Security Protocol For Routing in VANET

Janhavi R. Chaudhary
Department of Information Technology,
LDCE, Ahmedabad, Gujarat, India

ABSTRACT

VANET is new kind of Ad hoc. It is widely used in ITS (Intelligent Transportation Systems), which has many characteristics as large scale network, fast moving nodes, the frequently changing topological structure and easily divided networks. Therefore, routing protocol design must fully consider of this characteristics with much node information that bring a great challenge to the security of VANET. In this paper, we divide the information type into four categories based on different content, and analyze the security threats in different information type, then summarize the existing security technologies and give the possible research directions.

Keywords—*VANET; RSA; Security Protocol.*

I. INTRODUCTION

Traffic congestion on the roads is today a large problem in big cities. The congestion and related vehicle accommodation problem is accompanied by a constant threat of accidents as well. Wirelesses access in vehicular environment (WAVE) is a multi-channel approach, reserved for one control channel from 5.855 to 5865 GHz, for high availability, low latency vehicle safety communications [1]. An enhancement was required on IEEE 802.11 standard to support applications from the Intelligent Transportation Systems (ITS) [2]. The 802.11p standard is meant for VANET communication and uses dedicated short range communications (DSRC) spectrum.

Fig. 1.Traffic conditions of different cities or country

VANET safety applications depend on the exchange of safety information among vehicles (C2C communication) or between vehicle to infrastructure (C2I Communication) using the control channel. RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission [5]. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. The RSA algorithm involves three steps: key generation, encryption and decryption. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key [7].

A. FEATURES OF VANET

- The nodes in a VANET are vehicles and road side units
- The movement of these nodes is very fast.
- The motion patterns are restricted by road topology Vehicle acts as transceiver i.e. sending and receiving at the same time while creating a highly dynamic network, which is continuously changing.
- The vehicular density varies from time to time for instance their density might increase during peak

office hours and decrease at night times.

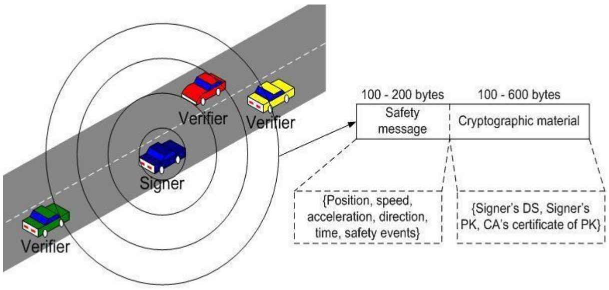
100 - 200 bytes
100 - 600 bytes
Safety message
Cryptographic material
Verifier
Verifier
Signer
Verifier
{Position, speed, acceleration, direction, time, safety events}
{Signer's DS, Signer's PK, CA's certificate of PK}

Fig.2. Encryption based VANET Architecture

VANET suffer from various attacks like Jamming, Node Impersonation Attack, Sybil Attack, Routing attack and different challenges like Message Authentication and Integrity, Message Non Repudiation, Message Confidentiality [3], Privacy and Anonymity, Liability Identification and Message fabrication, alteration, and replay can all be used towards impersonation.

II. PROPOSED METHOD

A. Encryption

When any RSU want to transmits public key (n, e) to vehicles and keeps the private key d secret. In RSU, first turns M into an integer m, such that 0 ≤ m < n by using an agreed-upon reversible protocol known as a padding scheme. Then computes the cipher text c corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done efficiently, even for 500-bit numbers, using Modular exponentiation. RSU then transmits c to vehicles.

B. Decryption

Vehicles can recover *m* from *c* by using private key exponent *d* via computing

$$m \equiv c^d \pmod{n}$$

Given *m*, recover the original message *M* by reversing the padding scheme.

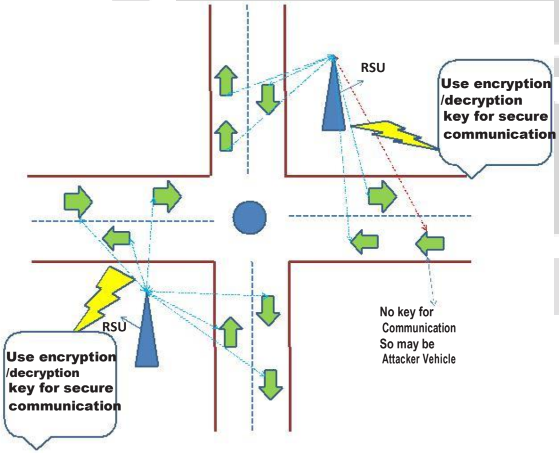
RSU
Use encryption /decryption key for secure communication
RSU
Use encryption /decryption key for secure communication
No key for Communication So may be Attacker Vehicle

Fig.4. Communication of vehicle to RSU

C. RSA Algorithm

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

- Choose two distinct prime numbers p and q. For security purposes, the integer’s p and q should be chosen at random, and should be of similar bit-length.
- Compute n = pq. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p + q -1), where φ is Euler's totient function.
- Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) are co prime. e is released as the public key exponent .e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as
  3) have been shown to be less secure in some settings.
- Determine d as d ≡ e−1 (mod φ(n)); i.e., d is the multiplicative inverse of e (modulo φ(n)). This is more clearly stated as: solve for d given dج e ≡ 1 (mod φ(n)). This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to e and φ(n), respectively. d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

