Identifying Malicious Nodes and Performance Analysis in VANET

J. Nethravathy¹ and Dr. G. Maragatham²

¹M. Tech Information Technology, ²Asst. Professor;
SRM University, Kattankulathur, Kancheepuram District, Chennai 603 203; India.

Abstract
In this approach, we define the attack as computation-based Denial-of-Service (DoS) attacks. Still without a few malice, the computation based DoS attacks can be easily initiated in a high density traffic scenario. For example, when traffic related messages (beacons) are sent 10 times per second as suggested by the DSRC protocol, a vehicle can be flooded with more neighbours within its radio range. To overcome this problem we have proposed the enhanced Prediction-based Authentication protocol using the detection algorithm to detect the DOS (Denial-of-Service) attacks earlier than the authentication moment in time. The mechanisms such as chained keys generation, position calculation, Merkle hash tree structure, and signature generation communications are used in the sender side. On the receiver side after receiving a beacon, the nodes checks for the authentication by applying techniques such as Attacked Packet Detection, DMN Technique, Self-Generated MAC Storage Technique, and Signature Verification mechanisms. Also, Performance study analysis is done with respect to parameters such as energy consumption, packet drop and average delay in receiving packets with respect to VANET.

Keyword: Denial-of-service (DoS), Message authentication (MACs), prediction based authentication (PBA), Enhanced Attacked packet detection (EAPD), Detection-of-Malicious Node (DMN)

Introduction
In an ITS (Intelligent transportation systems), VANETs form a key component. It works on the basics of MANETs (mobile ad hoc networks). MANETs are considered as a self network. That is, the network is formed by itself, hence they do not required any centralised control mechanism. Hence, in the ad hoc network concept each node can act as both a router as well as a data terminal. VANET is part of MANET, this way that all node can move liberally surrounded by the network reporting and wait linked, all node can talk by way of additional nodes in only hop or multi hop, and a few node could be Vehicle, Road Side Unit (RSU). The main objectives of this task are to answer mechanical issues correlated to communication protocols as well as data safety for car-to-car exchanges. The ultimate challenge was to solve the trouble of how to contact nodes not straight within data lines collection by employ neighbours as forwarders. [1].

In [2] the authors have proposed an efficient conditional privacy preservation (ECPP) protocol for safe vehicular interactions. The ECPP protocol can powerfully contract with the increasing revocation file even as achieving conditional traceability by the authorities. Instead of relying on a huge storage space at each OBU-On board Unit, as most of the previously reported schemes did, the future protocol be able to keep the necessary unknown key cargo space minimal without losing the security level. Meanwhile, the future protocol gain qualities in the fast authentication on safety messages and an efficient conditional privacy track means, which can give out as an brilliant applicant for the future VANETs.

Proposed System
Existing System
• Present system uses Fast Auth [3] to offer timely, lightweight and nonrepudiation authentication for vehicle-to-vehicle communication. The explanation creates in the existing system are: (i) The system cannot increase the packet-delivery ratio. (ii) Entire beacon message cannot be collected accurately (iii) The system fails to work, in case of any missing signal from the receiver At the beginning of a time frame, each vehicle generates ‘n’ chained private keys for the next ‘n’ beacons. This key is known as TESLA key. At each beacon gap, all vehicles predict its position relay in the next beacon.
• After position prediction, the vehicle spirit creates one space value of a public key and private keys. We used MHT, which ties these pre-computed keys as one and then generates a single public key or prediction outcome for all the possible movements.
• After the computation of position calculation and MHT creation, a vehicle signs the commitment of the hash chain and the prediction outcome from MHT using ECDSA[3] signatures, and broadcasts it along with the first beacon B0 in the time frame
• At receiver (RSU or OBU) side :

Hence, to overcome the shortcomings the proposed system is designed.

Proposed system
The following are the details in the sender side and receiver side details involved in the communication.
The Detection of Malicious Node (DMN)[4] algorithm is based on the following approach:

- A vehicle is measured to explain irregular activities if it drops or duplicate the packets received towards it so as to create pack in the network, misguide other vehicular nodes or destroy crucial messages for their selfish motives.
A truthful vehicle ahead the communication acknowledged to it suitably to other nodes in the network or creates right communication used for broadcast.

A vehicle resolve be present tag as a malicious vehicle, if the vehicle repeats abnormal behavior such that their distrust values, $D_v$ exceeds the threshold value $T_{md}$.

- The attacked packet detection algorithm is used to detect the Attacked packets [5] which are identified by the following Conditions. $F$ and $V$ are high because the position will change fast. $F$ with $V$ is low down for the reason that the vehicle positions will not change much. If the packet is attacked packet then it is discarded otherwise go to the verification phase.
- To reduce the storage cost of unconfirmed signatures, the recipient only reports a reduced re-keyed MAC.
- For the first beacon, the receiver verifies the ECDSA signature.

**System Overview**
The RSU plays a vital role in identifying the malicious node packets and clears those packets with correct packets with respect to all the vehicles in the scenario.

**Implementation Result**
In the existing system-PBA approach, the factors such as Security issues, end to end delay aspects and packet delivery time are accounted and the proposed approach has shown improved results which were encouraging. The experiment is carried out using NS2, fedora 8 with Hard Disk 40GB, Processor above 500MHZ, RAM 512MB. Following are the simple screen shots of the proposed work.
Figure 5: packet dropping

Figure 6: Malicious node find

Figure 7: Malicious node detected

Figure 8: End to end delay

Figure 9: Packet delivery and reliability

Figure 10: Energy (In J)
Conclusion
The enhanced Prediction-based Authentication protocol is secure and robust in the context of VANETs. To identify misbehaviours and nasty vehicular nodes in VANETs, we have used the technique DMN [4]. The technique [4] is considered to separate the nodes showing abnormal behaviour as well as striking the network presentation. It optimizes the selection of existing algorithm which selects all the nodes as verifiers which have distrust values. The simulation results indicate that the integrated approach provides higher throughput and reduces the end to end delay, when compared to that of the existing method. It also achieves the high packet delivery ratio and minimizes the delay overhead.

Acknowledgement
I express my sincere thanks to my project co-ordinator Dr. S. Suresh for his support and guidance.

References


