Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Recognizing and Thwart the Illegal Signature from Originator Data Dissemination Using Blowfish in VANET

[1]R.Janani and [2]Angayarkanni S A
[1,2]Assistant Professor,
[1,2]Department of Information Technology, R.M.K Engineering College, Chennai, India

***Abstract*—** Vehicular Ad-hoc network (VANET) is a technology where a car act as a node communicator with rest of the cars and the road infrastructure in the network. Vehicle location and speed information is continuously collected the VANET communication to manage. In VANET, the data will be disseminated from the source to the destination. While the spread of date from the originator is it possible for the attacker to some invalid send messages. The data are to detect and thwart before sending it to other vehicles. The research and development of the proposed VANET systems was the security of the data by the use of Blowfish algorithm in which it is used, the password protect, widespread.

Keywords- *VANET, Blowfish, Data Dissemination*

I. INTRODUCTION

Vehicular Ad-hoc network (VANET) is a network of vehicles and roadside infrastructure. Vehicle location and speed information is continuously collected by VANET nodes. On-board unit (OBU) processes the information from the various sensors on the car, and there are conditions of the vehicles. An on-board unit (OBU) is responsible for the communication with the external network, such as with other vehicles and the infrastructure. Road Side Unit (RSU) is an infrastructure for the communication between the vehicles for the exchange and information from a variety of different vehicles. The data transfer can be performed with the vehicle (V2V) and vehicle-to-infrastructure (V2I). The road has become a "network", today vehicles have been designed to networks to carry, with other vehicles via a communication link or channel to communicate. The opponent can track a vehicle by observing their communication and movement patterns. Privacy violation and anonymous communication are some security problems in VANET.

Nevertheless, these communications can be devastating if an opponent of the system for personal use. Therefore the communication of the vehicle should have the potential, the identity of the sender and the integrity of the message to verify. This can be achieved through the use of convenient signature scheme due to the intrinsic properties of the vehicles: very variable speed of vehicles of different concentration in a specific area/time, uneven roads characteristics and weather conditions in the development of such a protocol is threatening to be achieved. Too many messages of vehicles and RSU to a certain street, the message transmission rate and thus increase the power of the network effect. That is the reason why the scheme is a low complexity, reliable and fast authentication mechanisms should have. This work we have on the specification of the VANET security and production focus successfully with the problems. Firstly, the display of the network and security requirements are discussed. Security in VANETs is one of the two techniques. Vehicles can also rely on the Security Services innate to the use of public key communications, outstanding on the need for such a communication, the burden of proof for the safety in the vehicles of the network is not present. Blowfish is another algorithm designed to the where it uses passwords to protect. It is definitely one of the more flexible encryption methods available.

II. RELATED WORK

The ETSI (European Telecommunication Standard Institute) geo-ne work protocol [5] [6] allows multi-hop dissemination of messages in the VANET, merging of dissemination functionality in the vehicular networking layer and the conservation of the underlying MAC and PHY radio protocol layers, such as IEEE 802.11P are defined. The claim to forwarding (CBF) component of the geo-networking protocol [5] defines a timer-based distribution logic to send messages. A subscriber receives a message from node B, examined whether this has already been received and managed. Recent studies have an incompatibility for standard clustering approaches in the VANET scenarios, due to the high mobility involved [7], which has led to new proposals. The solution described in this work is that these proposals are inspired and employs a hybridization between clustering and beacon less (greedy) backbone Creation [8] the support of the local RSU different local cluster by communication with the cluster managers selected for their relative distance to orchestrate; as soon as the heads of state and government are selected, they will be used exclusively for the dissemination of data from the RSU to your personal local cluster can be used. The rest of the cars hear the news of Leader, or just a cluster, send message, the next cluster to connect and for incoming data, [4] vehicular ad-hoc networks wait is a promising new technology, this technology is a fertile area of attackers with its attacks on network try. She gave a broad analysis of the current challenges and solutions and critic for this solution, we also have a new solutions to help you secure VANET network to stay.

