Secure Message Broadcasting in VANET Using RSU based Authentication and Cascade Encryption

T. Kirthiga Devi
Department of Information Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India. E-mail: kirthigt@srmist.edu.in

R. Mohanakrishnan
Department of Information Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India. E-mail: mohanakrishnan_ra@srmuniv.edu.in

T. Karthick*
Department of Information Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India. E-mail: karthict@srmist.edu.in

Received July 24, 2020; Accepted September 30, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17062

Abstract

Vehicular ad-hoc networks were introduced by applying certain principles based on MANET where nodes are high mobility vehicles. Because of this mobility of vehicles topology were rapidly changing, hence Security issue will predominant in VANET. Since network is accessible from every node, any malicious node can easily targets or get access into the network. In order to eliminate this issue a RSU based authentication should be introduced. Also in order to secure the message broadcasting between nodes and eliminating certain attack like Man-In-The-Middle (MITM) attack, a cryptographic technique called cascade encryption are used to broadcast the message from one vehicle to other vehicle in a secure and efficient way. With the help these two concepts we can able to satisfy the privacy and security requirements of Vehicular ad-hoc networks in an efficient manner.

Keywords

VANET, RSU, MITM, Cascade Encryption.

Introduction

VANET plays vital role in improvising the travel experience and also mainly focusing on transportation system's safety[1]. Each vehicle in VANET has an embedded onboard unit which has the capability to communicate road condition and traffic data to every nodes with the help of RSU. For example whenever a car detects an accident or bad road conditions, it transfers those data to the nearest node i.e., either by broadcasting it to other cars or through RSU unit. With the help of this every node had an awareness about the environment of driving and also made a driving plan change if needed. Hence VANET helps in minimizing the accident numbers and ensuring a safe driving condition.

VANET utilizes DSRC with the help of IEEE 802.11p. Since VANET is wireless, it is vulnerable to most of the attacks, among those attacks Wormhole, Black hole and Man-In-The-Middle attack were common and provide a wide range of threat to VANET. The main objective of message broadcasting in VANET is providing trusted knowledge about current road condition.

Usually VANET allows an approximate distance up to 300 meters of distance, when the node crosses the range then signal breakdown occurs then new node can join with that node which is under the range[2].

Background

Generally VANET consist of three main components which are considered as basic building blocks of the architecture. These three components are common to all the VANET models. Those components are listed below.

A.) Trusted Authority (TA)

In VANET, the term Trusted Authority(TA) is used to indicate the Department of Transportation. The main role of TA is to monitoring road conditions in real-time with the help of RSU. This helps the Department of Transportation to take timely action during emergency like accident.

Also the registering authority were come under TA only. They are responsible for registering a new node i.e., a new car registration and providing certain system parameters.

TA will manage which vehicles can be inside the network based on OBUs. It will authorize OBUs for registration. TA plays a major role in managing security measures. Each users need to register their car's OBU through TA only. Once registered that OBU will be added to the database so that it will be used while enforcing security.

B.) Road Side Unit (RSU)

Road Side Unit are installed in the path of roadside that can act as interface between every nodes. It is a part of infrastructure of VANET. Since every RSU are connected to each other so that it can able to exchange data between them.

C.) On-Board Unit (OBU)

OBU is defined as the radio device which is installed in each and every nodes i.e., in every vehicles. These are responsible for interconnection between nodes. Also involves in transferring data between devices.

Categorization of VANET Attacks

Since VANET uses wireless technology, it is prone to numerous amount of attacks. But most predominant and dangerous attacks in VANET are Black hole attack, Man In The Middle attack and Wormhole attack. These attacks allows the attacker to disrupt or modify the working of VANET. These were plays a vital role while implementing VANET in real time.

A.) Wormhole Attack

Wormhole attack is termed as faking a path which is shorter than the legitimate one within the network, that can lead to create confusion in the routing mechanisms of the network which is based on the knowledge about the distance between those nodes. Usually it has one more number of nodes.

