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 4, April 2015

Key Based Authentication for Vehicular Adhoc Networks Using Relay Node

S.Subhashini[1], Dr .T.V.P Sundararajan[2]

Student, Dept. of ECE, Bannari Amman Institute of Technology, Sathyamangalam , Tamilnadu, India [1]

Professor, Dept. of ECE, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India [2]

ABSTRACT: Multicast is a crucial routine operation for vehicular networks, which underpins important functions such as message dissemination and group coordination. As vehicles may distribute over a vast area, the number of vehicles in a given region can be limited which results in sparse node distribution in part of the vehicular network. This poses several great challenges for efficient multicast, such as network disconnection, scarce communication opportunities and mobility uncertainty. In addition to security is added in order to avoid unwanted problems. The vehicles send information only to authenticated vehicles.

KEYWORDS: mobility uncertainty, authenticated vehicles

I.INTRODUCTION

In TMC, message forwarding metric is proposed to characterize the capability of A vehicle to forward a given message to a low speed while these assumptions are often invalid in a practical vehicular network. TMC is mainly used to exploit vehicle trajectories for efficient multicast in vehicular networks. The novelty of TMC includes a message forwarding metric that characterizes the capability of a vehicle to forward a given message to destination nodes, and a method of predicting the chance of inter-vehicle encounter between two vehicles based only on their trajectories without accurate timing information. TMC is designed to be a distributed approach. Vehicles make message forwarding decisions based on vehicle trajectories shared through inter-vehicle exchanges without the need of central information management group of destination nodes, which is defined as a vector of delivery potential of the message to each of the destination nodes. With this metric, a vehicle can simply forward a message to a vehicle that has a higher multicast delivery gain over the vehicle itself. The salient feature of TMC is that it is a fully distributed approach in which vehicle trajectories are shared through inter-vehicle exchange and a vehicle makes its message forwarding decision based on the trajectories it learns instead of relying on a central point for information management.

In this paper, it proposes key based authentication in which public key is set with the help of roadside unit. The Infrastructure Domain consists of the RSU‟s and the CA. The CA is connected to the RSU‟s and allow for the RSU to act as a proxy to the CA. Multi-hop communication is used between OBU‟s and RSU‟s when packets are forwarded from one OBU to another to reach the RSU. The public key is helps to find the number of vehicles within the communication range. After checking public key, the source node sends the private key to reach the destination node. The source node sends the data to relay node after checking public key. The source node sends the data to destination after checking private key. In which road side unit is placed to each trajectory for better communication and reduce the packet overhead.

II.RELATED WORK

A. MULTICAST ROUTING ALGORITHM

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other.In TMC, a novel message forwarding metric is proposed to characterize the capability of a vehicle to forward a given message to a group of destination nodes, which is defined as a vector of delivery potential of the message to each of the destination nodes. With this metric, a vehicle can simply forward a message to a vehicle that has a higher multicast delivery gain over the vehicle itself. To compute the metric, the key challenge is to predict the chance of encounter between two vehicles based only on their trajectories without accurate timing information.In this multicasting, the source node sends the data to multiple nodes with the help of relay nodes. The relay is nothing but intermediate node. With the help of intermediate node the nodes sends data to destination without any delay. But in this method lot of packet loss occurred without knowing destination. It randomly sends the data to destination. So, the occurrence of overhead is more.

III.PROPOSED METHOD

A. PUBLIC –PRIVATE KEY EXCHANGE

In this scheme, Public-key cryptography, also known as asymmetric cryptography. It requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used, for example, to encrypt plaintext or to verify a digital signature; whereas the private key is used for the opposite operation, in these examples to decrypt cipher text or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. In this key based authentication, both public key and private key is used in order to authenticate the message from unauthorised vehicles. In VANET, the public key mainly used to find the number of vehicles in the communication range. So, the number of vehicles in the communication range can be found easily. After finding the vehicles in the communication range the public key sends to another node, it converts plaint text to cipher text. Using the private key the authorised vehicles can able to convert the cipher text to plain text.