Despite these benefits, VANETs come with their own challenges, in particular in the aspects of safety and privacy. Lack of authenticated information in the network can be shared to malicious attacks and abuse to the serious dangers for the driver could represent [6], [7]. In addition, unlike traditional wired networks of several lines of defense such as firewalls and gateways are protected, attacks on wireless networks can come from various sources and target all nodes [8], [9]. Harmful vehicles could follow the activities of the specific driver on the provided information for the authentication of this data protection problems caused by the use of anonymity to address and attempts to temporary pseudonyms. But with these privacy proposals harmful vehicles could still be anonymous, that it was difficult for the trusted authority, such as vehicle management, harmful to monitor vehicles and their access to revoke. In order to tackle these problems the concept of the Blowfish algorithm for data protection and conservation of the proposed has been overcome.

III. VANET APPLICATIONS AND CHARACTERISTICS

There are many important applications of VANET. These applications can be divided into two categories (I) safety-relevant applications and (ii)-based applications [4] be categorized.

1. Safety Related Application

These applications are used to increase the safety on the roads.

Road Traffic Safety: These programs work on reducing the number of road deaths and injuries on the roads of the notification to the operator on the dangers in advance.

Cooperative Driving: The drivers have an important role to play in this application. How Violation warning, conflict, Curve Warning etc., lane merging and significantly reduce the service life - risk of accidents. In fact, many of the Accidents come from the lack of cooperation between the drivers.

Traffic optimization: Traffic through the use of signals such as jam can be optimized, accidents etc. to the vehicles, accordingly, you can select your alternative path and also save time.

2. User Based Application

Following are the services for the user.

Peer to peer application: These applications are very much useful to provide services like sharing multimedia files, movies, songs etc. among the vehicles in the network.

Internet Connectivity: People can connect with the Internet all the time. Thereby, VANET provides the constant connectivity of the Internet to the users.

Comfort and Quality of Road Travel : These applications offer comfort for travelers as 'Advanced Traveller Information Systems", "electronic payment systems", "Electronic Toll Collection', find the petrol station etc.

A. Characteristics of VANET

VANET has its own distinct characteristics, which are summarised as follows :

High Mobility: Node in VANETs in general move at high speed. This makes difficult position and a node, the protection of privacy to forecast.

Dynamic Topology: Due to the high level of mobility and a vehicles speed random node, the node position changes frequently. So, network topology in VANETs changed regularly. The connection between the vehicles in VANET has frequent interruptions due to the high level of movement of the nodes and frequent changes in the environment.

Unbounded network size: The size of the VANET is geographically unlimited. It means to VANET can be implemented for a city, several cities or countries.

Frequent exchange of information: Ad-hoc nature in VANETs motivated students with information from other vehicles and Rsu to collect. That is why the exchange of information between the nodes is often.

Wireless Communication: VANET is designed for the wireless environment; nodes are connected and their information via the wireless exchange. Consequently, safety measures must be considered during the communication.

Time Critical: The delivery of information to the nodes in VANET must be done within time limit so that it can perform the action accordingly, e.g. critical medical emergency messages must be delivered on time in order to save human lives.

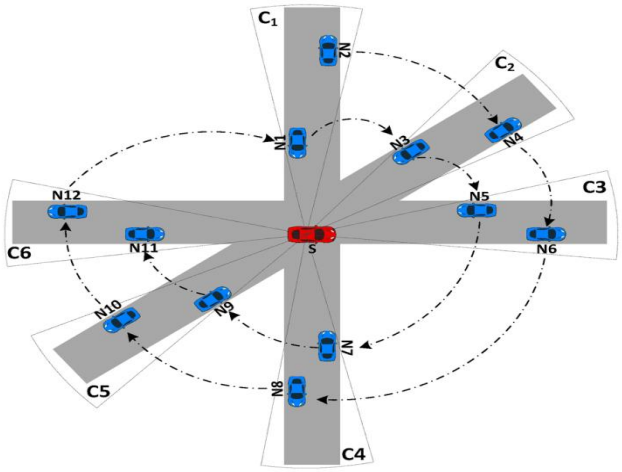

Figure 1: Data dissemination from the originator

IV. CHALLENGES IN DATA DISSEMINATION

Dissemination of data is a process of dissemination of data or information about distributed networks [1]. So, data dissemination in VANETs improves the efficiency of transport systems. It also enhances the quality of driving. Although this process seems to be very simple, but in reality it is hard for the vehicles to each other due to the large number of vehicles on the road to communicate. So it is a very demanding task for vehicles information about the network [7]. Some of the main issues in the dissemination of data are:

1. High Mobility and Frequent Disconnections:

The big challenge in VANETs is the high level of mobility and often isolated topology in different regions of the city. The traffic density is low during the night and in the suburbs, but network node density is very high, in urban areas and especially during the rush hours in the day time, the causes of common network interruption. There is no simple "one-for-all" solution for the data to all recipients that are over the city spread [1].

