Novel Algorithm for V2v and V2i Security by Fuzzy Logic Decision in Vanet

Ravi G, Satish S

Abstract: The recent developments in wireless communication technologies along with the costs of hardware allow both V2V and V2I communications for information exchange. Such a network is called Vehicular ad Hoc Network (VANET) which is very important for various road safety and non-safety related applications. However, Due to the wireless nature of communication in VANETs, it is also prone to various security attacks which are originally present in wireless networks. Hence to realize the highest potential of VANET, the network should be free from attackers, there by all the information exchanged in the network must be reliable should be originated from authenticated source. The system can be processed by the fuzzy logic method. It does not require any keys for data transmission. The system design is very efficient compared to other techniques. So the users prevent from road accident and traffic jam..

Keywords: VANET, On the Board Unit (OBU), Road Side Unit (RSU), Fuzzy Decision process, Current Forwarding Node (CFN).

I. INTRODUCTION

VANETs are the spontaneous creation of a wireless network for data exchange to the domain of vehicles. VANET's are the important key component of intelligent transportation systems (ITS). A VANET technology provides distinctive chance to develop numerous varieties of communication-based automotive applications [1]. The ITC configuration uses multi-hop broadcast to transmit traffic connected data over multiple hop to a cluster of receivers .In VANET vehicles movement are constrained by road. Road Side Unit and On Board Unit help to reduce the energy and storage consumption. Security is a key challenge in VANET. In a network the information node helps to update the status of the route to the node within the range. In early VANET most of the system uses DSRC (Dedicated Short range Communication) for the purpose of safety and securities of users. In sometimes it leads to time delay and jamming due to key mismatch or replication. Similarly TESLA scheme produce time delay it takes more time to generate keys. Using hash function the position should be predicted it generates both public and private key. Sometimes the system becomes vulnerable if the key is mismatched. In credit base Incentive scheme the computational cost of a system is so high [2]. Using identity based cryptography scheme Computational cost is low but the system design is difficult. In homomorphic signature it consumes more timing. But in fuzzy approach the accurate results can be obtained. In this the key generation is not necessary. The results should be produced by the fuzzification and Defuzzication. Compared to other methods it takes low time and energy for transmitting the data packets [4, 5].

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author

Ravi G*, Department of Electronics and communication Engineering, Sona College of Technology, Salem, India. Email: raviraj.govind@gmail.com
Sathish S, Department of Electronics and communication Engineering, Malla Reddy Engineering College for Women, Telangana, Email: cssathish2005@gmail.com,

The goal of the PBA is to design effective and scalable authentication for broadcasting of information with non-repudiation in V2V communication .the lightweight scheme uses chain key generation, position prediction, hash tree construction, and signature generation method to overcome denial of service attack and storage overhead of authentication. But it fails to reduce the high traffic densities and time delay for verification of vehicles, sometimes key replication or mismatch occurs [6]. It is not capable of handling the large network due to this it misses the beacon in the given interval of time and it cannot be reused. PBA operates only in online mode sometimes it does not help to update the routing information to the users when the network fails and the vehicle details should not be collected.

II. RELATED WORK

In a short time, a large number of vehicles arrive at in a network and realize the denial of service attack based on computations required more time for verification of vehicles and will lead to exhaustion of the resources available in the network. In early VANETs, packet loss caused by high mobility of vehicle had been resisted. The solution to the problem can be achieved by PBA (Prediction Based Authentication) [7], Chen Lyu[1]. It is a light weight scheme and helps to minimize the cost of computation with storage overhead by authentication of vehicles. In PBA scheme [8], we generate keys for transmitting the data packet. The Signature verification is often performed to support prediction outcomes from MHTs integrated into beacons ahead. The Prediction-based Authentication scheme is performed in three categories [9]:

- TESLA scheme: It is the foremost step used in PBA. In this scheme a system requires excess time for chain key generations.
- Position prediction: For each and every beacon interval, all the vehicles must predict their position. It leads to time delay.

- Merkle Hash Tree Construction: The position of vehicle should be predicted to construct its own public and private key [10,11].
- It is the most critical phenomenon. Sometimes, the collision of the packet occurs due to wrong key generation or replication by itself.

