International Journal of Modern Science and Technology, 2021;6(8):147-153.
ISSN: 2456-0235.
www.ijmst.co

Research Article

Neighbour node trust identification using cluster approach in VANET

R. Kethsiyal Majella*, S. Sumithra

Department of Electronics and Communication Engineering,
JJ College of Engineering and Technology, Trichy.
Tamilnadu, India.

*Corresponding author's e-mail: kethsi11@gmail.com

Abstract

The dynamic nature of vehicular networks imposes plenty of challenges in multi hop data transmission as links are vulnerable in their existence because of associated mobility of vehicles. Thus, packets frequently find it difficult to induce through to the destination having the limited lifetimes of links. Vehicular Ad-hoc Network (VANET), a novel technology holds a paramount importance within the transportation domain due to its abilities to increase traffic efficiency and safety. However, VANET can also include dishonest nodes like Man-in-the-Middle (MiTM) attackers getting to distribute and share malicious content with the vehicles, thus polluting the network with compromised information. In this regard, establishing trust among connected vehicles can increase security as every participating vehicle will generate and propagate authentic, accurate and trusted content within the network. In this paper propose a unique trust model, namely, Man-in-the-middle Attack Resistance trust model in connected vehicles (MARINE), which identifies dishonest nodes performing MiTM attacks in an efficient way also as revokes their credentials. Every node running MARINE system first establishes trust for the sender by performing multi-dimensional plausibility checks. Once the receiver verifies the trustworthiness of the sender, the received data is then evaluated both directly and indirectly. Extensive simulations are carried out to evaluate the performance and routing framework of MARINE rigorously in terms of the performance over the existing scheme models and the trust model.

Keywords: Vehicular Ad-hoc Network; Trust Model; Man-in-the-Middle; Resistance trust model.

Introduction

Vehicular Ad-hoc Network (VANET), an exceptional sort of versatile impromptu system, is a significant segment of the Intelligent Transportation Systems (ITS). VANETs contain some fixed foundations and a few vehicles, where vehicles go about as versatile hubs that can convey and hand-off information. Every vehicle can speak with different vehicles legitimately framing vehicle-2-vehicle communication (V2V) or speak with a fixed street side unit (RSU), shaping vehicle-2-infrastructure communication (V2I). V2V permits autos to "talk" to one another more than one or numerous bounces utilizing short-go correspondence, however is liable to visit correspondence interruption because of the vehicle joining or leaving from the system, distinctive vehicle speeds or moving headings. V2I is a reasonable arrangement when V2V correspondences are not accessible, yet its presentation relies upon explicit remote innovation and correspondence inclusion of RSUs. Because of the constraints of V2V and V2I, we think about the utilization of half breed vehicular correspondence, named Vehicle-2-X (V2X), to empower the consistent vehicular system network in Fig. 1. Two vehicles out and about can convey either through V2V or V2I, contingent upon the accessible associations and way choice standards [1].

While, in the mid-2000s, VANETs were viewed as a negligible coordinated utilization of MANET standards, they have from that point forward formed into a field of exploration in their own right. By 2015, the term VANET turned out to be for the most part equivalent with the more nonexclusive term Inter Vehicle Communication (IVC), despite the fact that the attention stays on the part of unconstrained systems administration, substantially less on the utilization of framework like Road Side Units

Received: 28.05.2021; Received after Revision: 02.08.2021; Accepted: 05.08.2021; Published: 20.08.2021.

(RSUs) or cell systems. Thusly, customary steering conventions dependent on the presence of a start to finish association can't be embraced straightforwardly in this interesting vehicular condition as moderate hubs can't generally be found between a source and a goal [2].

