ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Optimal Privacy- Preserving Authentication and Protection of Network from Black Hole Attack and Sybil Attack

P.Paul Raj[1], V.R.Yamini[2]

Assistant Professor, Dept. of ECE, Krishnasamy College of Engineering and Technology, Cuddalore, Tamilnadu, India[1]

PG Student [EST], Dept. of EEE, Krishnasamy College of Engineering and Technology, Cuddalore, Tamilnadu, India [2]

ABSTRACT: Optimal privacy-preserving authentication scheme based on HMAC and CMAC algorithm is used to determine the data and internet access in secure manner for VANET. VANET is a special form to provide communication between vehicles and nearby fixed Internet Service Provider. The group signature is widely used in VANET to realize anonymous authentication. The existing scheme based on group signature suffer from malicious node. To overcome this problem, first divide the precinct into several domains, in which Internet Service Provider (ISP) are responsible for distributing private keys and managing the vehicles in a localized manner, which also responsible for internet access. Then light weight authentication protocol is used for security purpose. (HMAC) Hash message authentication code and (CMAC) Cooperative message authentication code is used to reduce the computational delay for authentication. ISP is used to eliminate malicious nodes and protects the network from Sybil attack and Black hole attack.

KEYWORDS: VANET, HMAC, CMAC, Sybil attack, Black Hole attack**.**

I. INTRODUCTION

A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, connecting vehicles to one another so that a mobile Internet is created. The primary goal of VANET is to provide road safety measures where information about vehicles current speed, location coordinates are passed with or without the deployment of Infrastructure. Apart from safety measures VANET also provides value added services like email, audio/video sharing etc. VANET refers to Vehicular Ad Hoc Network. At present time, this is considered to be one of the rising technologies that will help in achieving intellectual inter-vehicle communications, flawless internet connectivity that will bring improvement in the road safety, necessary alerts and accessing various comforts and entertainment. This kind of technology combines WLAN, cellular and Ad Hoc networks for achieving the constant connectivity. VANET is independent and self managing wireless communication network, wherein all the nodes present in the network (VANET) act like the servers and/or clients in order to exchange and share information. The latest improvements done in the field of mobile ad hoc network (i.e. MANET) technology and the increasing safety needs and also the consumer's interest in Internet access have resulted in making the VANET to be one of the most important research topics. Communication between different vehicles and the communication from vehicle to roadside have become important parts of vehicle infrastructure integration.

A VANET may be seen as a special type of ad-hoc network used to provide communications between On-Board Units (OBUs) in nearby vehicles, and between OBUs in vehicles and Road-Side Units (RSUs), which are fixed equipment located on the road. The main advantage of VANETs is that they do not need an expensive infrastructure. However, their major drawback is the comparatively complex networking management system and security protocols that are required. This difficulty is mainly due to some specific characteristics of VANETs that allow differentiating them from the rest of MANETs such as their hybrid architecture, high mobility, dynamic topology, scalability problems, and

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

intermittent and unpredictable communications. These features have to be taken into account when designing any management service or security protocol.

Characteristics of VANET

Many different and sometimes competing design goals have to be taken into account for VANETs to ensure their commercial success. When equipped with WAVE (Wireless Access for Vehicular Environment, a novel type of wireless access dedicated to vehicle-to-vehicle and vehicle-to-roadside communications) in it forms a highly dynamic network. Although, some characteristics of VANETs are

A. Highly dynamic topology: The high speed of the vehicles along with the availability of choices of multiple paths defines the dynamic topology of VANETs.

B. Frequent disconnected network : The high speed of the vehicles in one way defines the dynamic topology whereas on the other hand necessitates the frequent requirements of the roadside unit lack of which results a frequent disconnections.

C. Mobility modelling and Prediction : The prediction of vehicle position and their movements is very difficult. This features of mobility modelling and prediction in VANETs is based on the availability of predefined roadmaps models. The speed of the vehicles is again an important for efficient network design. **D.Communication Environment :**As the mobility model may have different features depending upon road architecture highways or city environments. Communicating in these situations has to be taken care.