For the above reasons, we can go for fuzzy logic based approach. It gives accurate results and it does not have any key generation process. We can easily handle the vehicles with the help of adversary node even if they are not in the appropriate range.

VANET has two components namely On-Board Unit (OBUs) and infrastructure Road-Side Unit (RSUs). Multi-hop communication takes place to exchange information in shortest range by using a standard IEEE802.11P. A Malicious node generates false information and makes disturbance to other nodes in the network. This problem may be overcome by using the vehicular network IEEE 1609.2 standard that depends on public key infrastructure (PKI). Second, the application built on the network will face pollution attack as forwarders can inject polluted message into the network. For addressing pollution attack, it requires neither secure channel nor high computational overhead. Finally VANET helps to improve the driving experience and safety in the road and enables inter-vehicular communication. The efficiency can be improved by implementing the application called Congested Road Notification (CRN) to alert the vehicle, before congested by traffic jams[6]. In all these schemes Revocation service is difficult to efficient authentication in VANET and these schemes require extra secure channels so that the forged messages cannot be identified. We go for fuzzy logic based approach to overcome the traffic related problems and reduce packet loss which helps to improve the lifetime of the networks. These can be achieved by using binary values.

III. PROPOSED SYSTEM

The proposed system helps to overcome the issues in PBA. It reduces the storage overhead by splitting the vehicle location into zones. By creating adversary node with the help of localization algorithm to collect the information about vehicles (speed, time and distance) and it helps to avoid the verification time of vehicles. Fuzzy logic helps to remove the false node and whose value lies between 0 to 1. The system operates both in offline and online mode using recursion algorithm. By selecting next-hop node for transmitting information to neighbor node should consider two metrics as an input to the node namely position of vehicle from source to destination and its distance to its neighboring node. Here fuzzy logic uses Current Forwarding Node (CFN) to transfer data packets to its neighbor through intermediate node. The neighbor node with the maximum value of fuzzy output is selected as the first preferable next-hop neighbor node around a source.

A. Fuzzy Logic decision making Algorithm

1. Initially deploy the nodes in a network region.
2. Grouping the nodes for easy transmission.
3. Predict each vehicles position.
4. To calculate the distance between vehicles and network within the region.
5. Create a clone node and adversary node to update the routing information.
6. Implement localization algorithm.
7. Next done decision making by fuzzy logic based routing.
8. Then transmit the data pack.

B. Recursion algorithm

Clustering process

Initially vehicles in a network can be clustered or grouping based on their zone. The nodes inside the region are called as intra zone and beyond the region are called as inter zone vehicles, which is shown in Fig. 1.

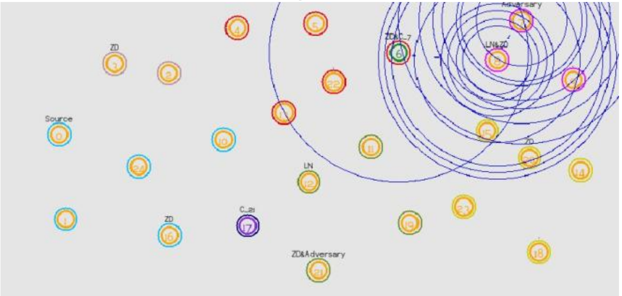

Fig: 1. Clustering of Vehicles

Action of advisory node

The central node in the network helps to update the information about the nodes in the network for the purpose of avoiding critical issues. The advisory node having ID to check and communicate the nodes in the network. Fig.2 shows the clone node creation.

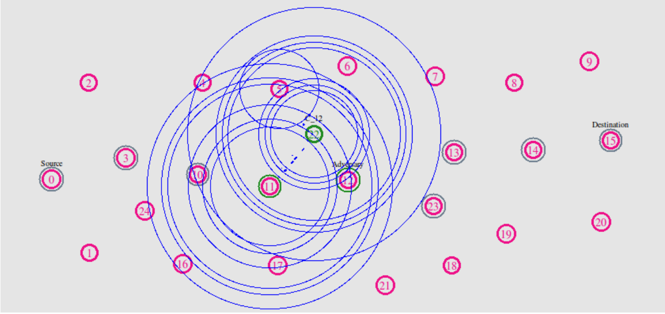

Fig: 2. Clone node creation

Adversary node creates clone node, it gives request to all its neighbor nodes. Clone nodes gathering their path information from these neighbor nodes. Fig. 3. Shows the, how the unnecessary nodes removed from the network.