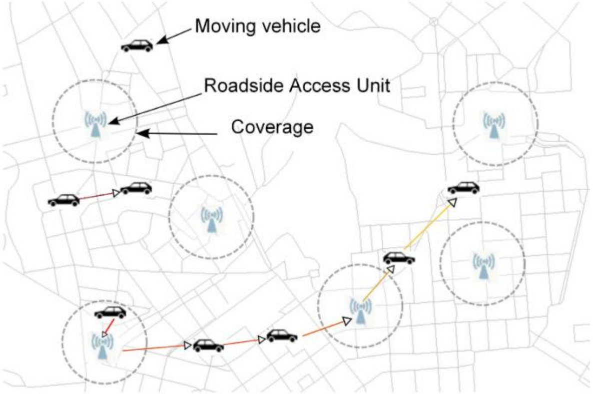

Fig. 1. Vehicular communications in ITS

There is a major test to structure a proficient directing convention to convey a bundle ideal with low dropping rate in VANETs. To accomplish the least deferral, some V2X-based geographic steering approaches are proposed. Their presentation intensely relies upon the vehicle thickness and traffic conditions. Notwithstanding, there is no utilization of forecast in these plans [3]. As moving ways of human frequently show a serious extent of reiteration because of customary visits of specific places and contacts with others during every day exercises, a vehicle's future areas can be anticipated. In the potential directions of moving vehicles are anticipated to encourage the course finding from the source to goal. Be that as it may, the directing exhibition of these investigations is simply dictated by the vehicle appropriation (for example thick or scanty) and vehicle speeds without abusing the fixed correspondence framework.

Our plan centres around three difficulties:

1. How to viably foresee a vehicle's future areas dependent on its past versatility designs
2. How to choose hubs for message handing-off given the anticipated development design toward the goal vehicle; and
3. How to accomplish programmed switch somewhere in the range of V2V and V2I to dodge detachments and guarantee high availability paying little heed to the situations and vehicle speeds in a VANET.

Our plan exploits the history portability and development example to anticipate the future way, where the proposed directing model is misused to proficiently process the time-arrangement information.

Proposed system

The information plane comprises of vehicle On Board Units (OBUs) and Road Side Units (RSUs), and executes activities indicated by the stream rules which are provided by the control plane. For the most part, an information plane node (OBU or RSU) comprises of two remote interfaces, Long Term Evolution (LTE) and Dedicated Short Range Communication (DSRC). The MARINE is a novel and efficient mechanism to evaluate the trust in VANET, which not only integrates the information and opinion shared by vehicles, but also takes the suggestions provided by nearby RSU. MARINE is a lightweight trust model that operates in two stages to evaluate inter-vehicular trust [4].

First, it evaluates the sender node to identify its trustworthiness. This is achieved via previous interactions and the recommendations provided by the neighbouring vehicles.

Second, once node-centric trust is calculated, the received data is evaluated in three distinct dimensions, i.e.,

- Information quality,
- Node’s message forwarding capability, and
- Opinions from neighbours. Data from the sender node is accepted only if both node and data-centric trust is computed successfully.

Otherwise the evaluator node will drop the data. MARINE relies on both vehicles (inter-vehicular trust computation) and RSU (infrastructure-based trust computation) to compute the overall trust on the sender and the received information.

In order to trust the received information, MARINE involves the following two steps, i.e., (1) node-centric trust computation, and (2) data-centric trust computation. Block diagram in fig. 2 shows the various trust computation used.

Node-centric trust computation

In the initiative, MARINE evaluates trust on sender transmitting the protection messages. The communication module embedded within the vehicles enables them to share messages with the neighbouring vehicles in a very specific range, which directly depends on the peak and position of the antenna on the transmitting vehicle. A slight change within the antenna position and height can distort the signal strength, which ultimately leads to a symbol loss. This impacts the message transmission range and therefore the neighbouring vehicles are also unable to receive the transmitted messages [4].

A slight change within the antenna position and height can distort the signal strength, which ultimately ends up in a sign loss. This impacts the message transmission range and also the neighbouring vehicles could also be unable to receive the transmitted messages. In this regard, we define “MRange” as a function of (1) distance (DMSMR) between MS and MR, (2) sender antenna height (ASender), and (3) receiver antenna height (AReceiver).

