AN ENCRYPTION ALGORITHM TO EVALUATE PERFORMANCE OF V2V COMMUNICATION IN VANET

Manpreet Kaur1, Rajni2 and Parminder Singh3

1Department of Electronics & Communication, Research Scholar, S.B.S.S.T.C, Ferozepur
er_rimi@rediffmail.com
2Assistant Professor, S.B.S.S.T.C, Ferozepur
rajni_c123@yahoo.co.in
3Senior Lecturer, Chandigarh Group of Colleges, Landran
Singh.parminder06@gmail.com

ABSTRACT

Wireless Communications are gaining more importance because they have opened new research fields by extending data networks connectivity to environments where wired solutions are difficult to install. The networks which are deployed in the areas where the needed infrastructure is not feasible to install are adhoc networks. Mobile Adhoc Networks (MANETs), in which each node acts as both data terminal and router uses wireless medium without the need of any centralized control. Vehicular Adhoc Networks (VANETs) are subset of MANETs. The successful deployment of vehicular communication requires Vehicle-to-Vehicle (V2V) & Vehicle-to-Infrastructure (V2I) communication with security to improve road safety and optimize road traffic. The technique used for secure communication in the presence of adversaries is known as cryptography. Cryptography refers to encryption in which a plaintext message is converted into a ciphertext and this can be done with private-key or public-key. In this paper, an algorithm based on private key encryption is used to make communication possible between two people with QualNet simulator.

KEYWORDS

Mobile Adhoc Networks (MANETs), Vehicular Adhoc Networks (VANETs), Intelligent Transport System (ITS), Security, Vehicle-to-Vehicle (V2V), Vehicle –to-Infrastructure (V2I).

1. INTRODUCTION

The process in which exchange of information via some transmission media takes place is known as network. VANETs are used for V2V and V2I communication considering all the aspects required by the process of cryptography. In Safety and non-safety applications of VANET, there is a requirement of V2V & V2I communication.

B.Karp in 2000 [1] discussed Greedy Perimeter Stateless Routing (GPSR) scheme in which the default packet forwarding strategy is the greedy strategy, where the sender selects the closest vehicle to the destination as the next hop. If the sender cannot find a forwarder based on the greedy strategy, it forwards the packet around the perimeter of the region containing itself and the destination. Giuseppe Ateniese in 2005 [2] presented a new re-encryption schemes that realizes a stronger notion of security and demonstrated the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Maxim Raya in 2006 [3] described the security problems of the emerging vehicular networks and it outlined the solution architecture and several

DOI:10.5121/ijcis.2013.3202
of its components. Tim Leinmüller in 2006 [4] aimed to define a consistent & future-proof solution to the problem of V2V/V2I security by focusing on SEVECOM (Secure Vehicle Communication). Pandurang Kamat in 2006 [5] proposed a security framework for vehicular networks using Identity-Based Cryptography (IBC), that provides authentication, confidentiality, message integrity, non repudiation and pseudonymity.

Xiaonan Liu in 2007 [6] described an Intelligent Transport System (ITS) which can be used under the security pattern to provide the appropriate solving measures in concern with the security issues of VANETs from some aspects. Department for Transport in 2008 [7] concluded that it had been seen from various studies that the number of lives lost in motor vehicle crashes worldwide every year is by far the highest among all the categories of accidental deaths. P. Caballero-Gil in 2009 [8] analyzed the features of inter-vehicle and vehicle-to-roadside communications to propose differentiated services for node authentication, according to privacy and efficiency needs. Zuowen in 2010 [9] proposed an improved privacy-preserving mutual authentication protocol for vehicle ad hoc networks by using secure identity-based group blind signature, the private encryption system and the public encryption system. Surabhi Mahajan in 2010 [10] discussed a comparison between the two schemes that are used to reduce the overhead in authentication, when roaming – proxy re-encryption scheme and new proxy re-encryption scheme. Hatem Hamad in 2010 [11] proposed a new method of message security by using the coordinates in GPS (Global Positioning System) service.

Sandhaya Kohli, Bandanjot Kaur in 2010 [12] discussed that vehicular adhoc networks are subclass of mobile adhoc networks which provides a distinguish approach for intelligent transport system (ITS). The survey of routing protocols in VANET is important and necessary issue for smart ITS. The proposed work discusses the advantages and disadvantages of these routing protocols. Umar Farooq Minhas in 2011 [13] described an important methodology required to enable effective V2V communication via intelligent agents. Nizar Alsharif in 2011 [14] explained that the reliability of position-based routing (PBR) in VANETs is ensured by proposing a set of plausibility checks that can mitigate the impact of PBR attacks without extra hardware requirement.