E. Unlimited Battery Power and Storage : Nodes in VANETs do not suffer power and storage limitation as in sensor networks therefore optimizing duty cycle is not as relevant as in sensor networks.

F.Safety Related: Applications like collision alert, road conditions warning, merge assistance, deceleration warning, etc. will be classified under safety related applications where the main emphasis is on timely dissemination of safety critical alerts to nearby vehicles.

G. Internet Connectivity Related: Accessing emails, web browsing, audio and video streaming are some of the connectivity related applications where the emphasis is on the availability of high bandwidth stable internet connectivity the main factors that would influence the adoption of VANET architecture for future vehicular applications would be -

1) Low latency requirements for safety applications.
2) Extensive growth of interactive and multimedia applications.
3) Increasing concerns about privacy and security.

II. GENERAL TERMINOLOGY

VANET: VANET refers to Vehicular Ad Hoc Network. Vehicular Ad-hoc Network (VANET) is a special form to provide communication among vehicles and between vehicles and nearby fixed roadside equipment. VANET is independent and self managing wireless communication network, wherein all the nodes present in the network (VANET) act like the servers and/or clients in order to exchange and share information.

ISP: Internet service provider (ISP) are responsible for distributing group private keys and managing vehicles in a localized manner, which also responsible for internet access for VANETs.

MANET: Mobile Ad-hoc Network (MANET) is a continuously self-configuring, infrastructure fewer networks of mobile devices connected without wires. But its speed and coverage area are less compared to VANET.

HMAC : HMAC stands for Hash-based MAC. It works by using an underlying hash function over a message and a key. Theoretically, any hash function could be used with HMAC, although more secure hashing functions are preferable.

CMAC: cooperative message authentication scheme named CMAC. By making the neighbouring vehicles cooperatively work, CMAC can ensure that a vehicle knows the authenticity of all received messages without verifying all the message signatures it receives.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

III. RELATED WORK

The following are the approaches followed Vehicular ad hoc Network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. Characteristic of VANETs is high-speed mobility, leading to limited communication time among ISP and vehicles.

IV. PROPOSED SYSTEM

The architecture of the proposed system is shown in Fig1.

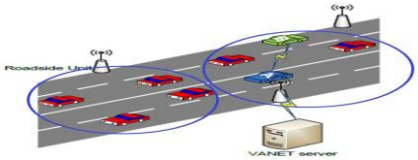

Fig. 1 The proposed architecture

Fig 1 shows that the vehicles are moving in the road side.ISP is responsible for distributing the private keys and generate the vehicle in the localized manner. ISP is instead of RSU. Enables the inter communication between mobile vehicles. Characterized by high dynamic network topology due to car mobility. If malicious node is entered into the network it easily accept the data and dropout the data. Using HMAC and CMAC algorithm to detect the malicious node and secretly share the message among the network.

A.InternetServiceProvider (ISP)

An Internet service provider (ISP) is an organization that provides services for accessing, using or participating in the Internet. Internet service providers may be organized in various forms such as commercial, community-owned, non profit, or otherwise privately owned. Internet services typically provided by ISP include Internet access, Internet transit, domain name registration, web hosting, collocation. This project is first divided into several domains, in which Internet service provider (ISP) are responsible for distributing group private keys and managing vehicles in a localized manner, which also responsible for internet access for VANETs. VANET suffers from different type of attacks and probably more than Mobile ad hoc networks due to their highly dynamic and volatile nature. Mobile Ad-hoc Network (MANET) is a continuously self-configuring, infrastructure fewer networks of mobile devices connected without wires. But its speed and coverage area are less compared to VANET.

Production cost	Inexpensive	Costly
Mobility	Low	High
Range	Up to 100m	Up to 600m
Nodes moving Pattern	Random	Regular
Reliability	Medium	High

Table .1 Comparison between MANET and VANET

The various attacks are as follows
1.Attackers track vehicles to obtain those drivers private information. Attackers use false identities to pretend like other vehicles.
2.Attackers diffuse false information to affect the behaviour of other drivers.
3.Attacker attacks the communication medium in VANET to cause the channel jam or to create some problems for the nodes from accessing the network relax the one-hop assumption.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

B. Attacks of Malicious node: Detecting and preventing malicious nodes launching Sybil and black hole attacks in VANETs by using MNDA (Misbehaving Node Detection Algorithm).MNDA mechanism is used to alleviate the burden on all nodes to perform the packet dropping DOS attack detection function as well as to reduce the number of trust relations that have to be established in the network.