III. VANET IMPLEMENTATION WITH RSU

A. VANET Simulation

The problem discussed in this section is ‘how VANET researchers are going to evaluate their proposed method. The ultimate evaluation tool is by doing outdoor experiments, but this solution has many drawbacks. Neither easy nor cheap to have a high number of vehicles in real scenarios especially in case of public safety related protocols. Difficult to analyze the performance in highly distributed environments like the case of VANETs. Impossible to compare between two protocols in the exactly same situation. Therefore, the only appropriate evaluation tool is by using simulation programs. Any simulation program consists of two complementary parts; network model and mobility model. The network model is responsible for identifying the communication stack; i.e. wireless channel model, antenna model, MAC layer, network layer, application layer and similar issues. The network model for VANET simulation programs is the same as that of MANET programs.

The mobility model is responsible for identifying different aspects of vehicle movement. It is the only new issue in VANET simulation programs. Vehicular mobility models are usually classified as being either microscopic or macroscopic models. When focusing on the macroscopic point of view, motion constraints such as roads, streets, crossroads and traffic lights are considered and the generation of vehicular traffic such as traffic density, traffic flows, and initial distribution of vehicles are defined. The microscopic point of view, instead, focuses on the movement of each individual vehicle and on the vehicle behavior with respect to neighbors such as lane changing and car following models. A realistic mobility model should include.

Accurate and realistic topological maps: Such maps should include different types of Roads that consist of different number of lanes. Intersections with traffic lights: Maps should contain intersection where vehicles should Slow-down. Vehicles are expected to react with traffic lights appropriately. Lane changing models: Drivers are not expected to still in their lanes for the entire Journey. Hence, lane-changing maneuvers should be included in the simulation. Smooth deceleration and acceleration: Since vehicles do not breakdown and accelerate abruptly, deceleration and acceleration models should be included. Obstacles.

The simulation should include obstacles in the vehicular mobility and the wireless channel. Intelligent driving patterns: Drivers interact with their environments, not only with respect to static obstacles, but also to dynamic obstacles, such as neighboring cars and pedestrians. Human behaviors: Drivers are humans not machines. All driving models should be probabilistic with a tolerance of errors which results in simulated accidents. Non-random distribution of vehicles: As it can be observed in real life, initial positions of vehicles are not uniformly distributed in the simulation area [10]. Different types of vehicles: The VANET technology is not addressed to sedan cars only buses, vans, trucks, trains and motorcycles are also involved. Each type should have its own models. Effect of the implemented protocol: Almost all mobility models are used to generate a predefined traffic prior to the simulation itself, without any effect of the implemented protocol. If the researcher wants to measure the net improvement of his protocol on the traffic flow, he must have a simulation program that allows changing of future Movements according to events from the network model.

IV. RESULT AND SIMULATION

Simulation of vehicle with RSU and encryption based security system was performed on MATLAB environment. Results show that RSA based security schemes involving Advance Encryption and Decryption domains are able to provide more security in vehicle ad-hoc network. After granting permission vehicle entering boundary where Road site unit also available, In this stage vehicle smoothly go on road or boundary.

V. CONCLUSION

Hence, RSA and AES key-management schemes for a VANET have been performed. From the results it has been shown that there is an increase in the efficiency of the system when there is a scheme in place. There is a considerable improvement in the data communication n between the nodes after key management techniques have been employed. After showing result it is found that the RSA algorithm is found to be the most efficient for the model used. All this has been proved on by simulation on the MATLAB. At critical security areas which are prone to attacks a key management technique is absolutely compulsory. Without it the delivery ratio becomes so less that there is no meaningful data communication possible. This technique can be used in security-sensitive applications like police and government agencies where VANETs are increasingly being used.

VI. REFERENCES

[1] M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5.doi: 10.1109/IC4.2015.7375676.

[2] L. Chen, H. Tang and J. Wang, "Analysis of VANET security based on routing protocol information," 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP), Beijing, 2013, pp. 134-138.doi: 10.1109/ICICIP.2013.6568055

[3] X. Y. Guo, C. L. Chen, C. Q. Gong and F. Y. Leu, "A Secure Official Vehicle Communication Protocol for VANET," 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan, 2016, pp. 482-485.doi: 10.1109/IMIS.2016.56

[4] A. Suman and C. Kumar, "A behavioral study of Sybil attack on vehicular network," 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, 2016, pp. 56-60.doi: 10.1109/RAIT.2016.7507875

[5] J. J. Haas, Y. C. Hu and K. P. Laberteaux, "Real-World VANET Security Protocol Performance," GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, Honolulu, HI, 2009, pp. 1-7. doi: 10.1109/GLOCOM.2009.5426188

[6] Liu Feng, Yang Xiu-Ping and Wang Jie, "Security transmission routing protocol for MIMO-VANET," Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, Changchun, 2014, pp. 152-156

[7] R. V. Alexandrescu, M. C. Surugiu and I. Petrescu, "Study on the implementation of protocols for providing security in average VANET intervehiculary network communication systems," 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, 2015, pp. WW-1-WW-6.doi: 10.1109/ECAI.2015.7301217.