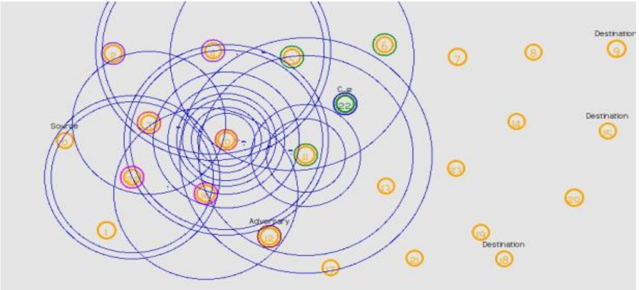

Fig: 3. Removing of Unnecessary Nodes

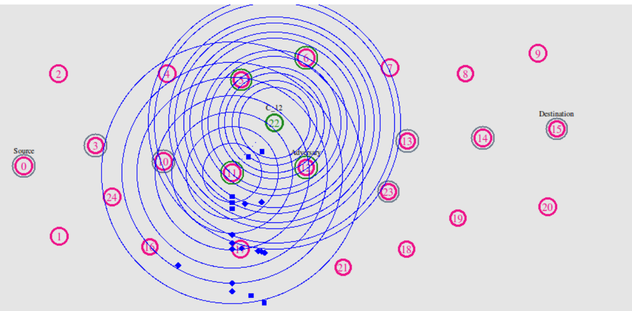

Fig: 4. Data loss

Fig. 4, shows the data loss in the network. After the generation of clone node it sends the detail of data loss from source to destination. It helps to identify the cause for data loss and to identify the false node to remove this from the routing path.

Localization algorithm

These system operates both in online and offline mode and no need to generation of keys for data transmission. By using this process it helps to find the vehicles information like speed ,distance and to track the vehicles location.

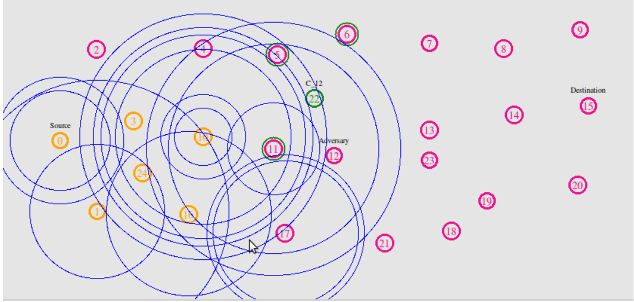

Fig: 5. Using XED and EDD localization algorithm

All sensor nodes encounter each other randomly for keeping position in the network.Advisory nodestores the list of encountered node preventing the network from replication attack. Fig. 5 show the localization algorithm,