2. SECURITY CHALLENGES

The necessities required to provide security in VANETs are:

1. Authentication: An authentication framework is necessary to identify and ensure that the participants are whom they claim to be to operate securely in VANETs.
2. Integrity: Integrity is required between two communicating nodes to protect data accuracy which is main security issue desirable in VANETs.
3. Confidentiality: The challenge to protect data content from the adversaries is confidentiality.
4. Non-Repudiation: Non-Repudiation refers to somebody who possesses the private key corresponding to the signing certificate with reasonable certainty but if the key is not properly safeguarded by the original owner, a major concern can be digital forgery.
5. Pseudonymity: Pseudonymity is the state of describing a disguised identity. A holder that is one or more human beings are identified but don’t disclose their true names.
6. Privacy: The protection of personal information of drivers within the network from other nodes but extracted by authorities in case of accidents is a major privacy issue which is desirable for VANETs.
7. Scalability: The ability of a network to handle growing amount of work in a capable manner securely is Scalability, which is the main challenge in VANETs.
8. Mobility: The nodes communicating in VANETs constantly change their locations with different directions and speeds making the network dynamic in nature. So, in order to make communication successful, it is challenging to establish security protocols.

9. Key-Management: The key is used to encrypt and decrypt information during communication process. When designing security protocols for networks like VANET, the issue of key management must be resolved.

10. Location-verification: This is necessary to prevent many attacks and is helpful in data validation process. Thus to improve the security of VANETs, a solid method is required to verify the nodes positions.

3. SCENARIO USED

The choice of algorithm should be dictated by the purpose of the encryption when encryption is implemented. Private Key encryption is used because it is faster than public key encryption. However, private key encryption does not provide for digital signatures or the signing of information. It is also important to choose well-known and well-reviewed algorithms. Such algorithms are less likely to include back doors that may compromise the information being protected.

The security policy should define acceptable encryption algorithms for use within the VANET System. The security policy should also specify the required procedures for key management. In order to successfully gain access to the information transmitted over the VANET, an attacker must capture the entire session and use a substantial amount of computer power and time to brute-force the key and decrypt the traffic. Unless the information is extremely valuable, any well-known, strong algorithm is appropriate for use in the VANET System.

4. ALGORITHM DESCRIPTION

The Algorithm implemented here in VANET system in a straight road is Private Key Encryption in which i and j remain secret. Vehicles V1 and V2 are assumed so as to communicate securely and thus need to agree on an encryption key.

1. V1 and V2 agree on two large integers a and b such that 1 < a < b.
2. V1 then chooses a random number i and computes I = a_i mod b. V1 sends I to V2.
3. V2 then chooses a random number j and computes J = a_j mod b. V2 sends J to V1.
4. V1 computes k1 = I_j mod b.
5. V2 computes k2 = I_i mod b.
6. We have k1 = k2 = a_{ij} mod b and thus k1 and k2 are the secret keys to use for the other transmission.
5. IMPLEMENTATION TOOL

The performance results have been evaluated using QualNet Simulator. QualNet is network evaluation software, which is written purely in C++ and is entirely modeled as Finite State Machine (FSM). It can run on a variety of operating systems like UNIX, Windows, MAC and Linux. It is equipped with an extensive range of libraries for simulating a variety of networks. The architecture of QualNet comprises of Application, Transport, Medium Access Control (MAC), Physical layer. A unique capability for accurate, efficient simulation of large-scale, heterogeneous networks can be provided by the features of QualNet. A robust set of wired and wireless networks can be simulated by QualNet. ITM (Irregular Terrain Model) can be supported with the QualNet. QualNet executes scenarios 5-10x times faster than commercial alternatives.

6. RESULTS AND DISCUSSIONS

In this paper, the different results have been evaluated using QualNet simulator. The results shown indicate that the packet is sent between sender and receiver by using private key encryption algorithm. This means the same key is used for encryption and decryption. This leads to increase in throughput with reduce delay.

![Figure 2. First packet received during transmission.](image)

From the figure 2, we have measured the throughput of moving Vehicles communicating with each other via Access Point (A.P) already shown in figure 1. V1 Communicates with V2 via Access Point which leads to the calculation of the throughput of V1. From the Figure1, when the communication starts between AP and V2 then the throughput of first packet is calculated at its arrival. The first packet arrives from V1 having Node ID 1=2.8 seconds. The simulation carried from the help of QualNet Simulator and the length of Packet = 1024 Bytes.

