Navdeep Kaur Randhawa / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp. 647-650

Design and Implementing PGP Algorithm in Vehicular Adhoc Networks (VANETs)

Navdeep Kaur Randhawa
(Department of ECE, GIMET, Amritsar(Punjab), India)

ABSTRACT
Vehicular ad hoc networks (VANETs) have attracted a lot of attention over the last few years. VANETs are being used to improve road safety .Many forms of attacks against VANETs have emerged recently that attempt to compromise the security of such networks. Such security attacks on VANETs may lead to catastrophic results such as the loss of lives or loss of revenue for those value-added services. Therefore making VANETs secure has become a key objective. For this PGP (Pretty Good Privacy) has emerged as an effective solution. The goal of PGP is to ensure privacy and strong authentication. PGP is a remarkable phenomenon that provides confidentiality, authentication, and compression for email and data storage.

I. INTRODUCTION
A Vehicular Ad-Hoc Network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres 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, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.
Vehicular Adhoc network (VANET) is a new form of Mobile Adhoc Network (MANET). It integrates mobile connectivity protocols to expedite data transfer between vehicles as well as between roadside equipment and available traffic in network. In VANET, Wireless device sends information to nearby vehicles, and messages can be transmit from one vehicle to another vehicle. Therefore, using VANET can increase safety and traffic optimization. Similar to other technology, in VANET there are some important and noticeable issues. One of the most important of them is Security. Since the network is open and accessible from everywhere in the VANET radio range, it is expected to be an easy target for malicious users. VANETs are new type of networks which are expected to support a large spectrum of mobile distributed applications that performed in vehicles. One of the most considerable services in VANET on the roads is that it can give drivers safety in driving. VANET can transmit useful information about road and traffic conditions as well as other noticeable information for people who drive in the range of the typical road. For example, if a car encounters a dangerous situation, then it can communicate with other cars and warn those cars which have not arrived at that place yet using Vehicle to Vehicle (V2V) communication.

II. BENEFITS OF ADHOC ARE MENTIONED BELOW
- Warning drivers about road conditions such as accidents or bad weather.
- Helping drivers to find the best available route to their destination.
- Enabling drivers to connect to internet while traveling within their cars.
- Enabling cars to establish communication between themselves by using capabilities of VANET provider infrastructure.
- If a car encounters problems, its driver can gain help using VANET-based network
- Vehicular networks over the Adhoc do not have critical situation in consuming computational and power resources, related to which are complicated issues in traditional Adhoc networks.
- Unlike Adhoc, in VANET there is the ability to use static infrastructure such as roadside base stations

The advancement and wide deployment of wireless communication technologies have revolutionized human lifestyles by providing the most convenience and flexibility ever in accessing Internet services and various types of personal communication applications. Recently, car manufacturers and telecommunication companies have been gearing up to equip each car with technology that allows drivers and passengers to communicate with each other as well as with the roadside infrastructure that may be located in some critical sections of the road, such as at every traffic light or any intersection or stop sign, in order to improve the driving experience and make driving safer.

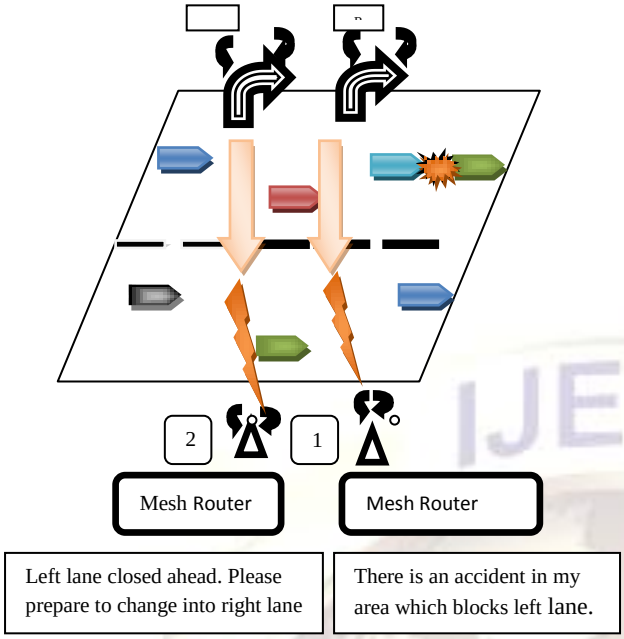


Fig:1 An example of road emergency response operation under VANET

III. APPLICATIONS OF VANETS

Mostly interests to MANETS belong to the VANETS but the features are different. Vehicles are likely to move in structured way. The connection with wayside equipment can similarly be indicated absolutely accurately. In the end, mostly automobiles are limited in their motion range, such as being controlled to pursue a paved way.

