Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

V2X SAFETY AND SECURITY ISSUES: A REVIEW

Nileema Pathak, *Computer Science and Engineering*, Sandip University, Nashik, India
nileemap@gmail.com
Dr. P.R Patil *Computer Science and Engineering* Sandip University Nashik, India
purushottam.patil@sandipuniversity.edu.in

Abstract— Vehicle to Everything (V2X) is a communication system used in a Vehicular Adhoc Networks that supports the exchange of information from a vehicle to moving components of the traffic system that might impact the vehicle. Technologies such as the Machine Learning, Internet of Things (IoT), 5G, cloud computing, have enhanced the digital capabilities of V2X technology. However, along with communication performance improvement there is increase in security and privacy issues. A trust value has to be calculated to mitigate the uncertainties and risk caused by unreliable information in vehicular environments. In this paper, a fuzzy trust model based on various vehicular parameters is proposed to secure the vehicular network.

Keywords— MDS, V2X, BSM, C-ITS

I. INTRODUCTION

The V2X technology is evolving at a very fast pace. It will transform the mobility ecosystem and the way drivers interact with their surrounding environment. The transportation systems are expected to provide low latency and reliable information flow between various entities involved in the traffic network. V2X communication involves various entities as shown in figure 1. In a Cooperative Intelligent Transportation Systems (C-ITS) these entities, connected vehicles and infrastructure collaboratively interact using specific message formats. Safety messages for V2X communications follow the BSM (Basic Safety Message) standard as stated by the international standards for vehicle communication [1]

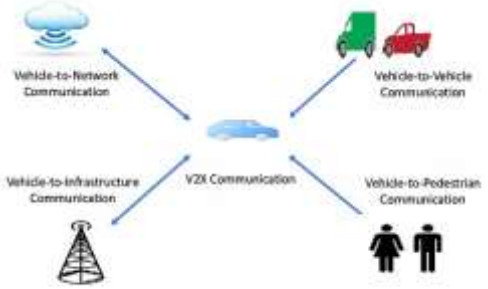

Fig.1 V2X System

As the BSM are constantly broadcasting data such as vehicle speed and location, this raises a threat about how to address privacy and data protection. In this paper the security architecture for handling the misbehaving vehicles in VANET, is discussed.

Vehicles in V2X can face security threats either from external intrusion or internal misbehaviour. Intrusion threats can be caused due to DOS attack, jamming attack, Sybil attack, and Wormhole attacks to name a few [2].
Whereas misbehaviour attacks are initiated from within of the network by capturing a legitimate vehicle and tampering its BSM to share misleading information among the neighbouring vehicles.

Such false information misguides the vehicles who receive the tampered BSM. This can cause dangerous hazards which may impact the traffic flow and also threaten the life of drivers. Therefore, protecting the safety messages from the misbehaving attackers is a very crucial activity to protect the V2X system from road traffic hazards.

Security systems can be classified broadly as proactive and reactive. Proactive security is basically an Intruder Detection system that prevents external attackers to access the system. Public Key Infrastructure (PKI) and certificates issued by authorized entities can be used for providing proactive security. Reactive security is a provision to identify malicious activities within the system, deliberately done by internal attackers. Reactive security systems use mechanisms that analyse system behaviour or state to detect attacks and failures.

II. Misbehavior Detection System

Basic safety message (BSM) are a packet of data generated by a node in a network. BSM packet is made up of information about vehicle status (position, velocity, size etc), timestamp, pseudonym, signature. These messages can be a means of attack and misbehaviour in the system. Misbehaviour Detection System (MDS) as a reactive security measure is required to detect misbehaviour and take action against it.

Misbehaviour in the system can be detected and analysed based on two approaches, namely:

- Entity centric misbehaviour
- Data centric misbehaviour

III. Entity-centric Misbehaviour Detection

Entity or Node misbehaviour detection involves behavioural and trust based detection. The main aim of these mechanisms is to find the trustworthiness of a vehicle or node in a VANET system [4].

Behaviour detection: Behavioural patterns of misbehaving nodes are analysed at protocol level. It also analyses the number of messages transmitted by a node in a particular time duration, or correctness of their format. It does not consider the data semantics.

Trust-based detection: The Trust-based mechanism requires collaborating with infrastructure to find the reputation of the nodes. It works on a recommendation system to find the correctness of information.

IV. Data-centric Misbehaviour Detection

Data-centric misbehavior detection analyses safety messages to verify trustworthiness of packets. It mainly checks for two characteristics in the data, namely plausibility and consistency.

Plausibility based detection is done to check whether the content of a received message is acceptable or not [4].
For example, plausibility of message travelling from one node to another can be verified using two subsequent basic safety messages. The time required and distance travelled is compared with the speed with which the message reaches the destination.

Consistency of information is checked on time series basis for a single packet. Also the consistency of the same data from multiple sources is also checked to determine the trustworthiness of received data. For example, a consistency check can be done to compare the vehicle speed mentioned in newly received message, with the previously calculated average speed of the vehicles that is being

analysed. Deviation from the average value are considered as inconsistent information and can thus be considered suspicious.

V. Misbehaviour Architecture

The misbehaviour detection system can use the local data stored in individual vehicles as well as the data that is stored on the cloud system. The misbehaviour architecture consists of Onboard units (OBU) in individual vehicles, Road side units (RSU) which serves specific area in the VANET environment and the cloud infrastructure that collects information like the vehicle ID, pseudonym of the vehicle, position time series data about all the individual vehicles [2].

