ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

A novel approach for key rehabilitation using modified WEP algorithm for VANETs

Viswanatham Subbaiah[1], Arathi R Shankar[2], Bhargav Raman S[3]

M.Tech, Digital Communication, E & C Department, BMS College of Engineering, Bangalore, India[1]

Associate Professor, E&C Department, BMS College of Engineering, Bangalore, India[2]

Team Lead-i Sense, CSE Department, Nihon Communications Solutions Pvt Ltd, Karnataka, India[3]

Abstract: Communication between vehicles plays a major role in avoiding accidents at crowded areas. Security of the data to be communicated is another aspect to be thought of. In this paper authors have made an attempt to establish secure communication within a VANET network using IEEE standard 802.11p protocol which covers 1000 meters range. Authors have proposed a novel approach to ensure more security with which a 40% more secure VANET network can be realized.

Keywords: WEP, security, VANET, 802.11p.

INTRODUCTION

Vehicular Ad-Hoc Network is a one type of MANET in which vehicles will act as a nodes and each node is capability of transmission of data which are interconnected to form a network .The topography created by the nodes will be dynamic and have significantly non uniform distribution. Transfer of information in VANET is not effective with existing algorithms of the MANET.The interconnection of between the vehicles helps to know of its geographic location as well as that of the neighbours. Data Transmission is possible between vehicles if they are within the VANET. The developments in the VANET will support number of wireless products that can now be used in vehicles. The ITS (Intelligent Transport System) proposed the WAVE (Wireless Access in Vehicular Environment) which defines an architecture that enables both V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). [1]

Features of VANET

VANETs has its own unique- characteristics.

1) Predictable mobility: compared to other types of MANET networks the VANET will differbecause vehicles should be followcertain conditions like traffic signals, respond for other vehicles and hence their mobility is predictable to some extent.
2) VANETs provide vehicle to vehicle and vehicle to infrastructure communication there by enhancing traffic efficiency.
3) There are no power constraints in VANETs, hence no need to provide any external power supply for the OBU (On Board Unit). It will be provided from battery of the vehicle.
4) Traffic densities can vary with respect to location and time[2].

Challenges and requirements in VANET

Challenges or issues of VANET network can be of two categories i.e. safety and non-safety.

- Signal fading: Fading of the signal during transmission of data vehicle to vehicle or vehicle to infrastructure can lead to loss of information. This factor is predominant in the case of urban regions.
- Bandwidth limitations: VANETs do not have any central coordinator which is responsible for the communication between the vehicle, handling the bandwidth, and connection between the vehicles is difficult to maintain. Bandwidth utilization and latency issues become significant.
- Security is one of the critical parameters in VANET, hence good security protocols are required.
- Due to high mobility and random changes in the network topology efficient routing protocol is very essential so that packet loss is minimized.

VANET Applications

The communication between the V2V and V2I allows the improvement on more number of applications and it will be provide exact information to drivers and travellers. The different types of devices like OBU, AU (Application Unit), RSU (Road Side Unit),various sensors and GPS receivers are capable to gather information that belongs to present node as well as neighbour nodes. This will be provide safety and trust information for passengers and travellers. VANET applications are categorized into mainly.

1) Comfort applications: It will mainly consider about the passenger or traveller'scomfort by providing information like nearest petrol station, hotels and restaurants and there prices.
2) II .Safety applications: These avoid accidents by guiding the vehicles into safety path by using communication between the V2V and V2I mode. This application will gather data from one node and pass that information to other nodes and provide safety while transmitting the data.

DOI 10.17148/IJARCCE.2015.44120

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Wireless technology has becomean integral part of our daily life. The main purpose of these technologies will be reduce the cost and provide mobility to the users. It is better to have more data privacy while transmitting the data. Wireless Equivalent Privacy (WEP) is a security protocol specified in IEEE Wireless- Fidelity (Wi-Fi) standard 802.11 that is designed to provide security and privacy. However, the WEP has "major security flaws". WLAN using this protocol is vulnerable to attacks. In this paper we proposed an algorithm to patch WEP protocol against these attacks[3].

THE PROBLEM STATEMENT

WEP uses RC4 encryption algorithm [4], which operates by expanding a short key into an infinite pseudo-random key stream. If an attacker flips a bit in the cipher text, then upon decryption, the corresponding hit in the plaintext will be flipped. If an eavesdropper intercepts two cipher text encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts.

The statistical attacks become increasingly practical as more cipher text that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others. Toensure that a packet has not been modified, WEP uses, an Integrity Check Value (ICV) field in the packet. To avoid encrypting two cipher text with the same key stream, an initialization vector (IV) is used to augment the shared key and produce a different RC4 key for each packet. The major attacks to WEP are given as follows:

1) Active attack Modification of the packet by modifying the ICV.
2) Passive attacks
a) Integrity violation by analysing the IV
b) Table based attack for decrypting every packet that is sent over the wireless link.

In order to avoid attacks these attacks, in [4] the author propose algorithm, which randomize the data from the unauthorized user by adding some standard randomness to it. This random characteristic is a function of the private attribute shared between transmitter and receiver only. In this approach therandomness is achieved by RC4 algorithm and distribution of randomness is provided with different algorithms to increase the complexity of rectifying the encrypted data and optimize utilization of randomness.