From the Figure 3, the throughput of Last Packet received by the AP from V1 (called Source Node) =100 Seconds approximately is calculated. After the Packet is received, the Vehicle Node sends the termination signal to do end of communication between two Vehicles with the Base Station (AP) Node.
The figure 4 represents the Throughput of Two Nodes with AP by applying Security Algorithm and also calculates the speed at which the two vehicles move when sharing the data. The speed at which the Vehicles move was 60m/s with a packet size of 1024 Bytes and approximately calculated value was 4200bits/s.
The average end-to-end delay in a VANET means that the source node (V1) sends packet to destination Node (V2) and total average time to reach the packet to destination Node. In this Figure 5 the total average time was 0.007 seconds approximately. This delay was due to retransmission and applying security Algorithm at 802.11 networks.

The signal transmission in between node to node or vehicle to vehicle has been shown in the Figure 6. This has been shown that each node sends packet to the other node and the sequence number updates. This way the vehicles communicate at the transport layer when the transmission starts between both ends.
7. CONCLUSION

Security measures guarantees that the transmissions of data are authentic that is data is accessible only by authorized parties. The security techniques can be applied to vehicular users in Vehicular Adhoc Networks. The algorithm used in the paper is private key encryption in which sender and receiver communicate securely with the help of encryption key. The algorithm reduces delay, increases throughput, provides authentication and higher security level in VANETs.

8. FUTURE WORK

The solution of the security problems is discussed (by the use of algorithm) that are encountered in VANET. The performances of data transmission in VANETs can be tested by applying more encryption algorithms to provide more security with increased throughput and reduced delay.

REFERENCES

[1] Karp B, Kung H T (2000) GPRS: Greedy Perimeter Stateless Routing for wireless networks. Proc 6th Annual Int Conf on Mob Computing and Netw: 243-254.
[2] Ateniese G, Fu K, Green M, Hohenberger S (2005) Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. Proc of the 12th Annual Netw and Distributed Syst Security Symp: 29-44.
[3] Raya M, Papadimitratos P, Hubaux J P (2006) Securing Vehicular Networks. J IEEE wirel commun.
[4] Leinmuller T, Buttyan L et al (2006) SEVECOM-Secure Vehicle Communication. Proc of IST Mob Summit.
[5] Kamat P, Baliga A, Trappe W (2006) An Identity-Based Security Framework for VANETs. Proc of the 3rd Int workshop on Vehicular adhoc netw: 94-95.
[6] Liu X, Fang Z, Shi L (2007) Securing Vehicular Ad Hoc netw.IEEE.
[7] Department for Transport (2008) Reported road casualties Great Britain: 2008 Annual Report. Road Casualties G. B. UK.
[8] Caballero-Gil P, Hernandez-Goya C, Fuster-Sabater A (2009) Differentiated Services to Provide Efficient Node Authentication in VANETS.
[9] Zuowen, Tan (2010) A Privacy-Preserving Mutual Authentication Protocol for Vehicle Ad Hoc Networks. J of Convergence Inf Technology.
[10] Mahajan S, Jindal A (2010) Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks.Int J of Convergence Applications.
[11] Hamad H, Elkoud S (2010) Data Encryption using the dynamic location and speed of mobile node. J Media and Commun Stud: 067-075.
[12] Sandhaya, Bandanjot ", A comparative Study of Routing Protocols in VANET", ISCE 10, pp.173
[13] Minhas U F et al (2011) A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks. IEEE:407-20.
[14] Alsharif N, Wasef, Shen X (2011) Mitigating the effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks. IEEE ICC Proc.
AUTHORS

MANPREET KAUR is B.Tech in Electronics & Communication Engineering (2009) from AIET, India. She is pursuing M.Tech in Electronics & Communication Engineering from SBSSTC, India. Her research interests are Wireless, Networks, Adhoc Networks, etc.

Ms. Rajni is currently Assistant Professor at SBSSTC, Punjab, India. She has completed her M.E. from NITTTR, Chandigarh, India, B.Tech from NIT, Kurukshetra, India. Ms. Rajni has about fourteen years of academic experience. She has authored a number of research papers in national, international conferences and reputed journals. Her areas of interest includes Wireless communication, and Antenna design.

Parminder Singh is B.Tech in Information Technology (2006) from Punjab Technical University, India. He has done M.Tech in computer science and Engineering from Punjab Technical University, India. His research interests are TCP/IP, Wireless, Networks issues, etc.