The unauthorized node capturing the packets and tunnel those packets with the other unauthorized node. It can be launched by attacker even without having more data about communication. The tunnel is an high frequency link which creates an illustration that two points of tunnel are near to both.

Here modes are broadly classified into two types. They are Hidden modes and Participation modes. In this the Hidden mode is further divided into Encapsulation and Replay. Also participation mode is classified as High Power transmission and out of band transmission.

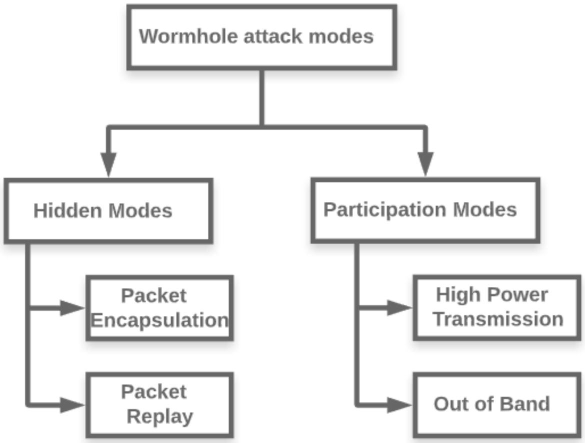


Figure 1 Wormhole attack

B.) Blackhole Attack

Black hole attack in VANET is major problem in achieving a good networking. Here an unauthorized vehicle which creates its own protocol for routing which in turns advertising as having a shortest route to reach desired destination vehicle that it intercept. When it receives data it drops the packets instantly.

The series of action in Black hole attack is given below.

- Initially the unauthorized node detect an actively available route and captures the desired address of destination.
- After this the unauthorized node will start sending a series of route reply packet (RREP) which includes the address of destination was spoofed with an unknown address of destination.
- Unauthorized node will send a route reply packet to next closely available legitimate vehicle which are belongs to a route that is legitimate.
- Then RREP which was received by the node which is legitimate is now replayed with the unauthorized node through the route by inverse source code.
- Then the information which are received through route reply will make the node that act as source to its routing table for updating.
- In the result of this a new route will selected by node which is act as source in order to select data.
- Finally the unauthorized node will start dropping all the data which are received by that node.

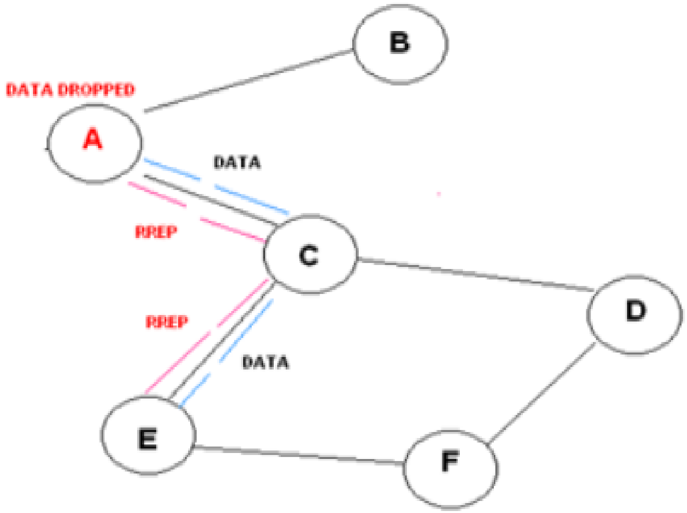


Figure 2 Wormhole attack

C.) Man-In-The-Middle Attack

MITM attack in VANET occurs during an unauthorized node captures or modify messages exchanged between the legitimate nodes. Passively, an attacker may sends data illegally on the communication between the legal vehicles. For example, attacker can capture communication of any vehicles and disclose that communication data to anyone by creating their benefits.

Also attacker can able to delete, create delay in time or edit the information in that network. Let's say, if an attacker receiving a important data like a message of a accident. Then attacker can able to change the message, creating time delay or even delete message.