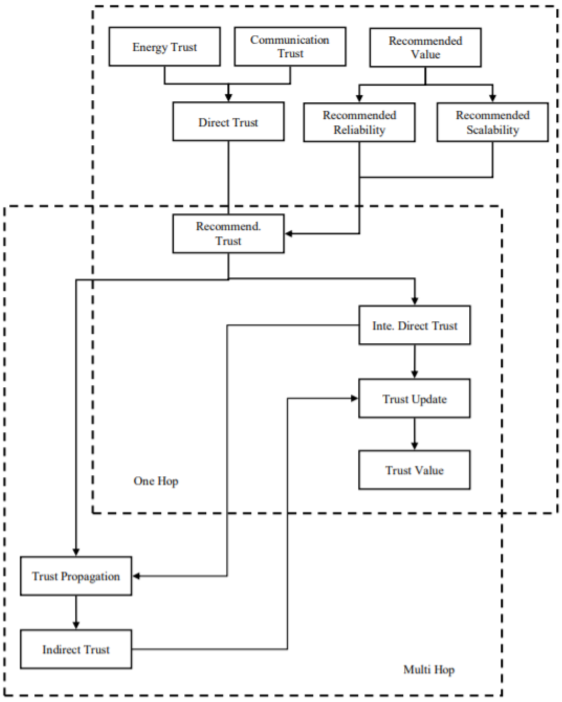

Fig. 2. Block diagram

Data-centric trust computation

Once node centric trust is calculated in Step 1, MR evaluates trust on the content of the received message. Since, messages can be delivered at the MR either directly or through intermediate neighbours, therefore, two methods of trust computation is performed in this step:

Direct Trust Computation

MR computes trust on the received message directly based on two important factors: (1) quality of the received message (MQuality), and (2) ability of the node to disseminate message [5].

Indirect Trust Computation

MARINE also takes into account the opinions generated by the intermediate vehicles. Specifically, the proposed system categorizes opinions provided by ‘n’ neighbor vehicles into two distinct classes, i.e., (1) positive opinions (P O), and (2) negative opinions (NO). Upon receiving an indirect message, MR computes indirect trust (ITR)

Infrastructure-based Trust Computation

Deploying infrastructure (such as RSU) along the road in both urban and rural areas is extremely challenging task due to (1) high cost, and (2) presence of different obstacles, thus affecting the coverage of RSU. However, RSU are often useful in disseminating messages by increasing the coverage area and providing the quasi global view of the general network. Therefore, from the trust management perspective, RSU are often helpful in broadcasting and sharing trusted information with plenty of vehicles.

Global Trust Computation

MARINE facilitates the vehicles to quickly identify MiTM attackers. In MARINE, every vehicle establishes a quasi-global view of the network, which enables them to evaluate trust in both the presence and absence of the RSU [6].

Structure of Trust Model

Through communication behavior of packets transmission between nodes, we calculate the integrated trust by factors including packet loss rate, energy of nodes and the recommendation trust, and it is called trust of node. The range of trust value is set from 0 to 1, and 0 is distrust completely, 1 is trust completely. Characteristics of Trust: Asymmetry, transitivity and composability. Asymmetry, if node A trusts node B, it does not necessarily means that node B trusts node A. Transitivity implies that if node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a center level. Composability means that trust values received from multiple available paths can be composed together to obtain an integrated value.