Black Hole Attack: Black Hole Attack, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. The attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet. In Black Hole attack a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information.

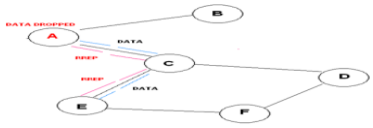

Fig. 2 Data Dropped

But due to the high mobility of vehicles, this technique is too heavy to deploy & is not realistic in VANET. A security protocol is proposed to recognize many Black Hole nodes in the network and to discover a secure & an optimal route from a source to a destination node. This proposed mechanism modifies the AODV protocol by introducing two new concepts in it named as data routing information (DRI) table scheme and cross checking scheme, which provide protection against a black hole attack. In first scheme (data routing information), during the route discovery process, additional information of two bits are transmitted by the nodes that respond to the RREQ message sent by a source node.

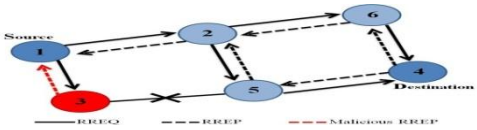

Fig .3 Black hole attack

In every node holds an extra data routing information (DRI) table. The second scheme (cross checking) relies on reliable nodes to transfer data packets. This protocol is very effective & provides a secure network for data transmission.

Sybil Attack: The **Sybil attack** in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

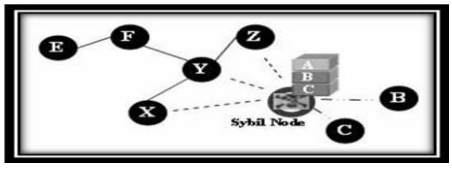

Fig.4 Sybil attack

Sybil attack, a malicious vehicle creates a large number of false identities in order to take over the control of whole VANET & inject fake information in the network to harm the legitimate vehicles. Sybil attack puts a great impact on the performance of the VANET by creating an illusion of existence of multiple vehicles in the network. The impact of this attack is that after spoofing the identities or positions of other vehicles in vehicular network, this attack may lead to other types of attack. Sybil attack in which a malicious vehicle creates a number of false identities of many vehicles & produces an illusion of extra number of vehicles on the road.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

V. WORKING OF THE ALGORITHM

A.HMAC (HASH MESSAGE AUTHENTICATION CODE)

HMAC stands for Hash-based MAC. It works by using an underlying hash function over a message and a key. Theoretically, any hash function could be used with HMAC, although more secure hashing functions are preferable. Commonly used hash functions are MD5 and SHA-1. As computers become more and more powerful, increasingly complex hash functions will probably be used. Furthermore, there are several generations of SHA hashing functions (SHA-256, SHA-384 and SHA-512) which are currently available but not very widely used as their added security is not yet believed to be needed in everyday transactions.

B. Use HMAC Speed is the main reason. Hash functions are much faster than block ciphers such as DES and AES in software implementation .Another advantage is that they are freely available. However, HMAC as a cryptographic mechanism is repudictable. Both a sender and a receiver can generate an exactly same HMAC output. This is unlike digital signatures which only the sender can generate.