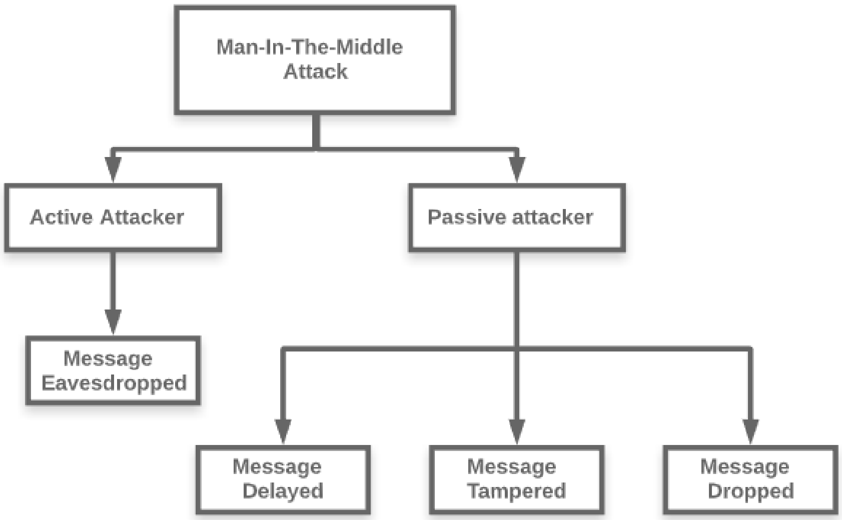


Figure 3 MITM attack

Existing System

There have been some protected mechanism in VANET in which it can able to prevent only certain attacks which are prone to it. Also there is a non availability of an reliable authentication system. Hence any new node can able to access the network from any node. So possibilities of malicious node is more in those systems.

Since in most of the proposed system the encryption can be done only with any one of the algorithm. For example, either of the encryption algorithms like RSA, ECC, etc., were only used. So there no security reliability for those messages as it can be compromised using certain attacks if the algorithm used is found.

In most of the systems when comes to attacks, only certain attacks like wormhole alone can be prevented. There is no certain preventive measures are implemented to overcome certain issue.

Proposed System

In order to eliminate unauthorized node connection or intrusion, we use Road Side Unit (RSU) based authentication. This will prevent the unauthorized node intrusion as only the authenticated nodes alone can enter into the network.

To enhance the data confidentiality, Instead of using same encryption algorithm, we can use combinations of cascade encryptions in order to avoid algorithm based attack. This will increase the complexity level of the decrypting the data without knowing the encryption algorithm and their combinations.

Since the combination of RSU based authentication and cascade encryption techniques will prevent most predominant attacks like Black hole attack, Wormhole attack and MITM attack.

Module Description

The proposed system is split into two different modules: RSU based authentication and cascade encryption.

A.) RSU based Authentication

This module helps in authenticating the vehicle and allow them into the network and also help in creating and maintaining a database which contains unauthorized node lists.

Initially when the car went for RTO registration it will be provided with two unique keys K1,K2,K3 and an ID also it will mapped with the SSID of the OBU of car in a database.

So whenever a car request a connection with the RSU, it broadcast its SSID to the RSU in encrypted form which is illustrated in A1 process. The RSU will then maps that SSID in the database and retrieves those keys which are belongs to the car which is illustrated in A2 process. Now calculate the hash of the decrypted message and compare it with the hash generated at RSU which is illustrated in A3 process.

If both the hash value is same then the car will get access to the network i.e., RSU will share the Encryption Algorithm Table (EAT). If it was different the car will be consider as unauthorized car list.