B. SECURITY

A certificate is an electronic document which uses a digital signature to bind a public key to an identity, ensuring authenticity of the certificate’s owner. In a (Public Key Infrastructure) PKI system, users communicate securely through use of a public-private key pair. The public key is known publically and the private key is kept secret. The public and private keys are mathematically linked, and even though the public key is known, it is infeasible to calculate the private key from the corresponding public key. The CA is the trusted authority in the network, and is responsible for handing out the initial authoritative information. The CA achieves this by wrapping the certificate with its private key, thus forming the CA’s signature on the certificate. The CA’s signature on a certificate ensures that only the CA could have signed the certificate, because only the CA holds the private key that created the certificate. The user is considered authentic once the user’s public key can be derived from the certificate and it can be verified that the node is who it claims to be. Authenticity requires that an identity is assigned to a vehicle in order to verify the source of a message and to hold the vehicle accountable for any malicious use. Privacy allows for a vehicle to communicate with other vehicles without disclosing its permanent identity. This is achieved by masking the vehicles permanent identity so that it is not known to other vehicles.

IV SIMULATION IMPLEMENTATION

A. NS2 (NETWORK SIMULATOR)

Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project. The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations.NS2 is developed as a collaborative environment. It is distributed freely and open source. A large amount of institutes and people in development and research use, maintain and develop NS2.This increases the confidence in it. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X..NS2 interprets the simulation scripts written in OTcl. A user has to set the different components (e.g. event scheduler objects, network components libraries and setup module libraries) up in the simulation environment. The user writes his simulation as a OTcl 12script, plumbs the network components together to the complete simulation. If he needs new network components, he is free to implement them and to set them up in his simulation as well. The event scheduler as the other major component besides network components triggers the events of the simulation (e.g. sends packets, starts and stops tracing). Some parts of NS2 are written in C++ for efficiency reasons. The data path (written in C++) is separated from the control path (written in OTcl).

B. SIMUALTION PARAMETERS

The parameters used in NS2 to create the simulation scenario are mentioned below

Table 1. Parameters used in NS2

PARAMETERS	CONFIGURATIONS
Protocol	DSR
Network interface type	PHY/Wireless PHY
number of nodes	50
Area	2000mX1200m
Simulation start time	0 sec
stop time	20 sec
Communication range	250m
Number of CBR	5
Public key	46

C. SIMULATION ENVIRONMENT

In simulation environment, the multicasting techniques are used. The one node act as the source node with the help of relay node sends the information to destination node. In which the RSU is placed to the trajectory for certificate authority.

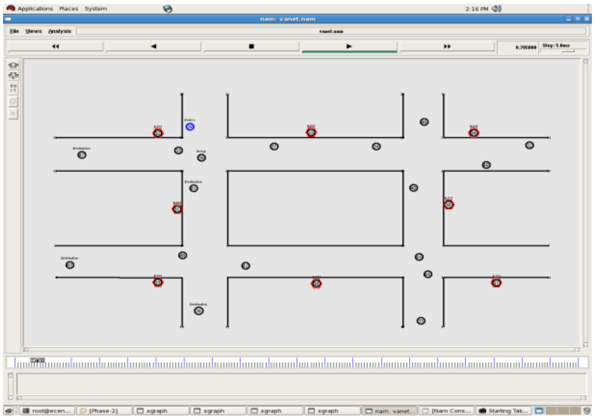


Fig 1. Multicasting performance

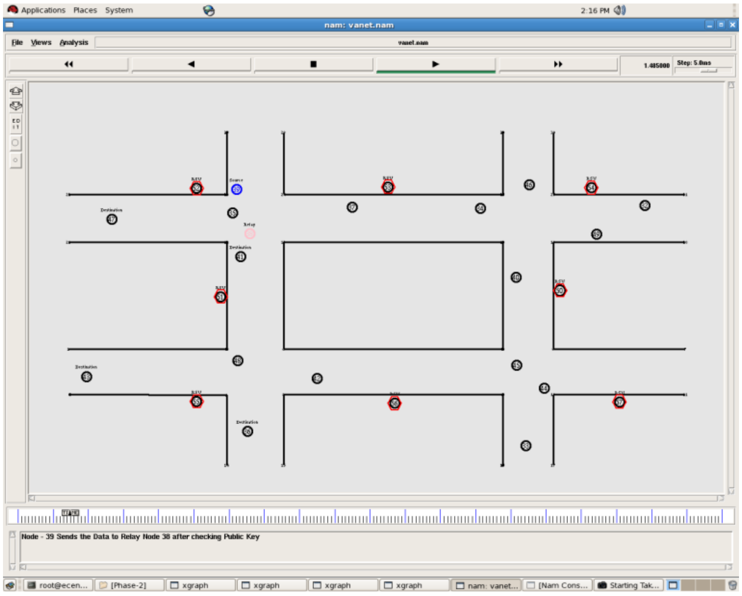
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