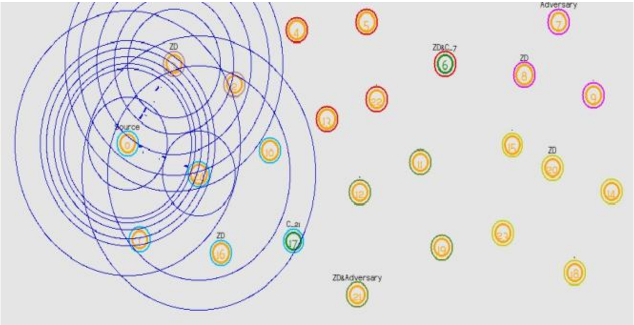

Fig: 6. Safe zones

IV. RESULTS AND DISCUSSION

A. Network Lifetime

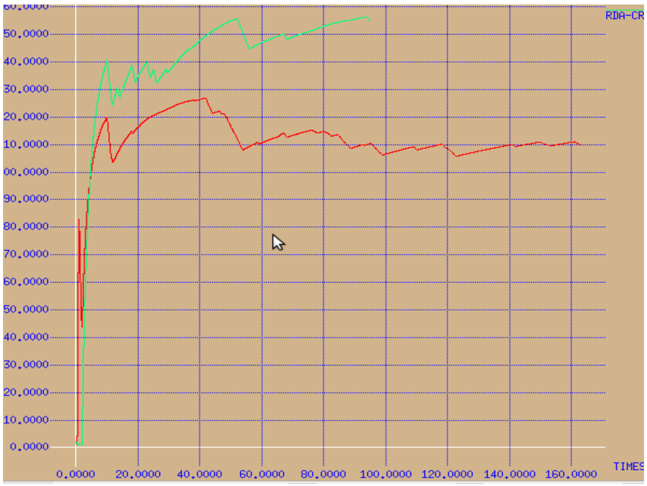

Fig: 7. Network lifetime

In Fig. 7 x-axis represents time in (m/s) and y-axis represents network lifetime. Compared to existing system it improves network lifetime around 10-15%.

B. Packet loss

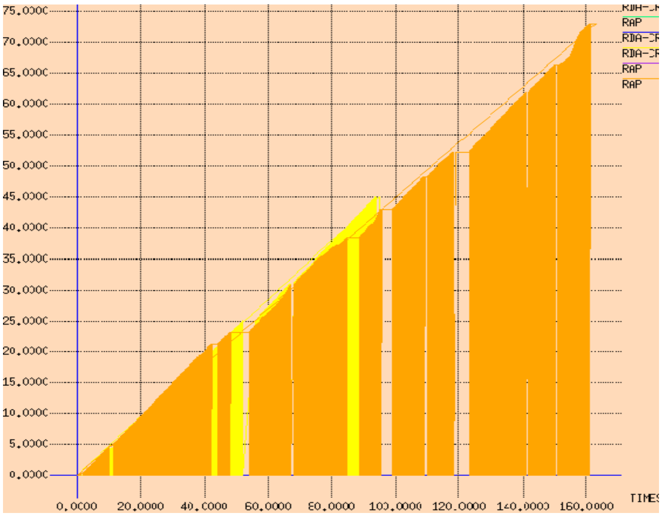

Fig: 8. packet loss

In this graph time is taken in x-axis and packet loss in y-axis which is shown in Fig 8. Packet loss can reduced approximately up to 45% from the existing system.

C. Channel measurement

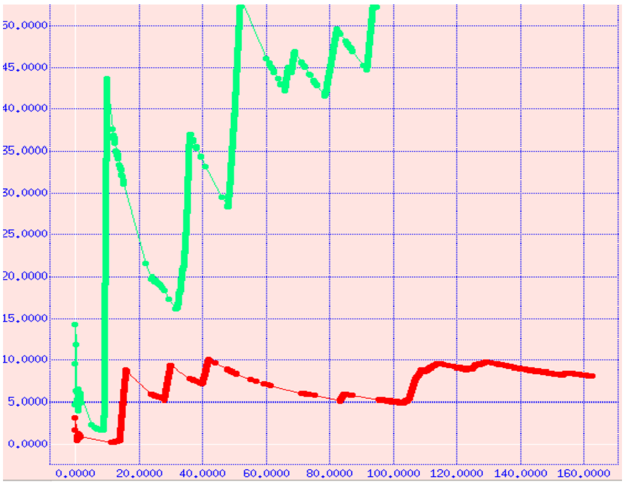

Fig: 9. channel measurement

Basically the performance of any system can be depends on channel measurements. It is important an important phenomena. In this system the fuzzy decision algorithm achieves 25% efficient channel measurement, in Fig. 9

D. Signal strength

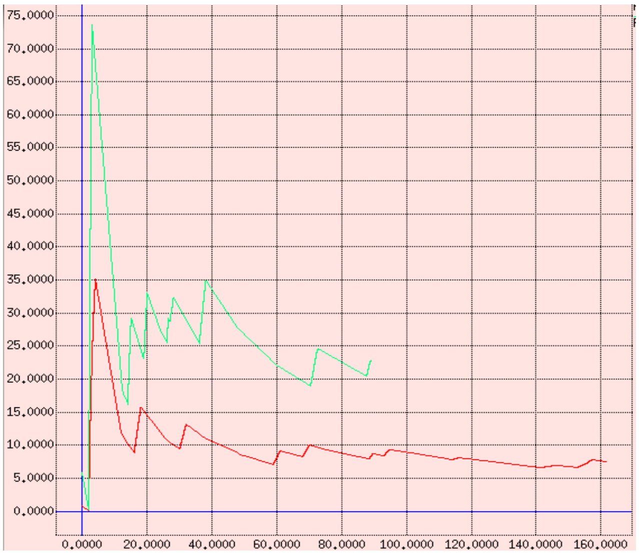

Fig: 10. signal strength

Signal strength is also called as field strength. It refers to the source power output is received by a reference network at a distance form source power. The Fig. 10 shows the signal strength.

