ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

A Holistic Protocol for Insider Attack Detection In VANET Using HMAC

Athira Haridas, Jais John

Abstract— **The Vehicular Ad-hoc network (VANET) consists of mainly three components, they are trusted authority (TA), road side unit (RSU) and onboard unit located inside the vehicles. VANET enables vehicles to communicate with each other and with RSUs. Security is a major problem in VANET. This paper focused on insider attacks. The insider attackers enter into the network and send some wrong messages. It results accidents; traffic block and may damages whole system of the network. The existing system of this paper shows the demonstration of insider attacks and the detection of malicious nodes using consistency checking. But this method cannot prevent the entry of malicious vehicles into the network and certificate revocation list (CRL) checking also a major drawbacks of this method, this produces long authentication delay. The proposed system uses Hash message authentication code (HMAC) for the prevention of insider attacks. It replaces the time consuming CRL checking and reduces the delay and packet loss, increases the message delivery ratio. This increases the rate of successful message transfers. Signature generation in addition with HMAC increases the authenticity and integrity of the message, and is used for the detection of attacks.**

Index Terms— **Vehicular Ad-Hoc networks (VANETs); hash message authentication code (HMAC), Insider attacker.**

I. INTRODUCTION

The Vehicular Ad-Hoc Networks uses cars as mobile nodes and create a network. VANET turns every participating vehicle into a wireless router or allow vehicles approximately 100 to 300 meters each other to connect. Then it forms a wide range of network. The three components of the VANETs are onboard components installed inside the vehicles, road side unit (RSU) situated on the side of the road and trusted authority (TA). In VANETs three types of communications are possible and are vehicle to vehicle communication, vehicle to road side unit communication, road side unit to road side unit communication

In VANETs vehicles are communicate with each other and with RSUs finally the network is connected to a server. The VANET have wide range of applications and mainly classified into three, and are traffic efficiency applications, safety applications, and infotainment services. Post crash notification, congestion road notification, sudden brake warnings these are the examples of safety applications. Path history, path prediction are the some of the examples of traffic efficiency applications. The infotainment services include online playing of game, video streaming, internet browsing. In VANETs security is a challenging issue. Attackers enter into the network and send some wrong messages. It creates traffic jams, the whole system jamming and sometimes results accidents. So the VANET has to be protecting to prevent the entry of malicious vehicles in to the network. The attackers are mainly classified into two and are insider and outsider attackers.

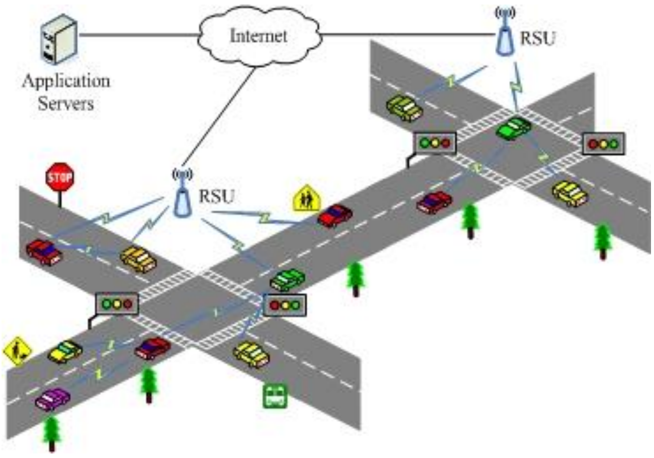


Fig. 1: The Vehicular Ad-Hoc network

Outsider attacks are the attack from the vehicle outside the network and are not in the part of the network where as insider attack is the attack from vehicle those who are inside the network and are more dangerous than outsider attacks. This paper focused only on insider attacks. The existing system of this paper demonstrates the insider attacks and the detection of insider attacks. But it does not prevent the entry of attackers into the network. Increased message loss ratio, increased delay are the two major disadvantages of existing system. The proposed system of the paper uses hash message authentication code (HMAC) for the prevention of attackers into the network. It provides both integrity and authenticity of the message. Here a pair of keys distributed for all the vehicles in the network. At the time of sending the message the HMAC is attached with the message, this provides the authenticity of the message. If we use only HMAC, it is impossible to find the sender of the message. As the result before sending the message the sender has to generate a signature on it. Before accepting the message the receiver has to verify the sender's signature on the message. The attackers fail to provide the digital signature and HMAC. The proposed system can completely control the entry of attackers into the network and also reduces the message loss ratio and propagation delay.

Manuscript received June, 2015.