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

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

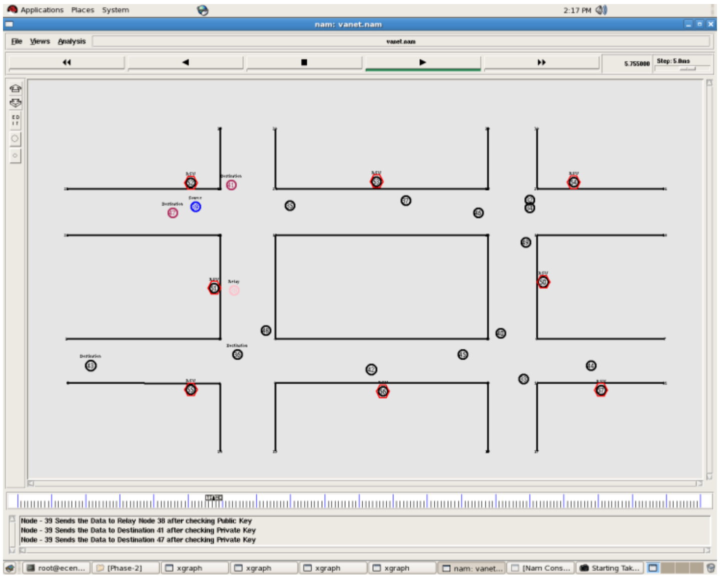
In fig 1. The multicasting performance is done, the node is mobile. The source node sends the information to destination. The start time is 0 sec and the total duration is 20 sec.



```
Node - 39 Sends the Data to Relay Node 38 after checking Public Key
```

Fig 2. Public key distribution

In fig 2. The source sends the message to relay node after checking public key. The source node 38 sends the data to relay node 39 after checking public key. The road side unit act as the proxy.



```
Node - 39 Sends the Data to Relay Node 38 after checking Public Key
Node - 39 Sends the Data to Destination 41 after checking Private Key
Node - 39 Sends the Data to Destination 47 after checking Private Key
```

Fig 3. Private key distribution

In fig 3. The source node sends the data or information to the destination node after checking private key. Thus the encryption and decryption is used in this process. The decryption process is used is implemented in this scenario.

D. SCENARIO ANALYSIS

In this scenario, throughput is calculated. Throughput is compared with encryption and without encryption. The number of packets delivered to destination is calculated.

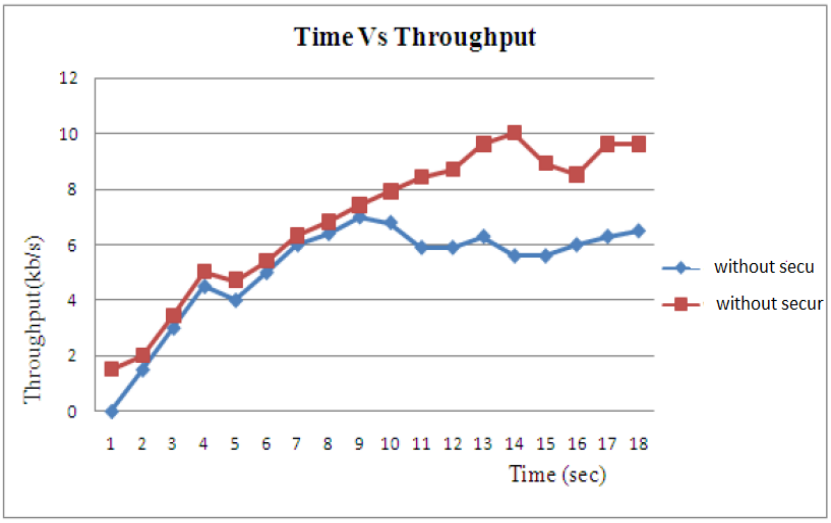


Fig. 1 Simulation time vs Throughput of receiving packets

In the fig 1, it shows the graph of time Vs throughput of receiving packet. Throughput is the average rate of successful message delivery over a communication channel.