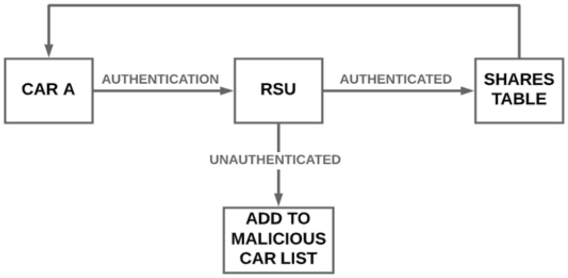


Figure 4 Architecture of proposed system

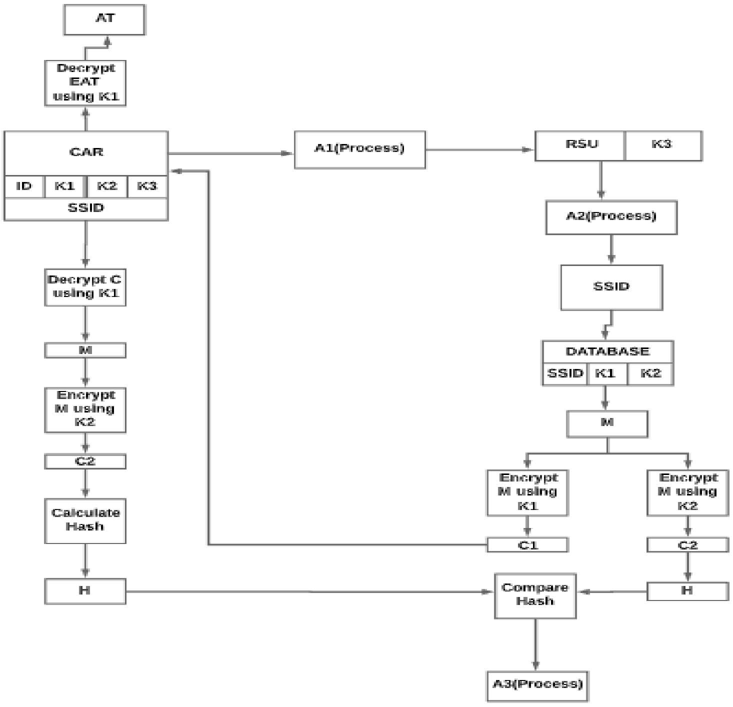
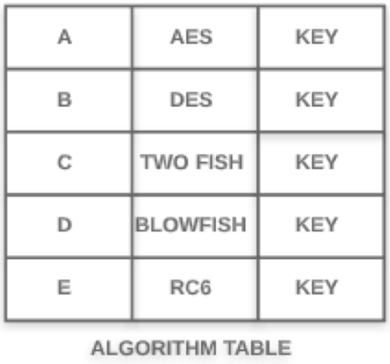


Figure 5 RSU based authentication

B.) Cascade Encryption

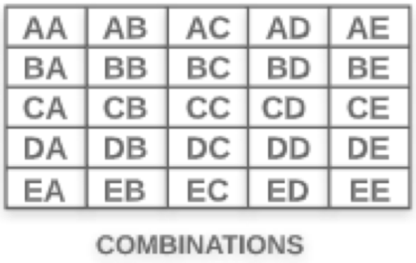
Cascade encryption is a process of encrypting an already encrypted data more than one times, with the help of using the same or a different algorithm. In other words it is also called as Multiple Encryption. Here we are going to use combinations of cascade encryption. So the encryption algorithms and its combinations were tabulated and named as follows.



A	AES	KEY
B	DES	KEY
C	TWO FISH	KEY
D	BLOWFISH	KEY
E	RC6	KEY

ALGORITHM TABLE

Figure 6.a Algorithm table



AA	AB	AC	AD	AE
BA	BB	BC	BD	BE
CA	CB	CC	CD	CE
DA	DB	DC	DD	DE
EA	EB	EC	ED	EE

COMBINATIONS

Figure 6.b Combinations

C.) Vehicle to Vehicle Communication (V2V)

V2V communication is termed as transfer of information from one vehicle to another vehicle. In our model only vehicle which are authenticated by RSU can able to achieve communication. Since only authenticated car have the algorithm table. Here first car selects a combination randomly from combination table then based on the combination it selects the algorithm from algorithm table. After this it encrypt the message using those algorithm and append the combination with the encrypted message. Now it send that message to another vehicle.