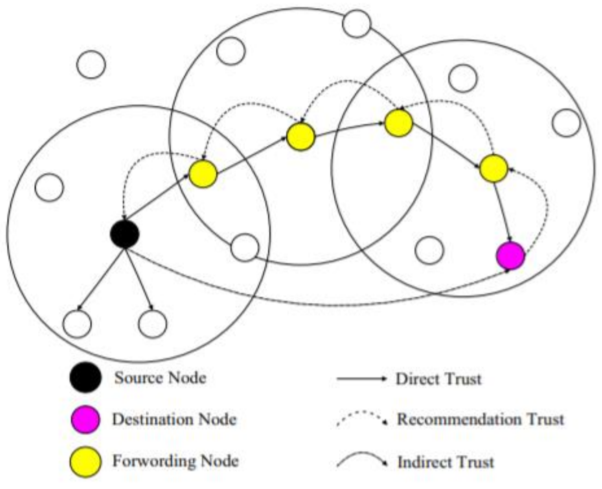

Fig. 3. Various nodes and trust module

One-hop trust module

When the source node wants to obtain the trust value aims at destinations, first of all, it calculates the distance between nodes based on the location (Fig. 3). If the distance is smaller than communication radius, enter into one-hop module. One-hop module contains direct trust module and recommendation trust module. Direct trust module contains communication trust module and energy trust module [7].

Communication Trust

When the distance between source nodes and destination nodes is smaller than that of the communication radius, they can transmit data directly. Based on the number of transferred data packets, the communication trust can be calculated.

Energy Trust

When the source nodes send message to destination nodes, the trust is calculated based on the neighbours' remain energy, to make sure that the forwarding nodes have the ability to receive and forward data packets.

Direct Trust

When the distance between source nodes and destination nodes is smaller than that of the communication radius, by combining communication trust with energy trust, the direst trust between nodes can be calculated.

Recommendation Trust

When the distance between source and destination nodes is smaller than that of the communication radius, they can directly transmit data packets. But if the number of communication packets is not large enough, just calculating the direct trust may not be able to correctly reflect the actual trust value. Set the common neighbors of source and destination nodes as the third party, and the third party provides their own trust aim at destinations to the source nodes, the provided trust is called recommendation trust [8].

Therefore, in one-hop module, the integrate trust between nodes depends on two aspects: direct trust and recommendation trust. If the number of communication packets is larger than or equal to the threshold, only the direct trust needs to be computed. Otherwise, the direct and recommendation trust need to be comprehensively calculated.

Results and discussion

Simulation setup

The proposed conspire and relating elective route(s) are re-enacted in NS-2 discrete occasion test system. The system comprises of 40 nodes initialized in a 1500m × 1500m region. The utilization the data rate 10Kbps model from NS-2, which utilizes an information pace of 10Kbps per connect. The parcel size is 1000 bytes. The portability model is set as "RandomWayPointMobilityModel" from NS-2 library. All the remote hubs in the information plane are overseen by a SDN controller [9]. Simulation parameters are listed in table 1.

Table 1. Simulation parameters

Parameters	Values
Tool	NS2
No. of Nodes	40
Area	150 X 1500
Routing Protocol	Hybrid PRM AODV
Malicious Nodes	1, 2, 4
Traffic	CBR
Transport Layer	UDP
Mobility Type	Random Waypoint
Channel Type	Wireless Channel
MAC Type	IEEE 802.11
Antenna Type	Omni Directional Antenna
Queue Type	DropTail-PriQueue
Queue Length	1000
Simulation START/STOP Time	0.0/5.0 s

Performance metrics

Throughput

It is the ratio of the total number of bits transmitted (Btx) to the time required for this transmission, i.e. the difference of data transmission end time (tend) and start time (tstart).

$T = B_{tx}/(t_{end}-t_{start})$

End-End Delay

The end-end delay of a data packet is characterized as the data packet takes a point in time to travel from the source node to the destination node. D is computed as the ratio of the sum of individual delay of each received data packet to the total number of data packets received.[10]

$D = (\sum_{i=1}^{N_{rec}} D_i)/N_{rec}$

Packet Delivery Ratio

The packet delivery ratio (PDR) of a receiver is characterized as the proportion of the number of data packets actually delivered over the number of data packets transmitted by the source node.

PDR= (no. of packets rec.in dest.)/(no. of packets send by source)

Packet Drop Ratio

The packet drop ratio (PDR) is characterized as the difference between the generated data packets in source node and received data packets in receiver node.