PROPOSED METHOD

Authors have proposed a method called as Modified WEP, where a random octet is inserted in a random position. The random position is obtained by RC4 as a function of the secret key. Currently, the octets contain random information. Octet insertion as shown in Fig.2 is applied to IV field in the packet format. IV uses one RC4 key-stream octet, to find random position for insertion of random octet.

Algorithm: IV randomization / extraction
a. Fetch packet number and IV from 802.11 protocol
b. Fetch random data content for the octet from memory
c. Calculate random position
d. Insert the octet at the calculated random position

IMPLEMENTATION

The proposed algorithm was implemented using Visual C++ to verify the functionality at the system level. Furthermore, the algorithm was behaviourally modelled in EXATA (Emulator tool) to obtain simulation and verification. Random insertion positions in above test simulation are calculated by the process specified above.

Results and Analysis

Scenario

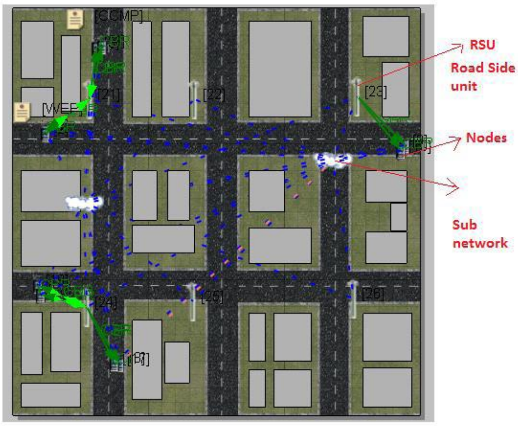

Fig 1: Simulation Scenario

The above Scenario depicts a VANET network with two sub networks, RSU (Road Side Unit) s and nodes. It will specify the way of communication take place between the nodes.

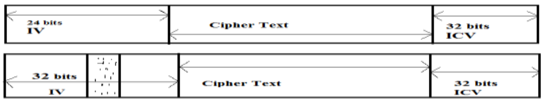

Figure 2: Structure of WEP and modified WEP

The above Figure 2 represents about the normal structure of WEP and the modified WEP in which eight bit random data is inserted.

Number of packets Encrypted

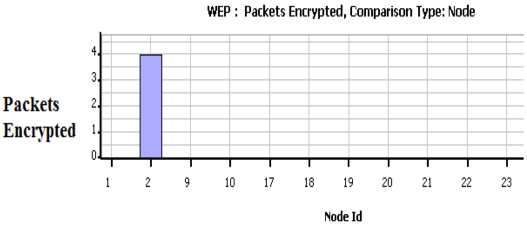

Figure 3: Number of packets Encrypted

The above figure will represent the total number of packets encrypted at node 2 which acts as a transmitter node.

DOI 10.17148/IJARCCE.2015.44120

Number of packets Decrypted

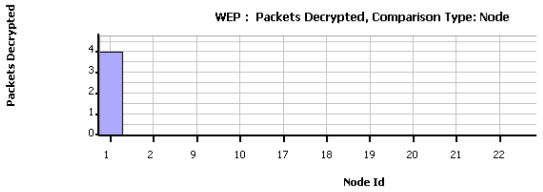

Figure 4: Number of packets Decrypted

The above figure will represent the total number of packets decrypted at node 1 which acts as a receiver.

PERFORMANCE IMPROVEMENT WITH MODIFIED WEP

Insertion of an 8-bit random octet in 24-bit IV at any random position, obtained from Calculate-random position function, results in 6,144 (24*28) different patterns of the same IV. This means an attacker needs to analyse 6,144 more patterns to decrypt the message in case of an IV collision .Thus, the improvement in security is 6,144 times for IV based attacks.

CONCLUSION AND FUTURE WORK

The implementation of MWEP algorithm has led to enhanced security. The complexity of decryption is increased by inserting one more random octet into the ICV field so that the complexity will increase and more security is provided.

Thus the algorithm provides a robust WEP security system without increasing the overall implementation cost.

ACKNOWLEDGEMENT

The authors would like to acknowledge to BMS College of Engineering, NIHON COMMUNICATION Pvt Ltd for rending full support to execute the project work and TEQIP II for their support and financial assistance rendered during the tenure of this project work.

REFERENCES

[1]. Manpreet Kaur, Rajni and Parminder Singh “New proxy re-encryption method to evaluate performance of v2v communication in a straight road scenario”. 20-21 Sept. 2013.pp 84 - 90

[2]. YaseerToor et al., “Vehicle Ad Hoc Networks: Applications and Related Technical issues”, IEEECommunications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3, pp. 74-88.

[3]. Y. - C. Hu and K. Laberteaux, “Strong Security on a Budget,” Wksp. Embedded Security for Cars, Nov. 2006;

[4]. Maxim Raya e al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005, Alexandria, Verginia, USA, pp.

[5]. Hannes Hartenstein et al., “A tutorial survey on vehicular Ad Hoc Networks”, IEEECommunication Magazine, June 2008, pp.

[6]. Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and computing, 2010.

[7]. Aaron E. Earle, “Wireless Security”, Handbook, 2006.

DOI 10.17148/IJARCCE.2015.44120