Athira Haridas , *PG Scholar, Electronics and Communication Dept Nehru College of Engineering and Research Center Thrissur, India.*

Jais john, *Assistant Professor, Electronics and Communication Dept Nehru College of Engineering and Research Center*

II. INSIDER ATTACKS IN VANET

The attack inside the network is called insider attack, and is very dangerous to the network. The insider attackers enter into the network and send some wrong messages. This results the system jamming and accidents. At first the insider attack is demonstrated by using ns2 software. This shows how an insider attacker attacks the VANET. Then the attack is detected by using model based consistency checking. Each vehicle contains a model of the VANET; in this model average speed of the vehicle is recorded. Before accepting the message each vehicle has to verify the consistency of the message by using respective models. If the consistency checking fails ignore that particular information. But this method does not control the entry of the attackers into the network. This is a major drawback of the existing system.

III. DETECTION OF INSIDER ATTACKS

The VANET consists of trusted authority (TA), on board unit (OBU) and road side unit (RSU). TA manages identities of all the vehicles in the network. The certificates of the some of the vehicles are cancelled due to some reasons, and is called certificate revocation list (CRL). The certificate revocation lists send to all the vehicles, at the time of receiving the message, each vehicle have to check whether the receiver's name in the CRL. The size of CRL is very large, so the CRL checking produces long authentication delay. It reduces the packet delivery ratio, increases the delay and packet loss.

In the proposed scheme, message send by each vehicle append with hash message authentication code (HMAC). The HMAC is calculated by the help of a share secret key. The message transmitted from sender to receiver consists of

$$M_i|\mu_{\ i}|HMAC_{kf}|\ (F_i,ID_i)$$

M_i – message sent by the i^{th} vehicle

μ_i- signature of the message M_i

Kf- Secret key

$HMAC_{kf}$ – HMAC computed using secret using secret key Kf

F_i- Hash of the message M_i

ID_i – identity of the i^{th} vehicle sending the message

The signature generation can be done by the help of elliptical curve digital signature algorithm. The HMAC is calculated by a shared secret key between the sender and receiver. The TA issues a pair of keys to all the vehicles in the network. Each vehicle have a public key and private key, the private key knows only the vehicle and public key is uniformly distributed to the network. Consider a vehicle A, the private and public key pair of A can be written as (Pr_a, Pu_a), the private and public key pair of B can be written as (Pr_b, Pu_b). If A wants to send a message to B then first generate a secret key S_{AB}.

S_{AB}= Pr_a*Pu_b= Pr_b*Pu_a.

The HMAC is calculated by using this secret key and is appending with the message, the signatures are generated by using the public key of B. The B verifies the message the HMAC by constructing the shared secret key. If the verification of the HMAC is successful then the sender is authentic, as only authenticate user can compute shared secret key using private key. The attacker vehicle not has the private key, so it cannot create the secret key. This prevents the attack from the unauthorized vehicle. Once the HMAC verification success then the receiver verifies the signature. If the signature verification fails then the sender is an insider attacker. The checking time for the HMAC is very less compared to CRL checking

A. Hash message authentication code (HMAC) code

It uses a cryptographic key and a hash function. The cryptographic hash function, such as MD5 or SHA-1, may be used for the calculation of HMAC. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key. The MAC is sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key. Then compares the MAC functions produced by the sender and the receiver. If the two values match, the message has been correctly received.

$$HMAC\ (K,m)=H((K\ XOR\ o_{pad})\ |\ H((\ K\ XOR\ i_{pad})\ |m))$$

H- a cryptographic hash function,

K- a secret key

m - the message to be send

| - the concatenation

O_{pad-} the outer padding

I_{pad-} the inner padding

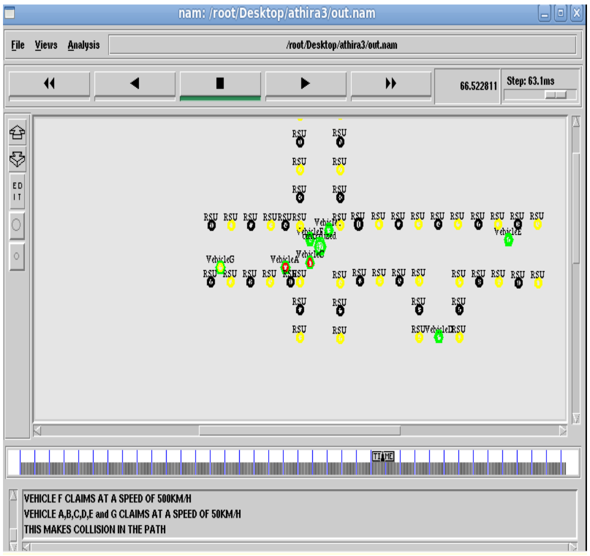
B. Elliptical curve digital signature algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA).This algorithm is used for digital signature generation. The ECDSA consists of three main components, and are given below.

