JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

An Id-based Authentication Scheme With A Focus On Impersonation And Modification Attack On VANET

Nischitha. S.B[1*], Shubha Bhat[2]

[1]Computer Science and Engineering, Dayananda Sagar College of Engineering, Autonomous, Bengaluru, India
[2] Computer Science and Engineering, Dayananda Sagar College of Engineering, Autonomous, Bengaluru, India

*Corresponding Author: nisha3377@gmail.com, Tel.: +918904549039

Available online at: www.ijcseonline.org

Accepted: 06/Jul/2018, Published: 31/Jul/2018

Abstract: VANETs (Vehicular Ad Hoc Networks), are similar to MANETs (Mobile Ad Hoc Networks) in which the nodes are vehicles. The vehicles exchange messages among themselves and these messages could be regarding the traffic status on road or the condition of the vehicle. The messages could get tampered by an adversary who wishes to gain the information regarding the vehicle. He could also track the vehicle which would violate the driver's privacy. Hence these messages have to be secured. The adversary could modify the messages which could vary the exact information sent by the vehicle; also he could impersonate as an authorized user and tamper the information. The aim is to protect the vehicle against the two attacks; modification attack and impersonation attack. The energy consumed by the source node to send it towards the destination is calculated.

***Keywords*—**VANET, modification, impersonation, energy

I. INTRODUCTION

Vehicular ad hoc networks are a variant of mobile ad hoc networks where the nodes are vehicles. They exchange the messages among themselves regarding the traffic status, vehicle's condition, weather condition and so on. The communication is aided through the OBUs (On Board Units) which will be equipped inside the VANETs. There are two types of communication which take place between VANETs; vehicle to vehicle communication and vehicle to infrastructure communication. Here the infrastructure role is played by the RSU (Road Side Unit) placed near the ends of the road and which will communicate with the vehicles through the OBUs. This communication is done through the internet. The control centre holds the information about every node and is always active. The RSU will send the information regarding the traffic status to the traffic control centre which in turn will pass this message to other vehicles. The messages transmitted could be tampered by the adversary. He could perform the attack by modifying the data sent by the vehicle and/or impersonate by pretending as an authenticated vehicle and misguide the vehicles. Thus the privacy of the authenticated user could be disturbed. The main aim is to prevent the data from these two attacks. The structure of the VANET is as shown in the figure 1.

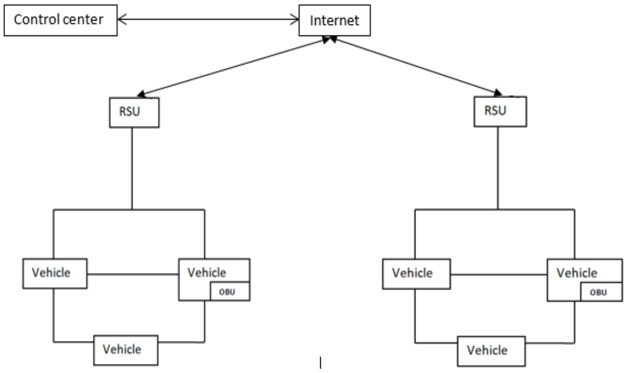


Figure 1: VANET Architecture

II. EXISTING SYSTEM

The Vehicular Ad hoc Network (VANET) is the wireless communication mode, adversaries against VANETs could control communication channels fairly easily, i.e. adversaries could intercept, modify, replay and delete messages transmitted in VANETs easily. Therefore, VANETs are vulnerable to many kinds of attacks. Therefore, the security of messages transmitted in VANETs is very important for many practical applications. Hence these messages have to be secured against the attacks by the adversary.

III. PROPOSED SYSTEM

The messages that are been sent among the vehicles will be in the text format mostly. Since the messages are exchanged with the help of the internet, it is more vulnerable to the adversary to perform any kind of attack over it. Hence these messages have to be in a form such that no third person except the sender and the receiver will know the exact message sent. For this purpose authentication of messages plays a major role in maintaining the real identity of the vehicle and hence secure the message. A control center acts as a trusted party which has all the information about every vehicle. For authentication encryption and decryption is done over the messages. RSA algorithm is used to obtain pair of public and private keys. Using these keys the message will be encrypted at the sender and decrypted at the receiver. The energy and time consumed to transmit the message from one vehicle to the other has to be minimum

IV. METHODOLOGY

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours. NS2 is an object oriented simulator written in OTcl and C++ languages. While OTcl acts as the frontend (i.e., user interface), C++ acts as the backend running the actual simulation.