PDR= no. of packets send-no. of packet received

In this module, a wireless mesh network is created with the software defined network. All the nodes are configured and randomly deployed within the network area (Fig. 4). Since our network is a wireless mesh network, nodes are assigned with initial energy, transmitting energy and receiving energy. A routing protocol is implemented in the network. Sender and receiver nodes are randomly selected and therefore the communication is initiated.

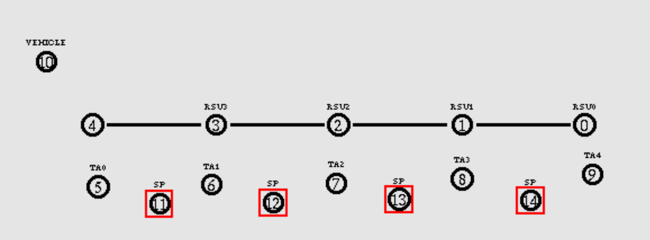

Fig. 4. VANET Deployment

Fig. 5 showing that content can be delivered to the legitimate vehicles in presence of MITM attackers with delaying capabilities. This metric indicates that the messages arrived at the legitimate nodes but with certain delay with low energy consumption. Further, high CBR is achieved within the network in presence of distributed malicious nodes, while, the network with fleet of malicious nodes attains low CBR. This is because of the actual fact that fleet of malicious vehicles are delaying the packets together, thus, high number of packets are delayed in such locations and as a result, the legitimate vehicles receives the content but not in time.

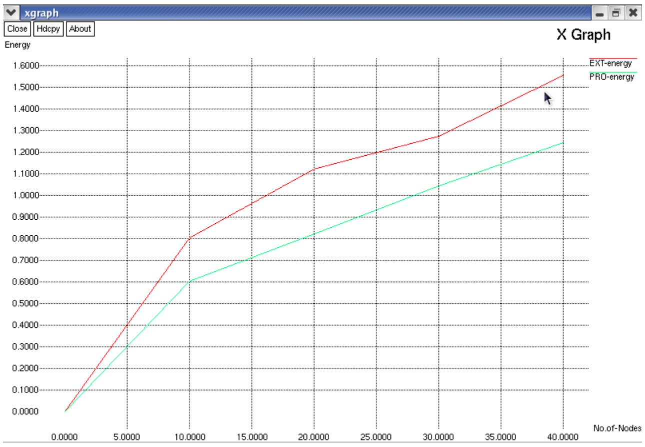

Fig. 5. Energy vs Nodes

Fig. 6 shows end-to-end (E2E) delay within the presence of MITM which are delaying the packets by 2 s. It can be seen that the E2E delay increases when the network is introduced with such dishonest nodes which are delaying the messages. Ideally, the legitimate vehicles should receive such legitimate messages with minimum delay, however, MITM attackers with message delaying capability prohibits the legitimate nodes to receive the messages in time.

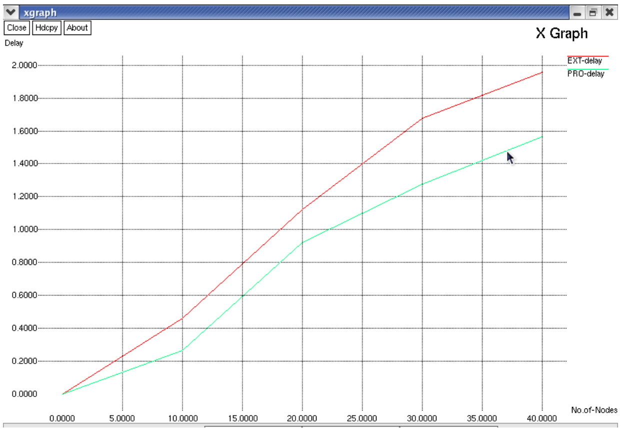

Fig. 6. Delay vs Node

Further, the fig. 7 also depicts that E2E delay increases when the attackers are distributed throughout the network. Since, a large portion of the network is affected because of distributed attackers, therefore, the general E2E delay increases within the network.