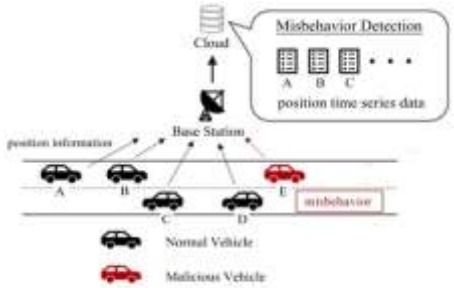

Fig.2 Misbehavior Architecture

Once the misbehaving nodes are detected, the details are stored on the global system. Trustworthiness is based on two types of trusts namely direct trust and indirect trust [6].

Direct trust refers to the trust value associated by between two nodes. It can be calculated based on previous mutual experience between the pair of nodes.
For example node A checks the location parameter of node B for the newly received packet and compares it with a recently received packet from node B to check its validity.

Indirect trust is trust obtained from other source or neighbouring vehicles. Once a trust relation is established between two nodes, the nodes can recommend each other to other nodes in the network. For example, when node A communicates with node B, there is a direct trust between node B and node A, but Node B can also communicate with neighbouring nodes like nodes C and D and ask for their recommendation about node A. Finally, the indirect trust value is collected from all nearby neighbours and an average trust value is calculated. The indirect trust has less weightage as compared to direct trust value [5].

VI. Fuzzy Trust Model

Since there is uncertainty in finding the trustworthiness of a node in a VANET system, Fuzzy logic can be an appropriate approach to identify the discrepancies in the network.
Fuzzy Logic can be used in decision making or classification of the input into fixed output classes, when the input is in a fuzzy state or a grey less state in between 0 and 1 logic.
Fuzzy Logic can be applied in two phases:

- First phase, the node centric method, node authentication is done to check the validity of the node. The invalid nodes are identified as outsiders and are filtered out.
- Second phase, the plausibility and consistency verification, the time stamp of the message is checked. If the received message time is in the acceptable threshold range, it is processed further. Then location accuracy and speed consistency is also checked.

Trust establishment model involves:

- the direct trust establishment wherein every node is responsible to maintain its past experience with the neighbours
- the indirect trust establishment where trust is calculated based on recommendation and collaboration with other nodes and infrastructure
- the above information is used for trust evaluation process through fuzzy logic [7].

Table 1. Fuzzy Logic

Node ID	**Direct Trust**	**Indirect Trust**	**Final Trust**
Node A Node B Node C	1. Static Node centric information verification based on protocol. 2. Local Plausibility, consistency check within trustee and trustor nodes.	1. Behaviour and trust between multiple neighbouring nodes and RSU / Cloud (Recommendation or Reputation system) 2. Plausibility and consistency check in Collaboration with other nodes.	Fuzzy logic applied to direct and Indirect trust weights

A rule base is created to classify the input fuzzy levels to two categories of output namely Trusted node and Not Trusted node. The raw inputs of direct and indirect trust weights are converted into fuzzy sets using the fuzzfier. The fuzzifier output is fed to the inference engine which uses the rule base to classify the input. Finally the defuzzifier converts the fuzzy set obtained from inference engine to a fixed logic.

VII. CONCLUSION

Trust management solutions should be able to identify trustworthy vehicles or messages from untrustworthy once. This is a challenge in ad-hoc networks due to uncertainties in the network. In this paper, we have discussed various threats that contribute to the trust weight calculation and the trust model establishment in VANET. A Fuzzy logic based approach using direct and indirect trust management is proposed. Major challenge in establishing trust is deciding the appropriate trust threshold. False positive and false negative alarms need to be avoided in future work related to misbehaviour detection.

REFERENCES

[1] Sultan Ahmed Almalki & Jia Song "A Review on Data Falsification-Based attacks In Cooperative Intelligent Transportation Systems" International Journal of Computer Science and Security (IJCSS), Volume (14) : Issue (2) : 2020
[2] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi "Trust Establishment Techniques in VANET" Springer-Verlag Berlin Heidelberg 2013 DOI: 10.1007/978-3-642-36169-2_8
[3] Rens W. van der Heijden, Stefan Dietzel, Tim Leinm¨uller, Frank Kargl "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems" IEEE Communications Surveys & Tutorials · October 2016, DOI: 10.1109/COMST.2018.2873088

[4] Xiaoya Xu , Yunpeng Wang and Pengcheng Wang "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks" Hindawi Journal of Advanced Transportation Volume 2022, https://doi.org/10.1155/2022/4725805

[5] Kealan Mannix, Aengus Gorey, Donna O'Shea and Thomas Newe "Sensor Network Environments: A Review of the Attacks and Trust Management Models for Securing Them" Journal of Sensor and Actuator Networks https://doi.org/10.3390/jsan11030043

[6] Toshiki Okamura, Kenya Sato "Misbehavior Detection Method by Time Series Change of Vehicle Position in Vehicle-to-Everything Communication" Journal of Transportation Technologies, April 2021, https://doi.org/10.4236/jtts.2021.112018

[7] Rasheed Hussain , Jooyoung Lee, and Sherali Zeadally "Trust in VANET: A Survey of Current Solutions and Future Research Opportunities"
IEEETransactions on Intelligent Transport Systems IEEE 2020 Digital Object Identifier 10.1109/TITS.2020.2973715

[8] Sohan Gyawali, Yi Qian, and Rose Qingyang Hu "A Privacy-Preserving Misbehavior Detection System in Vehicular Communication Networks" IEEE Transactions on Vehicular Technology : DOI 10.1109/TVT.2021.3079385