- Private key: It is a secret number, known only to the person that generated it. A private key is a randomly generated number
- Public key: It is a number that corresponds to a private key, but does not need to be kept secret. The public key can be calculated from a private key, but not vice versa. A public key can be used to determine if a signature is authorized or not.
- Digital signature: A digital signature is a mathematical scheme for demonstrating the authenticity of a message. A valid digital signature gives a proof to believe that the message was created by a known sender, and the content of the message is not altered at the time of transmission.

IV. EXPERIMENTAL RESULTS

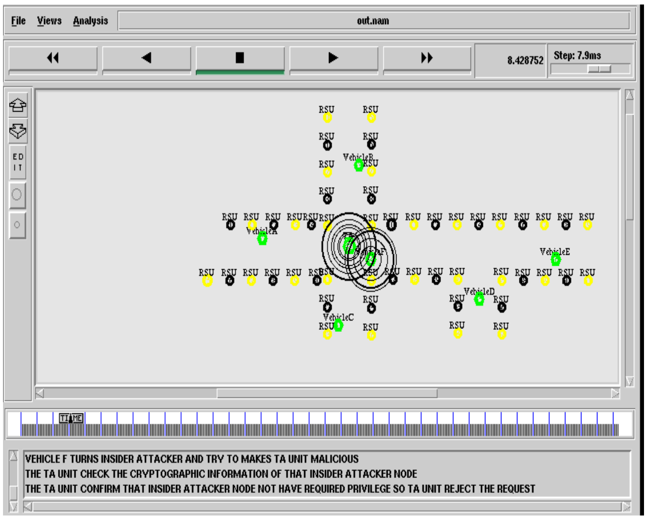
The proposed technique is implemented using NS2 simulator. The parameters used here are packet delivery ratio, Delay and packet loss.



VEHICLE F CLAIMS AT A SPEED OF 500KM/H
VEHICLE A,B,C,D,E and G CLAIMS AT A SPEED OF 50KM/H
THIS MAKES COLLISION IN THE PATH

Fig.2. Demonstration of insider attacks

The vehicle F claims that, is moving at a speed of 500 Km/hr. It is wrong information. It result insider attacks in the network.



VEHICLE F TURNS INSIDER ATTACKER AND TRY TO MAKES TA UNIT MALICIOUS
THE TA UNIT CHECK THE CRYPTOGRAPHIC INFORMATION OF THAT INSIDER ATTACKER NODE
THE TA UNIT CONFIRM THAT INSIDER ATTACKER NODE NOT HAVE REQUIRED PRIVILEGE SO TA UNIT REJECT THE REQUEST

Fig.3. Detection of insider attacks

The vehicle F act as insider attacker, the TA unit checks the cryptographic information of F. But F fails to provide cryptographic information such as HMAC and digital signature. So it ignore the information from F.

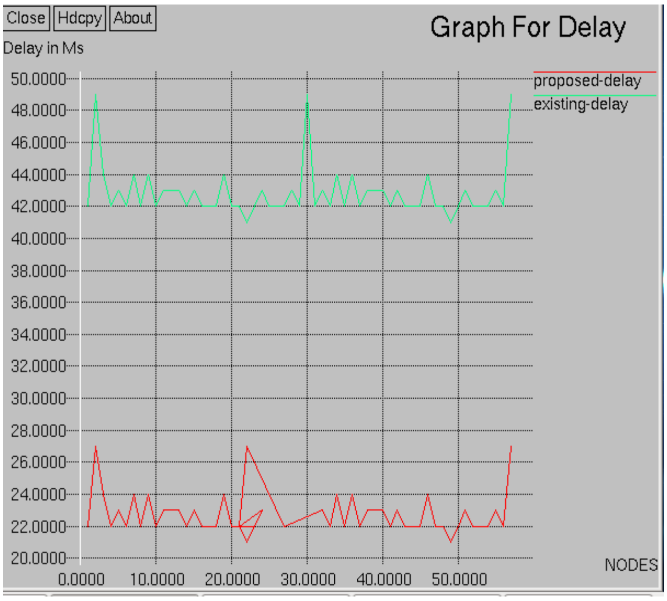


Fig.4. Graph for delay

Compared to existing system, the proposed system delay is very less. This increases the speed of message transfer in the proposed system.