2. Data Transmission in presence of Disconnection:

The big challenge in VANETs is the high level of mobility and often isolated topology in different regions of the city. The traffic density is low during the night and in the suburbs, but network node density is very high, in urban areas and especially during the rush hours in the day time, the causes of common network interruption. There is no simple "one-for-all" solution for the data to all recipients that are over the city spread [1].

3. Data Distribute over the Mesh Nodes:

For efficient data dissemination, many roadside units are connected together to form an infrastructure like mesh network and cooperatively disseminate data to the vehicles. So, it becomes very difficult how to distribute data in the mesh network [1].

A. Types of Data Dissemination

Dissemination of data is a process of dissemination of data or information about distributed wireless networks. The aim of the dissemination of information is the optimal use of network resources the data of all users [1]. Different types of data dissemination in VANETs used:

1. V2 I/I2V dissemination (vehicle of the infrastructure or the RSU)
2. V2V dissemination (vehicle-to-vehicle)
3. opportunistic dissemination
4. peer-to-peer distribution
5. cluster-based distribution

A. V2I/I2V Dissemination

It consists of two types of mechanisms: push and pull. In Push-based data dissemination, data pouring and buffering concepts are used. With casting data concept, road is selected with high mobile vehicles and Data Center will send the data to the vehicles on the same road as well as on the crossing roads. Data Center is a computer with a wireless interface that collects the data from the outside and provide it to the vehicles. And buffers are placed at the intersection to save the data and data from this buffer in moving vehicles [3]. So, in the push-based data dissemination, data efficiently from the moving vehicles and roadside Units (RSU) to another vehicle [1]. When pulling data dissemination scheme is that of vehicles used when you some information from the data center or from any other vehicles would like to receive. This scheme is mainly of vehicles for the questions and answer [3].

B. V2V Dissemination

In vehicle to vehicle data dissemination flooding and relaying mechanisms are used [1]. In flooding, data is broadcasted to all nodes that participate in data dissemination. One to all communication is done here. In the relay type of data dissemination, relay node is selected and this node forward the data to next relay hop and so on. Relay approach is generally preferred for congested networks .

C. Opportunistic dissemination

In opportunistic data dissemination, messages are stored at each intermediate node and forwarded to every encountered node till the destination is reached.

D. Peer-to peer Distribution

In P2P distribution, the source node stores the data in the memory and sends the data to the network only if you are promoted by another node.

E. Cluster Based Distribution

On the reduction of broadcast storms and for a better delivery ratio, a data packet from a minimum of between nodes to the target will be forwarded. To do so, the nodes in a cluster, in which a node or more data in the cluster collects arranged and send them to the next cluster [1].

V. FEATURES OF THE INFORMATION DISSEMINATION PROTOCOLS

There are some features or functions that the dissemination of the protocols must have and these functions are given below:

1. Scalability
2. Effectiveness
3. Efficiency
4. Dissemination delay
5. Robustness

VI. ALGORITHM DESCRIPTION

The advantages of the use of different vehicular backbone sub-networks of several originator. The protocol is as an independent layer on top of the Mac and placed by an application framework that the dissemination, for example a File Download or Streaming video requires. Have several originator the data transfer can be performed in parallel, because there are several nodes in different locations on the network, the data at the same time the distribution are distributed.

In addition, each vehicle has a backbone, the specific characteristics of the approach used (described below), the data more efficiently to a simple flooding algorithm in comparison to be able to spread, met. Participant candidates for each backbone with self-delay mechanism in a similar way as geo-networking protocol selected, but your choice is permanent and not package-based. The delays mechanism works in a very simple way: each node has its own timeout; if no messages were received before the timeout expires, the node changes its policy to backbone node - BN and initiates a selected package; otherwise it will be a node locked. This self-healing mechanism works for backbone and inhibited locked node node are not allowed, and a billion should theoretically incoming packets from one source: its previous hop.

A. Blowfish encryption

The data transformation process for Pocket Brief uses the Blowfish Algorithm for Encryption and Decryption, respectively. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data for a fast, free alternative to existing encryption algorithms. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. By using blowfish encryption algorithm, the data disseminated from the originator is safeguarded from the advisory and the illegal signature is checked by using feistel cryptographic technique.