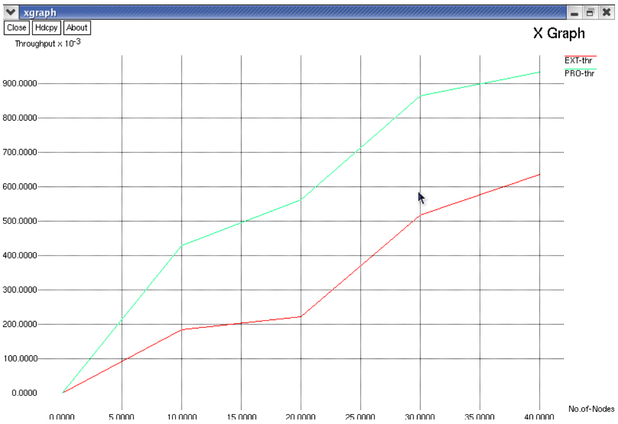

Fig. 7. Troughput vs Delay

Conclusion

VANET is that the prospective for ITS where a secure and attack-free environment is required to realize the specified traffic efficiency. However, due to the open nature of VANET, it is exposed to various attacks, such as MITM attacks. In this paper, presented a novel trust model to increase network security by quickly detecting and revoking dishonest vehicles and their generated content were proposed. This mechanism enables the vehicles to quickly identify misbehaving vehicle along with its malicious content, which is then revoked from the pool of trusted vehicles. Extensive simulations are carried out to the efficiency of MARINE in presence of three different flavours of MiTM attackers. Simulations results suggest that MARINE is an attack resistant trust model which provides high accuracy in detecting trusted content in presence of MiTM attacks.

Conflict of interest

The authors of this work declare no conflict of interest.

References

[1] Zhao J, Cao G. VADD: Vehicle Assisted Data Delivery in Vehicular Ad-hoc Network. IEEE Transactions on Vehicular Technology 2008;57:1910-22.

[2] Wang Q, Fan P, Letaief K. On the Joint V2I and V2V Scheduling for Cooperative VANETS With Network Coding. IEEE Transactions on Vehicular Technology 2012;61:62-73.

[3] He D, Zeadally S, Xu B, Huang X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Information Forensics and Security 2015;10:2681-91.

[4] Du R, Chen C, Yang B, Lu N, Guan X, Shen X. Effective Urban Traffic Monitoring by Vehicular Sensor Networks, IEEE Transactions on Vehicular Technology 2015;64:273-86.

[5] Salahuddin MA, Al-Fuqaha A, Guizani M, Cherkaoui S. Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles. IEEE Internet Things Journal 2015;2:133-44.

[6] Salahuddin M, Al-Fuqaha A, Guizani M. Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles. IEEE Internet of Things Journal 2015;2:133-44.

[7] Liu K. Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as A Software-Defined Network, IEEE/ACM Trans Netw 2016;24:1759-73.

[8] Lyu C, Gu D, Zeng Y, Mohapatra P. PBA: Prediction-Based Authentication for Vehicle-To-Vehicle Communications. IEEE Transactions on Dependable and Secure Computing 2016;13:71–83.

[9] He Z, Cao J, Liu X. SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication. IEEE Netw 2016;30:2-7.

[10] H. Li, M. Dong, and K. Ota, Control Plane Optimization in Software-Defined Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology 2016;65:7895-904.

[11] Zhang L, Wu Q, Domingo-Ferrer J, Qin B, Hu C. Distributed Aggregate Privacy-Preserving Authentication in VANETS. IEEE Transactions on Intelligent Transportation Systems 2017;18:516-26.

[12] Jo HJ, Kim IS, Lee DH. Reliable Cooperative Authentication for Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems 2018;19:1065-79.

[13] Ghafoor H, Koo I. CR-SDVN: A Cognitive Routing Protocol for Software-

Defined Vehicular Networks. IEEE Sensors J 2018;18:1761-72.

[14] Weng J, Weng J, Zhang Y, Luo W, Lan W. BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN-based VANET. IEEE Transactions on Vehicular Technology 2019;68:822-31.

****