load among the available TSs. In this process to maintaining the separate time slot as well as key for every user.

Collusion attack

Due to the dynamic nature of VANET the vehicle nodes are inter related with the key generation node and thus lead to the security issue, as soon as

collusion takes place the cluster head selects another KG node and keying process continues.

Diffie-Hellman key exchange

the channel. The data send from source to destination on network through a base station. That time have any attacker to attack the data, so implement to avoid that data loss on network, using the secret key is generated for an each node; it has secure and more flexible on the network. Finally using the Key as well as timeslot the RSU is to allocate the each time slot for each user. We have to take parameters for throughput, delay and level using to better results on the network.

Simulation

This section presents the simulations that we performed to evaluate the security. We used the ns2 software (version 2.34 with the 802.11p amendment. The wireless bandwidth and the radio transmission range were assumed 6 Mbps and 300 m, respectively. In this model, we used an m-value of 3 for distances less than 50 m, 1.5 for distances between 50 and 150 m, and 1 for distances above 150 m. The default number of vehicles was set to 100, and their minimum and maximum speeds were set to 15 and 30 m/s. Each scenario was repeated ten times, and the final results are the average of the ten runs. Five RSUs were evenly deployed City map used in the simulations. across the map to balance their loads as much as possible. Two of the four corner RSUs were wired to the RSU at the center, whereas the other two corner RSUs and the one at the center were simulated to have an Internet connection. Each RSU was simulated to be wired to an SP, linked through an access point to a second one, and connected through the Internet to a third one. Consistent with the literature, the delay for an RSU to access the wired SP was set to 20 ms, and the delay for accessing the wireless SP was set to 50 ms. The delay for an RSU to send a message to another was

uniformly distributed over the range [0.05, 0.1] s. Each vehicle generates every 5 s a new request that randomly targets one of the 15 SPs. Hence, the default value of the request rate (R_r) was set to 12 requests per minute. The size of data packets was set to 350 B. This value was chosen to ensure that the size of the encrypted packet will be less than the maximum transmission unit (MTU) of 802.11 MAC (1500 B) after adding the necessary headers. The Internet user registration process was substituted by installing at the RSUs data files that include users' information. These files are read by the RSU agent (ns2 C++ class) that processes the user connections from the vehicle agent. The processes of generating different keys were implemented as functions in their corresponding agents. The cryptographic operations were implemented using the Crypto++ package. The widely used AES algorithm was used for the encryption and decryption of messages.

VI. CONCLUSION

In this paper, we have proposed a method for enhancing the security of vehicular communication using Diffie-Hellman key exchange. The detection system using the Diffie-Hellman key exchange method used to be one of the most interesting key distribution schemes use today. However, one must be aware of the fact that although the algorithm is safe against passive dropping, it is not necessarily protected from active attacks distribution to allow malicious nodes to interact within the network for transferring data between sources to destination and hence complete security could not be achieved within the network due to the presence of malicious nodes. In order to provide more secure communication between source and destination, DH uses risk as an input to

determine how much source node can be trusted, so that only trusted nodes are allowed to communicate and hence high security can be achieved within VANET. They have to take a throughput, delay and delivery ratio are network performance on the network. It most efficient and security based data transmission.

VII. REFERENCES

1. M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," in Proc. SASN, Alexandria, VA, Nov. 2005, pp. 11–21.
2. K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "AMOEBa: Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007
3. C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Comput. Commun., vol. 31, no. 12, pp. 2803–2814, Jul. 2008
4. H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 16–22, Aug. 2008.
5. 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.
6. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun. Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008
7. J. Petit and Z. Mammeri, "Analysis of authentication overhead in vehicular networks," in Proc. WMNC, Budapest, Hungary, Oct. 2011, pp. 1–6.
8. K. Mershad, H. Artail, and M. Gerla, "ROAMER: Roadside Units as message routers in VANETs," Ad Hoc Netw., vol. 10, no. 3, pp. 479–496, May 2012.
9. K. Mershad and H. Artail, "SCORE: Data scheduling at roadside units in vehicle ad hoc networks," in Proc. ICT, Jounieh, Lebanon, Apr. 2012, pp. 1–6.
10. Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" in vehicular technology, vol. 62, no.2, feb 2013.