Figure shows the basic architecture of NS2. NS2 provides users with executable command ns which take on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (Otcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles.

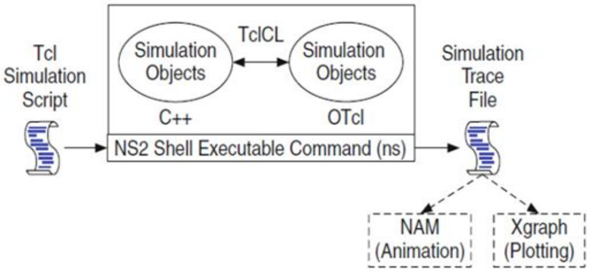


Figure 2: Basic Architecture of Ns2

V. DESIGN AND IMPLEMENTATION

A. Architecture

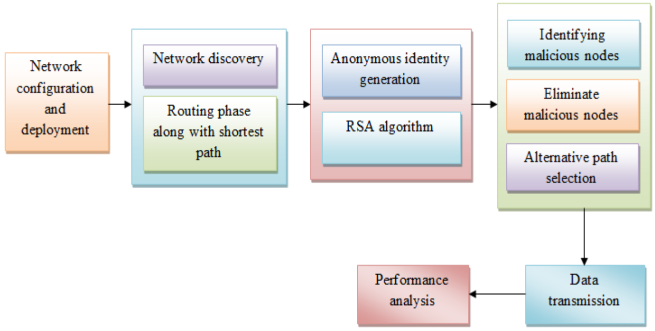

Network configuration and deployment
Network discovery
Routing phase along with shortest path
Anonymous identity generation
RSA algorithm
Identifying malicious nodes
Eliminate malicious nodes
Alternative path selection
Data transmission
Performance analysis

Figure 3: Basic Architecture Diagram

The above figure represents the architecture of the proposed system. In the first step the network is configured with the network parameters like number of nodes, initial energy, and channel type propagation. The network is discovered and using the distance formula the shortest path between the source and destination is calculated. Using RSA algorithm the public and private key pairs are obtained. The message is encrypted using public key and decrypted using the private key. When the message is passed along the path the attacker may try to attack the nodes through which the message is passed. Then the attacked node is identified and the message is reached to the destination through an alternative shortest path securely.

The modules have been explained as follows:

1) Network Creation & Deployment: First define the Network configuration parameters i.e., specify the number of nodes, initial energy, MAC, propagation, Receiver power, sleep power, transmission power, Channel Type, Propagation or Two Ray Ground i.e., radio-propagation model, network interface(Phy/WirelessPhy),MAC type(Mac/802_11),interface queue type(CMUPri Queue), link layer type, antenna model (Antenna /Omni Antenna), max packet in ifq, number of mobile nodes, X axis distance, Y axis distance Initial Energy, Initial energy in Joules. Then deploy all the nodes into the network with some moving velocity.
2) Network Discovery: After the nodes are created then assign the node positions with the set destination of x

value, y value and h distance. Configuration of the nodes in the network by specifying values to network configuration parameters.

3) Routing Phase along with shortest path: In this phase using the distance formula the shortest distance between the source and the destination has been calculated.
4) Anonymous identity generation: The data to be transmitted from the source is been collected. This data is been encrypted using the RSA algorithm. There will be two keys generated which is public key and private key. The data is encrypted to form a cipher text. This data is sent across the network.
5) Identifying malicious nodes: The size of the data packet is varied when it is attacked by the adversary. By this way the malicious node is found out and the existing path and the node is blocked and alternate path is chosen.
6) Alternative path selection: The encrypted data is collected by all the nodes which are involved in the data transmission between the source and the destination node. The data packet will be of a certain size, it will be varied if the malicious node has attacked the data packets. Hence the malicious node will be detected and the path through which the data was transmitting in the beginning will be changed. The alternative path will be chosen and the data is sent through that securely.
7) Performance analysis: The performance analysis is done by plotting PDR graph and calculating the execution time.

B. RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Key generation:

- Generate two large prime numbers: p and q
- Let $n=p*q$
- Let $m=\phi(n)=(p-1)(q-1)$
- Choose a number which is co-prime to m with $GCD((\phi(n),e)=1; 1<e< \phi(n)$
- Find d such that $d*e \bmod \phi(n)=1$
- Publish e and n as the public key; keep d and m as private key

Encryption:

$$\text{Cipher}=(\text{message})^{e} \bmod n$$

Decryption:

$$\text{Message}=(\text{cipher})^{d} \bmod n$$

By using the RSA algorithm technique the public and private key pairs have been generated and each vehicle has its own pairs. This information will be present in the control center and it has the information about all the authenticated vehicles. Thus the message is encrypted using the public key and sent across the path towards the destination. Even though its been tampered by the adversary he will not be able to decrypt it due to the complexity of the algorithm. Once the receiver gets the message, it will decrypt using its private key.

C. Simulation parameters:

Table 1 summarizes the simulation parameters required to evaluate the performance of the proposed system

Sl.no	Parameters	Values
1	Number of Nodes	39
2	Node energy	100 Joule
3	Sensing	Automatic
4	Simulation Area	1500*1000
5	MAC header	272bits
6	RTS& CTS Packet Size	256bits
7	ACK Packet Size	256bits
8	Transmitting & Receiving power	0.05V
9	Data transmission rate	1Mbps
10	Controller node	36th node
11	Attacker Nodes	37th and 38th

VI. RESULT AND ANALYSIS

Test cases

A. Initialization Testing

Functional requirement no.	Functional requirements	Sub Modules	Module name	Results
F1	Created 30 to 40 Nodes	Nodes Creation	Network initialization Module	Tested ok
F2	Configur Network Parametes	Assign Parameters	Network initialization Module	Tested ok

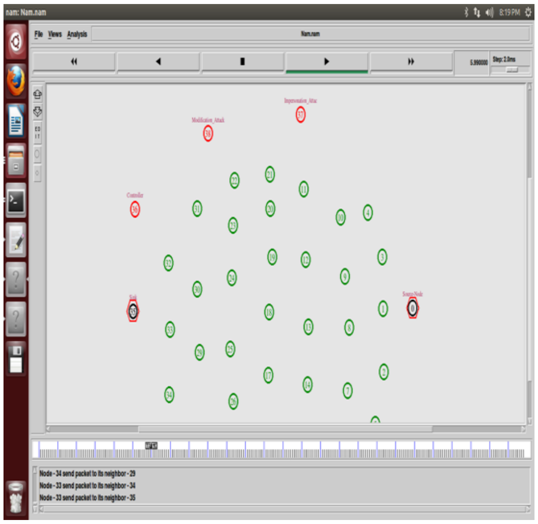
B. Functional Testing

Functional requirement no.	Functional requirements	Sub Modules	Module name	Results
F1	Apply RSA algorithm	Generate the keys	Anonymous identity generation	Tested ok
F2	Identification of Malicious	Avoid Malicious nodes	Anonymous Identification	Tested ok

C. Interface testing

Interface	Source Module	Destination Module	Input parameter	Output parameter	Result
i-5	Anonymous Identity generation	Identifying malicious nodes	Encrypted data transmission	Eliminates the malicious/attacker nodes	Tested ok
i-2	Nodes creation	Node Deployment	Nodes with energy parameter and their positions	Average of 30 to 40 nodes are created and establish the connection	Tested ok

In the project result and analysis section, system performance is estimated using a variety of factors to verify whether the predefined intensions are satisfied or not. This section includes the details of the project results, providing a description of the project's performance and explaining it using a graph.



Node - 34 send packet to its neighbor - 29
Node - 33 send packet to its neighbor - 34
Node - 33 send packet to its neighbor - 35

Figure 4: Modification and Impersonation attack

Figure shows the two attacker nodes: modification attacker and impersonation attacker. These two nodes will be detected and an alternative path will be selected and data will be transmitted through that path.