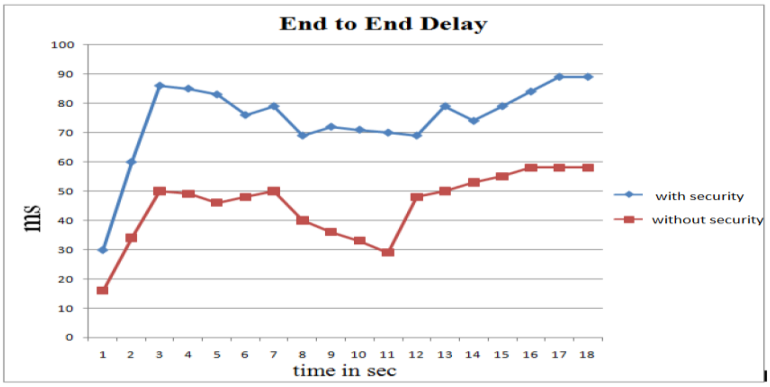


Fig. 2 time in sec vs ms

In the fig 2, it shows the graph time in sec vs. ms end to end delay. End to end delay is the time taken by a packet to travel from source to reach destination.

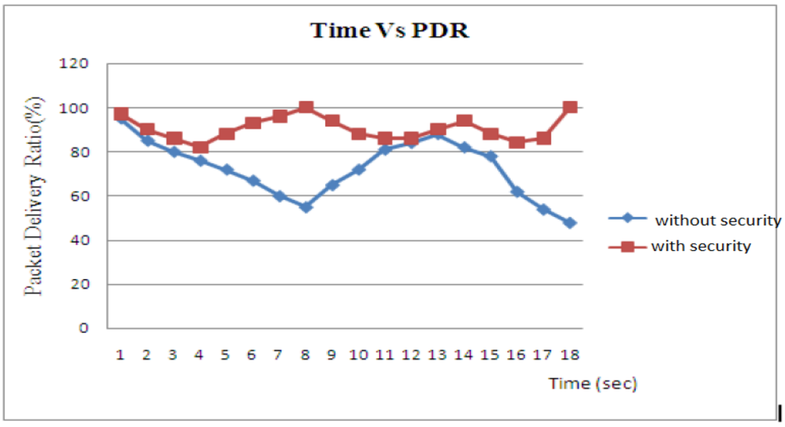


Fig .3 time in sec Vs packet delivery ratio (%)

In Fig 3, Time in sec Vs PDR. It is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination

V.CONCLUSION

VANETs are able to offer safe roads and convenient driving. Without privacy, plain authentication is not enough to maintain a secure system. Authentication alone allows for tracking and privacy alone does not provide for trust as the user is not authentic. Therefore, both authentication and privacy are necessary in a VANET

REFERENCES

[1] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, “Design of 5.9GHZ DSRC -based vehicular safety communication,” IEEE Wireless Communications, vol. 13, no. 5,
pp. 36–43,2006.
[2] Dedicated Short Range Communications (DSRC) home, http://www.leearmstrong.com/dsrc/dsrchomeset.htm.
[3] F. Farnoud and S. Valaee, “Reliable broadcast of safety messages in vehicular ad hoc
networks,” in Proc. IEEE INFOCOM, 2009, pp. 226–234. [4] T. Kitani, T. Shinkawa, N. Shibata, K. Yasumoto, M. Ito, and T. Higashino, “Efficient vanet-based traffic information sharing using buses on regular routes,” in Proc. IEEE VTC Spring. IEEE, 2008, pp. 3031–3036.
[5] D. Zhang and C. Yeo, “Enabling efficient wifi-based vehicular content distribution,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 3, pp. 479–492, 2013.
[6] A. Miloslavov and M. Veeraraghavan, “Sensor data fusion algorithms for vehicular cyber-physical systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp.1762–1774, 2012.