Table- I: Route Accessibility

S.No	Route status	Fuzzy value	Route information
1.	Low	0.5	Busy
2.	Good	0	Less traffic
3.	Expensive	1	No traffic

From the table I, the route information can be predicted in three states namely low, good and expensive. Here, users can identify busy routes and it helps to identify the path which is not suitable to travel that is in low state. Whereas good status indicates less traffic, the expensive state indicates no traffic in the route so that they can be easily travelled without traffic jams.

V. CONCLUSION

The motivation of the fuzzy based decision making process is to reduce the packet loss, signal strength and also improve the network lifetime. With the help of adversary node the users can be prevent from accidents even when there in safe region and to reduce critical situations. The data loss can be reduced. It creates alternative path for reducing the network traffic.

REFERENCES

1. Chen Lyu, Dawu GU, Yunze Zeng and Prasant Mohapatra, PBA: “Prediction-Based Authentication for Vehicle-to- Vehicle Communications” IEEE transactions on Dependable and secure computing vol. 13, no. 1, Jan / Feb. 2016
2. M. Raya and J. P. Hubaux, “Securing vehicular ad hoc Networks,” J. Computer. Security vol. 15, no. 1, pp. 39–68, 2007.
3. C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, “An Efficient identity-based batch verification scheme for Vehicular Sensor networks,” in Proc. IEEE INFOCOM, pp. 816–824, 2008.
4. J. T. Chiang and Y. C. Hu, “Cross-layer jamming detection and mitigation in wireless broadcast networks,” in Proc. ACM Mobicom, pp. 346–349, 2007.
5. B. H. Bloom, “Space/time trade-offs in hash coding With allowable errors,” Communication.ACM, vol. 13, no. 7, pp. 422–426, Jul. 2007.
6. N. Lyamin, A. Vinel, M. Jonsson, and J. Loo,”Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks,” IEEE Communication Lett. vol. 18, no. 1, pp. 110–113, Jan. 2014.
7. P. Sheela Rani and R.Vinston Raja “Implementing Efficient Prediction Based Algorithm for Vehicular AdHoc Networks” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2015
8. J. L. Huang, L. Y. Yeh, and H. Y. Chien, “ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular AdHoc networks, ” IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262,Jan. 2011.
9. Xiang Li, Na Ruan, Fan Wu, Jie Li and Mengyuan Li “Efficient and Enhanced Broadcast Authentication Protocols based on Multilevel μTESLA,” IEEE 978-1- 4799-7575-2014.
10. A. Wasef and X. Shen, “EMAP: Expedite message authentication protocol for vehicular ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 12, No. 1, pp. 78-89, Jan. 2013.
11. A. Wasef and X. Shen, “Efficient Group Signature Scheme Supporting Batch Verification for Securing Vehicular Networks”, Proc of IEEE ICC, 2010.

AUTHORS PROFILE

Ravi G received his Doctoral Degree of Ph.D. in Information and Communication Engineering from Anna University, Chennai, INDIA in the year of 2016. He completed his Master of Engineering in Sona College of Technology (Anna University), Salem and Bachelor of Engineering in V.L.B. Janaki Ammal College of Engineering and Technology (Bharathiyar University), Coimbatore in the years of 2007 and 2002. His research areas are Wireless Communication, Wireless Ad hoc Networks, Wireless Sensor Networks and Optical Communication.

Sathish S received his Doctoral Degree of Ph.D. in Information and Communication Engineering from Anna University, Chennai, INDIA in the year of 2015. He is currently working as Professor in department of ECE, Malla Reddy Engineering College for Women UGC autonomous, he constantly proved excellence in teaching and all academic work. He is expertise in Wireless Communication, Wireless Sensor Networks, and Mat lab.