As soon as the vehicle receives the message it fetches the combination which is appended by the sender then it maps the combination from algorithm table. Once the algorithm was identified it then decrypt the message using those algorithm.

Even though any malicious user sniff the encrypted message and finds the combinations, he can't able to decrypt the message because only authenticated car can have the algorithm table. Hence it eliminates those unauthorized and malicious users.

As we explained above only because of those malicious user only most of the attacks have been raised. So by eliminating those unauthorized and malicious users we can able to eliminate most of the attacks like wormhole attack, Blackhole attack and MITM attack can be eliminated.

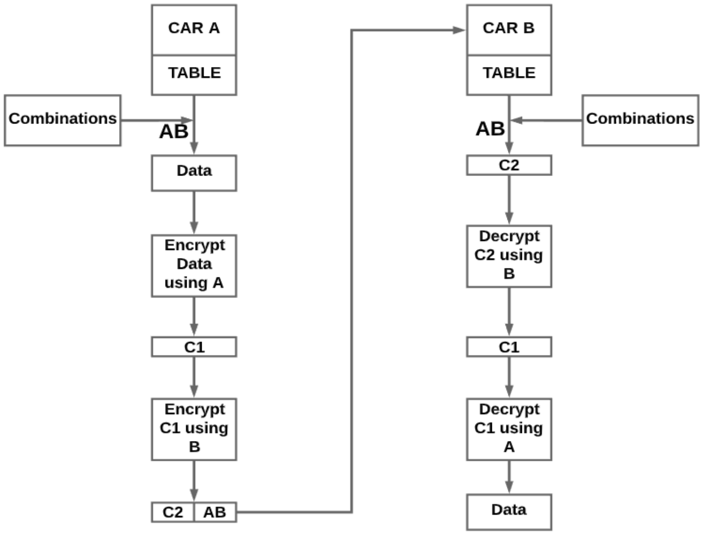


Figure 7 Vehicle to Vehicle Communication

D.) Time Comparison Graph for algorithms

The encryption and decryption time of algorithms used are shown in the graph below.

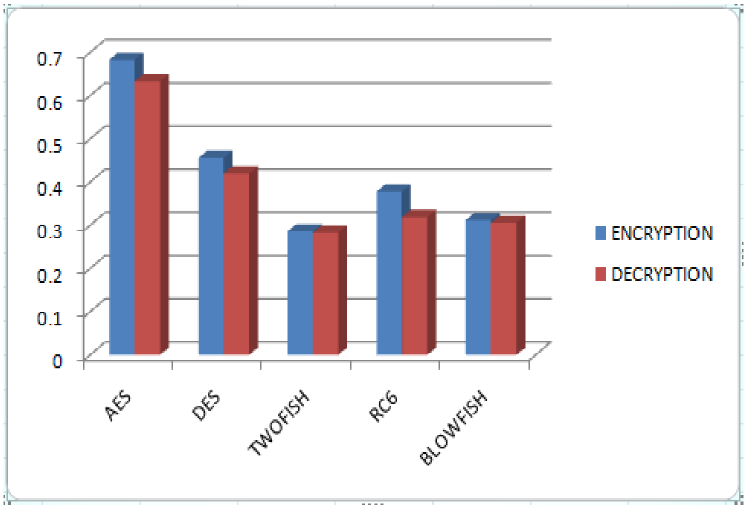


Figure 8 Time Comparison Graph

E.) Computation Speed for Algorithms

The computation speed for encryption and decryption of algorithms used are shown in the graph below.