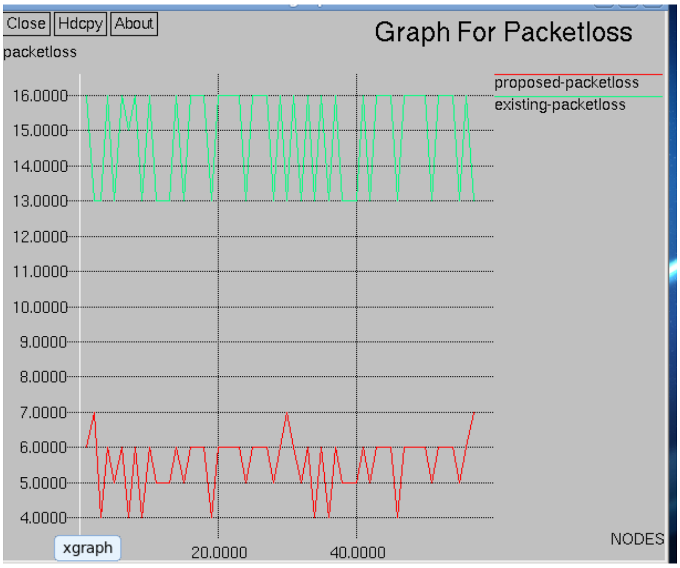


Fig.5. Graph for packet loss

In the proposed system the packet loss is very less. This increases the rate of successful message transfer.

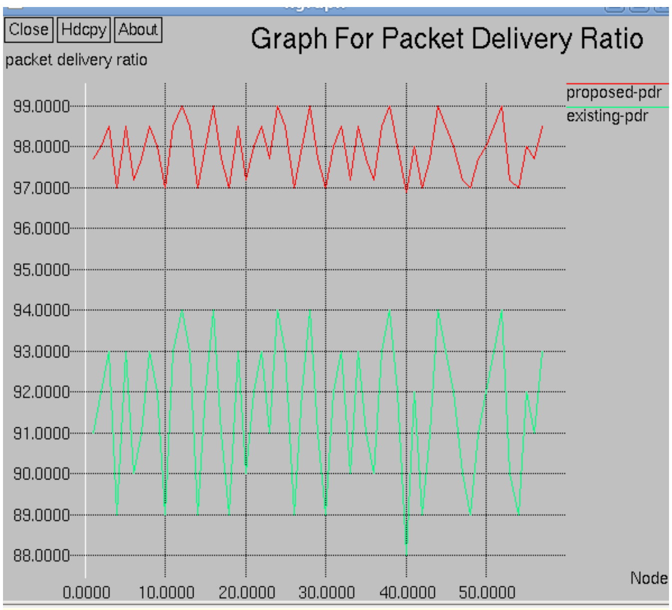


Fig.6. Graph for packet delivery ratio

In the proposed system the packet delivery ratio is 98-99 percentages. This make successful delivery of the all the packets.

V. Conclusion

This paper uses a secure data transmission scheme for the detection of insider attacks in VANET. The Hash message authentication code provides authenticity and integrity of the transmitted message and the Elliptical curve digital signature algorithm used for the signature generation increases the truthiness of the message. This detect attacks from vehicle those who are inside the network. HMAC checking replaces the time consuming CRL checking. This increases the packet delivery ratio and decreases the delay and packet loss. As the result data transmission speed is very high compare to existing system.

ACKNOWLEDGMENT

The authors would like to thank Nehru College Of Engineering And Research Center, for providing the technical support.

REFERENCES

[1] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, “Communication patterns in VANETs,” IEEE Commun. Mag., vol. 46, no. 11, pp. 119–125, Nov. 2008

[2] 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

[3] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs,” in Proc. 1st ACM Int. Workshop VANET, New York, 2004, pp. 29–37.

[4] Z.Cao, J.Kong, U. Lee, M. Gerla, and Z. Chen, “Proof-of-relevance:Filtering false data via authentic consensus in vehicle ad-hoc networks”, in Proc. IEEE INFOCOM, pp. 1–6, Nov. 2008

[5] B. Bako, F. Kargl, E. Schoch, and M. Weber, “Advanced adaptive gossiping using 2-hop neighbourhood information,” in Proc. IEEE GLOBECOM , pp. 1–6, Dec 2008

[6] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah and Jamalul-lail bin Ab Manan “Classes of Attacks in VANET”, pp. 1-6, April 2011

[7] Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl “Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols” in EEE Transactions On Vehicular Technology, Vol. 62, No. 4, pp. 1505-1517, May. 2013

[8] Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, and Joseph Mouzna ” Mitigation of insider and outsider DoS attack against signature based authentication in VANETs”, pp. 152-157, Feb. 2014

[9] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li “Efficient Privacy Preserving Authentication for Vehicular Ad Hoc Networks” IEEE Transactions On Vehicular Technology, Vol. 63, No. 2, pp. 908-919, February 2014