VANET suggests unlimited advantage to companies of any size. Vehicles access of fast speed internet which will change the automobiles' on-board system from an effective widget to necessary productivity equipment, making nearly any internet technology accessible in the car. Thus this network does pretend specific security concerns as one problem is no one can type an email during driving safely. This is not a potential limit of VANET as productivity equipment. It permits the time which has wasted for something in waiting called "dead time", has turned into the time which is used to achieve tasks called "live time".

If a traveler downloads his email, he can transform jam traffic into a productive task and read on-board system and read it himself if traffic stuck. One can browse the internet when someone is waiting in car for a relative or friend. If GPS system is integrated it can give us a benefit about traffic related to reports to support the fastest way to work. Finally, it would permit for free, like Skype or Google Talk services within workers, reducing telecommunications charges.

IV. SCOPE

The most favorable target is the more useful, efficient and safer roads will built through vehicular networks by informing to basic authorities and drivers in time in the future. Another target is to discover the advancement of vehicular ad hoc networking (VANET) wireless technologies.

V. BENEFITS OF VANETs

- Congestions : Reduced
- Accidents are avoided
- Improved Entertainment
- WIFI access
- Online Music
- Real time position
- Find restaurants

VI. VANET BASIC RISKS

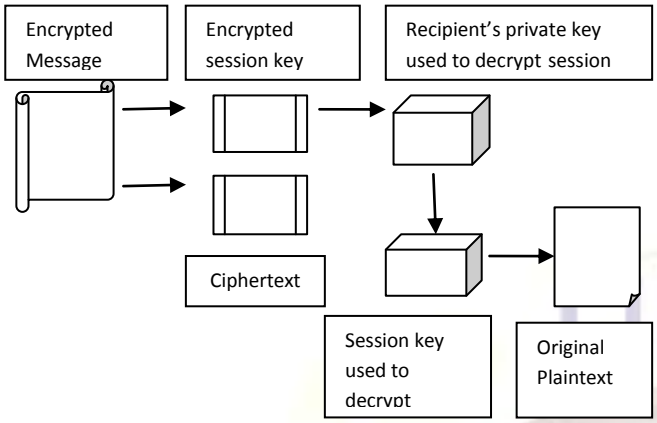
Unfortunately, there is some bad news about VANET. In VANET, there are some problematic issues most of which are flied around security issues such as data integrity, privacy, and confidentiality. Moreover, there are some issues which can influence the efficiency of VANET such as unpredictable temporary situations (e.g. creating traffic jam because of an accident). The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. It is necessary that all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. These problems in VANET are difficult to solve because
of the network size, the speed of the vehicles, their relative geographic positions, and the randomness of the connectivity between them. There is a classification of three major groups of behavior of attackers:

• Insider versus outsider
• Malicious versus rational
• Active versus passive

- **Insider vs. Outsider.** The insider is an authenticated member of the network that can communicate with other members. As will be explained later, this means that he possesses a certified public key. The outsider is considered by the network members as an intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

- **Malicious vs. Rational.** A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and

consequences. On the contrary, a rational attacker seeks personal profit and hence is



more predictable in terms of the attack means and the attack target.

- **Active vs. Passive.** An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

As the security threats and attacks can be exploited in VANETs, so the security solutions must be implemented to thwart those attacks. For this by applying PGP encryption algorithm (128 bits) security on VANET can be increased.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communication. PGP encryption applications include e-mail and attachments, digital signatures, laptop full disk encryption, file and folder security, protection for IM sessions, batch file transfer encryption, and protection for files and folders stored on network servers and, more recently, encrypted and/or signed HTTP request/responses by means of a client side and a server side.

VII. HOW PGP ENCRYPTION WORKS?

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression, among other things, strengthens crypto graphic security because it reduces the patterns found in languages. PGP then creates a session key. The session key works with a very secure, fast conventional (symmetric) encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key, This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

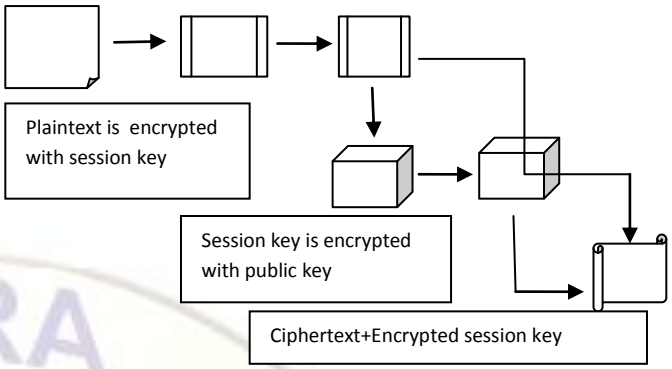


Fig:2 PGP ENCRYPTION

Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the session key, which PGP then uses to decrypt the conventionally (symmetrically) encrypted cipher text.