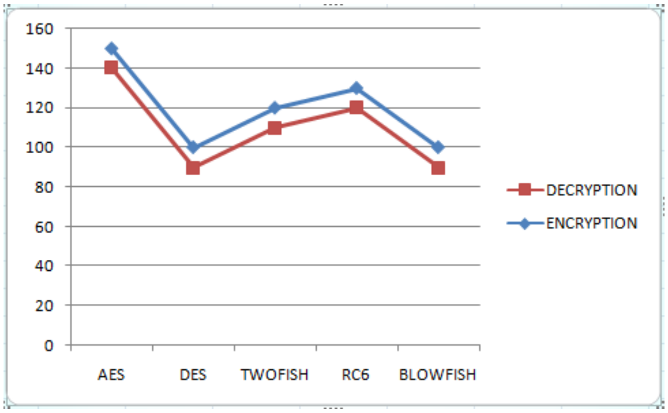


Figure 9: Computation Speed Graph

Conclusion

The inputs from previous researchers, experimental analysis it has been seen that there's an enormous scope for exploration within the field of VANET attacks. It has been identified that the non-control data attacks are more unknown compared to the control data attacks. There are still grey area unexplored in the model with their impact potential still its undetermined. It’s also seen that the prevailing protection mechanisms against the attacks are often improved. VANET still needs more security so as to realize a far better data confidentiality and integrity. The proposed system will help in protecting the VANET against those attacks which occur predominantly in VANET network.

Future Implementation

The proposed system protects VANET only those attacks which occurs predominantly alone. Further attacks like DDOS, Spamming, Greedy drivers attacks based analysis can also be implemented in the future. The system may also fail in some cases against attacks that are mentioned above.

References

Alazzawi, M.A., Lu, H., Yassin, A.A., & Chen, K. (2019). Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Network. *IEEE Access*, *7*, 71424-71435.

Zhang, L., Hu, C., Wu, Q., Domingo-Ferrer, J., & Qin, B. (2015). Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. *IEEE Transactions on Computers*, *65*(8), 2562-2574.

Ayana, B.C., & Joy, M. (2014). Secure Message Broadcasting with Encryption Mechanism in VANETs. *International Journal of Advanced Trends in Computer Science and Engineering (ICCEIT-2014)*, *3*(4), 55-60.

Al-Qutayri, M., Yeun, C., & Al-Hawi, F. (2010). Security and privacy of intelligent VANETs. In *Computational Intelligence and Modern Heuristics*. IntechOpen.

Wu, Q., Domingo-Ferrer, J., & González-Nicolás, U. (2009). Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology*, *59*(2), 559-573.

Xie, Y., Wu, L., Shen, J., & Alelaiwi, A. (2017). EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. *Telecommunication Systems*, *65*(2), 229-240.

Mansour, M.B., Salama, C., Mohamed, H.K., & Hammad, S.A. (2018). VANET Security and Privacy-An Overview. *International Journal of Network Security & Its Applications (IJNSA)*, *10*(2), 13-34.

Raw, R.S., Kumar, M., & Singh, N. (2013). Security challenges, issues and their solutions for VANET. *International journal of network security & its applications*, *5*(5), 95-105.

Sakthipriya, N., & Sathyanarayanan, P. (2014). A reliable communication scheme for VANET communication environments. *Indian Journal of Science and Technology*, *7*(5), 31–36.

Bhoi, S.K., & Khilar, P.M. (2013). Vehicular communication: a survey. Institution of Engineering and Technology (IET) Networks, *3*(3), 204-217.

Karthick, T., & Manikandan, M. (2019). Fog assisted IoT based medical cyber system for cardiovascular diseases affected patients. *Concurrency and Computation: Practice and Experience*, *31*(12), e4861. https://doi.org/10.1002/cpe.4861.

Hubaux, J.P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security & Privacy*, *2*(3), 49-55.

He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, *10*(12), 2681-2691.

Qu, F., Wu, Z., Wang, F.Y., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *16*(6), 2985-2996.

Anandan, M., Manikandan, M., & Karthick, T. (2020). Advanced Indoor and Outdoor Navigation System for Blind People Using Raspberry-Pi. *Journal of Internet Technology*, *21*(1), 183-195.