C. HMAC Algorithm

The purpose of a MAC (Message Authentication Code) is to authenticate both the source of message and its integrity without the use of any additional mechanisms. An HMAC (Keyed-Hash Message Authentication Code) function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender and compares the result computed with the received MAC. If the two values match, the message has been correctly received and assured that the sender is in the community of users that share the key. This standard specifies an algorithm for applications requiring message authentication. MACs based on cryptographic hash functions are known as HMACs. The purpose of a MAC is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. HMACs have two functionally distinct parameters, a message input and a secret key known only to the message originator and intended receivers. Additional applications of keyed hash functions include their use in challenge response identification protocols for computing responses, which are a function of both a secret key and a challenge message. An HMAC function is used by the message sender to produce a value that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender and compares the result computed with the received MAC. If the two values match, the message has been correctly received and the receiver is assured that the sender is a member of the community of users that share the key. Vehicular Ad hoc Networks also known as VANETs enable vehicles that are not necessarily within the same radio transmission range to communicate with each other. VANETs also allow vehicles to connect to Internet Service Provider (ISPs). The latter are connected to the Internet, forming a fixed infrastructure that offers them the capability of communicating with each other and with roaming vehicles. ISPs support cooperative and distributed applications in which vehicles and ISPs work together to coordinate actions and to share and process several types of information. ISPs have so far been used for different roles such as data disseminators, traffic directories, location servers, security managers and service proxies. In this paper focus on routing; namely we exploit ISPs to route packets between any source and destination in the VANET. This is the first attempt to use the ISP backbone to efficiently route packets to very far locations in VANETs by using geographic forwarding. Evaluate the ISP backbone routing performance via the NS2 simulation platform. Compare scheme to existing solutions and prove the feasibility and efficiency of our scheme in terms of query delay, packet success delivery ratio and total generated traffic.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

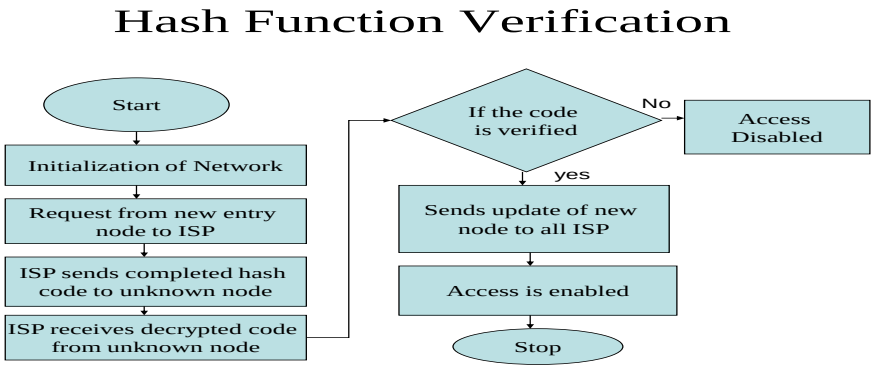

Fig. 5 Hash function verification

E. Steps followed in HMAC

Step1: start the program.
Step2: Initialization of network.
Step3: Request from new entry node to ISP.
Step4: ISP sends completed hash code to unknown node.
Step5: ISP receives decrypted code from unknown node.
Step6: Check the coding and verified the coding, if the coding is verified successfully continue the process, otherwise stop the connection.
Step7: Send update of new node to all ISP.
Step8: Access is enabled.
Step9: Stop the program.

F. COOPERATIVE MESSAGE AUTHENTICATION CODE

ISP may not cover all the busy streets in a city or a highway. For example, at the beginning of VANETs deployment period or due to the physical damage of some ISP or simply for economic considerations. In this project introduce a cooperative message authentication scheme named CMAC. By making the neighbouring vehicles cooperatively work, CMAC can ensure that a vehicle knows the authenticity of all received messages without verifying all the message signatures it receives. Parents and children of any node cooperate to detect any corrupted packets sent by the node and nodes in the network cooperate with a central controller to identify the exact location of all attackers.

Advantages

- Finding the routing good put.
- Calculated in number of packet dropped in the selfish node.
- Detecting and punishing selfish nodes in vehicular ad-hoc network.

H. LIGHTWEIGHT AUTHENTICATION PROTOCOL

It improves the security and routing of VANET by optimizing the features of light weight authentication protocol. The light weight authentication protocol for VANET, which is used for fast routing and data transmission.

I.SELF HEALING KEY ALGORITHM

All the vehicle nodes in a particular network will be having a common key for that network. The ISP will provide all information about the network to all vehicle nodes in that network. If a vehicle node in network may enter the network 1 which has a group of vehicle nodes with a commonly shared key have to be connected. Hence, for this purpose Self Healing Key to provide the key to connect network2 to the network 1. The unknown key will get the common key from

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

the ISP (Internet Service Provider).The objective of self-healing key distribution is to enable group users to recover session keys by themselves, without requesting additional transmissions from the ISP, even when they miss some broadcast messages. One major benefit of the self-healing key distribution mechanism is the reduction of energy consumption due to the elimination of such additional transmission. Also in some applications, e.g., unidirectional broadcast channel from the ISP, the self healing key distribution mechanism seems to be the ideal solution.