B. Feistel Networks

A Feistel network is a cryptographic technique in the construction of block cipher-based algorithms and mechanisms. A Feistel network implements a number of iterative algorithms on a block of data and is typically used for block ciphers that large quantities of to encrypt the data. A Feistel network works by splitting the data block into two equal pieces and the use of encryption in several rounds. Each round implemented permutations and combinations of the primary function or keys are derived. The number of rounds will vary depending on the Cipher implemented, a Feistel network. In addition as a reversible algorithms, Feistel network produces the same output until the input is same.

C. Multiple originators

The most important change to the work on the formation of a backbone lies in the possibility of several fragments of the backbone of several authors to generate. This solves a number of problems from earlier implementations such as:

_several Access Points (originator)data on the vehicles to disseminate

_a faster backbone formation time (similar clustering algorithms);

_homogeneous backbones in relation to their properties and the stability of the entire backbone are less dependent on a single source (originator);

_backbone structures with a small number of hops and therefore more efficient data in a fast way to spread.

The most important change of the work concerning the formation of a backbone lies in the ability to generate multiple fragments of backbone from multiple originators. The suitability parameters in a local area is used: In this case, it means that each node, on the border of the backbone for the election of the next backbone nodes in a greedy fashion is responsible, can be selected. In addition a Backbone node discards all other dial-package from other backbones. The extension of the Backbone is interrupted if each node on the edge belongs to a selected package sends and this is only by nodes from the edge of another backbone: this means that the area is already covered. A node is selected as the a originator copyright, to the Backbone separated. This newly constitute the backbone has all the characteristics of a single-generator backbone, besides the fact that it is not the only one in the network.

CONCLUSION

In this paper there is increasingly stringent security when the data from the originator spread, the technologies in the solution of VANETs security and data protection should be much more complex with the Blowfish algorithm. Therefore, cross the illegal signature from the advisory can easily be detected. In addition, security and privacy should at the same time that brings the compromise between security and data protection to the light.

References

[1] X. Shen, R. Zhang, X. C. L. Yang, and B. Jiao, "Cooperative data dissemination via space-time network coding in vehicular networks,"in Proc. IEEE GLOBECOM, Atlanta, GA, USA, Dec. 9–13, 2013, pp. 3406– 3411.

[2] X Lin, R Lu, C Zhang, H Zhu, PH Ho, "Security in Vehicular AdHoc Networks", IEEE Communications Magazine, April 2008.

[3] P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Private Vehicular Communications", 7th International Conference on ITS, 2007.

[4] S. Ucar, S. Coleri Ergen, and O. Ozkasap, "Multi-hop cluster based ieee 802.11p and lte hybrid architecture for VANET safety message dissemination," Vehicular Technology, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2015.

[5] European Telecommunications Standards Institute ETSI TS 302 636- 4-1 v1.2.1; Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4, Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality, July 2014.

[6] European Telecommunications Standards Institute ETSI EN 302 636-3 v1.2.1; Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3, Network architecture, December 2014.

[7] A. Baiocchi, P. Salvo, F. Cuomo, and I. Rubin, "Understanding spurious message forwarding in VANET beacon-less dissemination protocols: an analytical approach," IEEE Transactions on Vehicular Technology, 2015.

[8] Lin, X., Sun, X., Ho, P.-H., & Shen, X. (2007). GSIS: A Secure and Privacy-Preserving Protoco for vehicular communications. IEEE Transactions on vehicular technology , 3442-3457.

[9] L. Briesemeister, A. G. DaimlerChrysler, Berlin, Germany and G. Hommel, "Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks", First Annual Workshop on Mobile and Ad Hoc Networking and Computing, (MobiHOC), (2000), pp. 45-50.

[10] P. Salvo, F. Cuomo, A. Baiocchi, and I. Rubin, "Investigating VANET dissemination protocols performance under high throughput conditions," Vehicular Communications, vol. 2, no. 4, pp. 185–194, 2015.

[11] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An IdentityBased Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transactions on, Parallel and Distributed Systems, vol. 21, no. 9, (2010) September, pp. 1227-1239.

[12] G. Samara and W. Al-Salihy, "A new security mechanism for vehicular communication networks", Proceeding of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), (2012), pp. 18-22.