Fig3:PGP DECRYPTION

VIII. PROBLEM DEFINITION

64 bit encryption indicates that the size of the key used to encrypt the message is 64 bits. 64-bit encryption standard was used in some early Internet and wireless communication encryption algorithms such as DES and WEP. Unfortunately, 64-bit encryption has proved too easy to decipher or crack in practice. Now, 128-bit encryption (for example PGP encryption) have replaced the 64-bit encryption keys (DES).

As the security threats and attacks can be exploited in VANETs, so the security solutions must be implemented to thwart those attacks. For this by applying PGP encryption algorithm (128 bits) security on VANET can be increased.

IX. METHODOLOGY USED

As in figure 4 given below various nodes(let say 2-6), with two stations:

STATION 1 and STATION 2, interact with each other over wireless network and every node or any node can act as malicious node in network. Malicious node is basically attacker's node that can alter or destroy the actual message while two stations are interacting with each other.

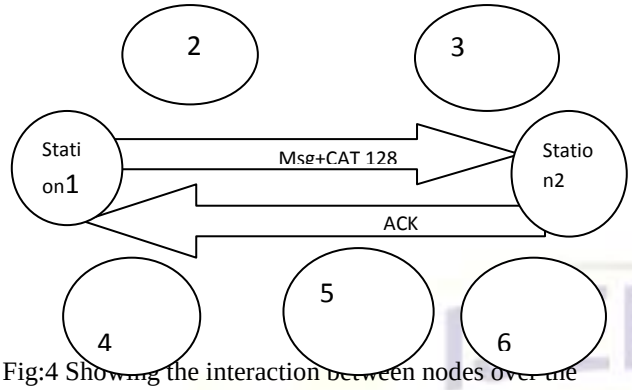


Fig:4 Showing the interaction between nodes over the network

So in order to protect the message (or its contents) from being altered or destroyed, PGP(Pretty Good Privacy) encryption is used.PGP basically provides: Compatibility, Confidentiality, Digital Signatures, Certificates.

X. RESULTS AND DISCUSSION

Security is implemented over VANET with PGP(Pretty Good Privacy) algorithm. It provides end to end connectivity. And messages can be send successfully between sender and receiver without any interruption.PGP algorithm(128 bits) is implemented for security, which is faster as well as secure than previously implemented algorithms.

REFERENCES

[1]"VANET",http://en.wikipedia.org/wiki/Vehicular_ad-hoc_network.

[2] Farzad Sabahi "The Security of Vehicular Adhoc Networks",presented at Third International Conference on Computational Intelligence, Communication Systems and Networks,2011

[3] A. Hamieh, et al., "Detection of radio interference attacks in VANET," presented at the GLOBECOM,NJ, 2009.

[4] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho,and Xuemin (Sherman) Shen, University of Waterloo "Security in Vehicular Ad Hoc Networks",2008.

[5] What is Vanet-applications of Vanet http://www.wifinotes.com/mobile-communication-technologies/what-is-vanet.html.

[6] Wenmao Liu Harbin Institute of Technology China "An autonomous road side infrastructure based system in Vanets".

[7] Xiaonan Liu, Zhiyi Fang, Lijun Shi, "Securing Vehicular Ad Hoc Networks",2007

[8]" PrettyGood Privacy", http://en.wikipedia.org/wiki/Pretty_Good_Privacy.

[9]"PrettyGoodPrivacy",http://en.wikipedia.org/wiki/Pretty_Good_Privacy#PGP_Corporation encryption_applications.

[10] "PGP: A Hybrid Solution", http://www.sans.org/reading_room/whitepapers/vpns/pgp-hybrid-solution_717.

[11]" Pretty Good Privacy", http://en.wikipedia.org/wiki/Pretty_Good_Privacy#PGP_Corporation encryption_applications.

[12]" PrettyGood Privacy", http://en.wikipedia.org/wiki/Pretty_Good_Privacy#Compatibility

[14]" Pretty Good Privacy", http://en.wikipedia.org/wiki/Pretty_Good_Privacy#Digital_signatures

[15] " Pretty Good Privacy", http://en.wikipedia.org/wiki/Pretty_Good_Privacy#Certificates

[16] Wenmao Liu Harbin Institute of Technology China "An autonomous road side infrastructure based system in Vanets".