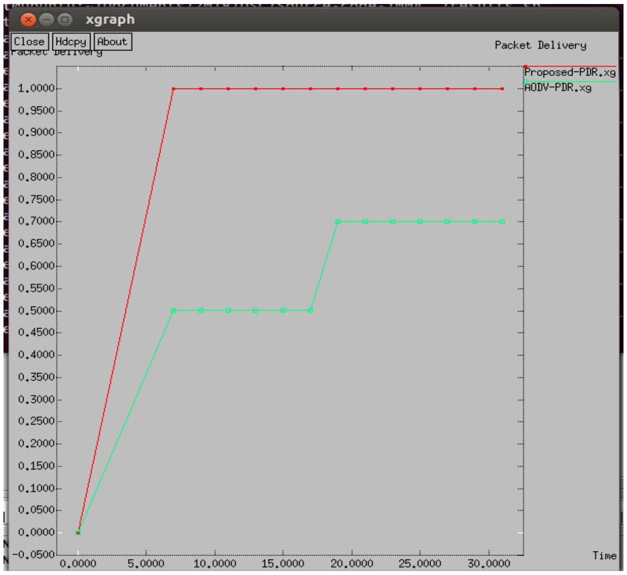


Figure 5: PDR graph

The proposed system PDR (Packet Delivery) is compared with the AODV and the graph is plotted.

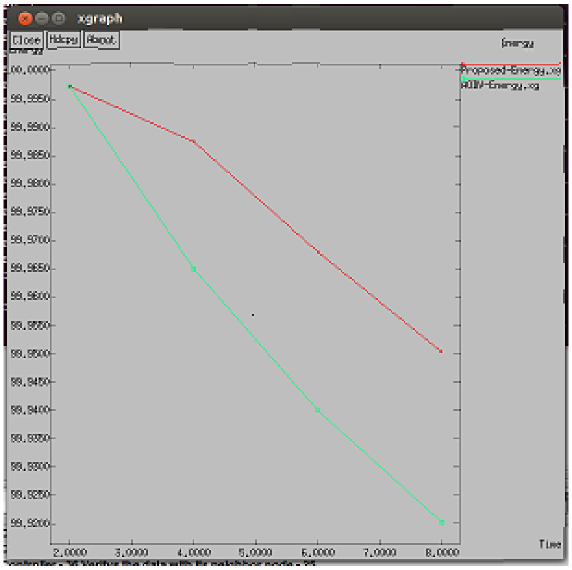


Figure 6: Energy graph

VII. CONCLUSION

The communication between the VANETs is carried out securely by choosing the shortest path between the sender and the receiver vehicles. The message has been secured using the encryption and decryption techniques. The RSA algorithm has been used to obtain the public and private key pairs. The two attacks that is modification attack and the impersonation attack has been identified and an alternative path has been chosen. Even though the data packet is obtained by the attacker it is not decrypted since it is strongly secured by RSA algorithm and data has been transmitted securely over that path. The execution time is less when compared with the AODV.

REFERENCES

[1] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “SPECS: Secure and privacy enhancing communications schemes for VANETs,” Ad Hoc Netw., vol. 9, no. 2, pp. 189–203, 2011.

[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETs): Status, results, and challenges,” Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2012.

[3] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, “Detecting misbehaviors in VANET with integrated root-cause analysis,” Ad Hoc Netw., vol. 8, no. 7, pp. 778–790, 2010.

[4] Y. Toor, P. Muhlethaler, and A. Laouiti, “Vehicle ad hoc networks: Applications and related technical issues,” IEEE Commun. Surveys Tuts., vol. 10, no. 3, pp. 74–87, Sep. 2008.

[5] A. Boukerche, H. A. B. FOliveira, E. F. Nakamura, and A. A. F. Loureiro, “Vehicular ad hoc networks: A new challenge for localization-based systems,” Comput. Commun., vol. 31, no. 12, pp. 2838–2849, 2008.

[6] IEEE Trial-Use Standard for Wireless Access in Vehicular Environment—Security Services for Applications and Management Messages, IEEE Standard 1609.2-2006, Jul. 2006.

[7] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.

[8] J. T. Isaac, S. Zeadally, and J. S. Camara, “Security attacks and solutions for vehicular ad hoc networks,” IET Commun. J., vol. 4, no. 7, pp. 894–903, 2010.

[9] J. P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[10] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, “An identitybased ring signature scheme with enhanced privacy,” in Proc. Securecomm Workshops, 2006, pp. 1–5.

[11] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.

[12] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in Proc. 27th Conf. IEEE INFOCOM, Apr. 2008, pp. 1903– 1911.