VI. RESULTS AND DISCUSSION

Using the HMAC and CMAC algorithm defines the throughput, delivery ratio and packet delay is low when compared to an CRL process because which can easily avoid the attacks.

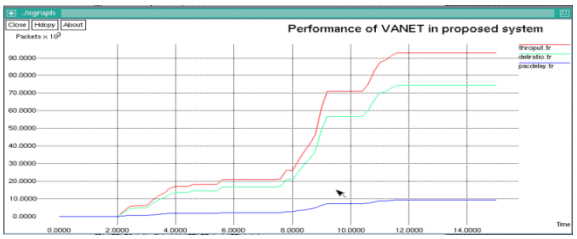

Fig .6 Simulation time Vs throughput, delivery ratio, packet delay

In the fig .7,it shows the graph of time Vs throughput, delivery ratio and packet delay of receiving packet. Throughput is the average rate of successful packet delivery. Packet delay is low when compared to an existing system.

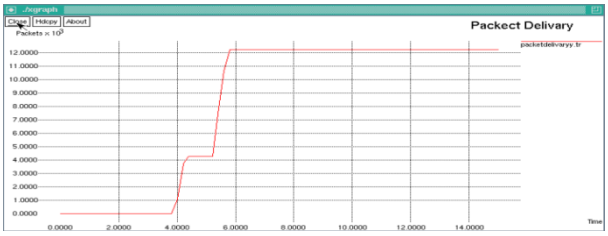

Fig.7 packet delivery Vs time

In the fig.8, it shows the graph of packet delivery of received bits. Delivery packet is high over the communication channel.

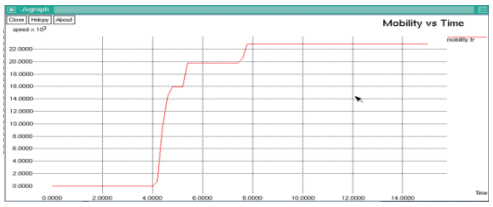

Fig. 8 Mobility Vs Time

In the fig9, shows the graph of mobility Vs time. when compared to the MANET ,VANET mobility is high because it cover upto600m.when mobility is high means performance, speed is also high.

VII. CONCLUSION AND FUTURE WORK

In this project NS2 Simulation is carried out to determine the message packet and internet access in secure manner using HMAC and CMAC algorithm. Light weight authentication protocol is used for security purpose by using NS2

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

simulator. ISP eliminates the malicious node and protects the network from Sybil attack and Black hole attack. In future work Hardware implementation will be carried out by using PIC16F887 micro controller.

REFERENCES

[1] Xiaodong Lin, *Student Member, IEEE*, Xiaoting Sun," GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE transactions on vehicular technology, VOL. 56, NO. 6, November 2007
[2] Yipin Sun, Xiaodong Lin, Xuemin (Sherman) Shen, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications", Yipin Sun, IEEE Transactions on vehicular technology,2010.
[3] Yong hao, Yu Cheng, chi zhou,"A distributed key management framework with cooperative message authentication in vanets", , IEEE journal on selected areas in communications, vol. 29, no. 3, march 2011
[4] Bharati Mishra, Saroj Kumar Panigrahy, Tarini Charan Tripathy," A Secure and EfficientMessage Authentication Protocol for VANETs with Privacy Preservation", World Congress on Information and Communication Technologies 11 – 14 December 2011.
[5] Vinh Hoa LA, Ana CAVALLI, "Security attacks and solutions in vehicular ad hoc networks": A SURVEY . International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.
[6] Ranjitha. P Securable Message Authentication System in Vehicular Ad Hoc Networks by using Trusted Authority, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE),ISSN: 0976-1353 Volume 8 Issue 1,April 2014.