International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 3327-3333
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

ACCIDENT ALERT MESSAGE TRANSMISSION USING VANET

[1]B.Sathyasri , [2]Priyanka Paree Alphons
[1]Assistant Professor .[2]UG Student ,Electronics And Communication Engineering.
VEL TECH ,Avadi ,Chennai -6000 062,Tamil Nadu,India
Priyankasaagar97@gmail.com

Abstract:

Vehicular ad hoc networks (VANETs) have the prospective to transform the way people travel through the creation of exchanging and making use of information with wireless communications network . However, VANETs are vulnerable to security threats due to increasing reliance on communication, computing, and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality,non repudiation ,access control, real-time operational constraints/demands, availability, and privacy protection. In this paper, an attack-resistant trust management scheme (ART) is proposed for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Particularly, data trust is evaluated based on the data sensed and collected from multiple vehicles. The proposed trust management theme is valid to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

Keywords: **ART**(Attack resistant trust),VANET(vehiclular Ad-Hoc networks), mobile nodes ,environmental protection ,trustworthiness.

Introduction

In the growing needs for increased safety and efficiency of road transportation system have promoted automobile manufacturers to integrate wireless communications and networking into vehicles. The wirelessly networked vehicles naturally form Vehicular Ad-hoc Networks(VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need of centralized administration. VANETs have the prospective to transform the way people travel through creations of exchanging and making use of information wireless communications network .In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing ,processing, and wireless communication capabilities. Both Vehicle-to Vehicle(V2V)andVehicletoInfrastructure(V2I) communication enable safety applications that provide warnings regarding road accidents, traffic conditions (e.g., congestion, emergency braking, icy road) and other relevant transportation events. However, VANETs are vulnerable to threats due to increasing reliance on communication, computing and control technologies. The unique security and privacy challenges posed by VANETs include integrity (data trust), confidential, non repudiation, access control, real-time operational constraints demands, availability, and privacy protection. VANET became progressively important and popular in many countries as part of the Intelligent Transportation Systems (ITSs), as it is foreseen and envisioned to alleviate many of the current transportation problems and will allow a wide spectrum of promising ITS applications Even though VANETs enable many attractive features and applications, inevitably their security will incur countless challenges, threats, vulnerabilities and risks if such security sensitive networks did not address and account for security requirements prior to deployment. An explainable example - if a time-critical message sent by an

"innocent" vehicle and was intentionally modified or discarded or re-routed to the misguided receiving unit by an routing vehicle, severe consequences will be the result (e.g. the innocent vehicle may get accused, possible injuries and deaths, etc). The demands the growth of a robust and reliable security method and need intensive and deep studies to help in preventing nasty activities in the network. Many funded-projects on VANET security have been actively conducted mainly by USA, Japan and the European Union.

VANET Architecture:

Figure.(1) shows the basic VANET network architecture has the following main compone (V) equipped with on-board unit (OBU), (2) (RSU) sparsely distributed all over the netwo network infrastructure, and the Trusted Communications can be V2V or V2I. RSU with wider coverage than vehicles coverag generally equipped with GPS units for positi license plate (ELP) for vehicle identification and ranging (RADAR)/light amplification amplification of radiation (LASER) techn used for knowing the position of other ve supplied with high battery power. A trusted may be installed in the back end. The O communicate wirelessly using the Dedicat Communications (DSRC) protocol, and has 75 MHz at 5.9 GHz frequency, whereas th communicate using a secure fixed netw Internet).

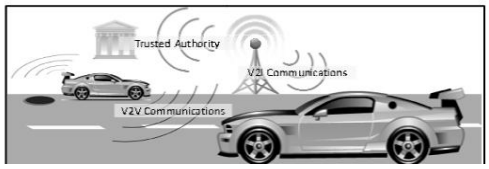


Fig.1Illustrative VANET architecture.

Existing System:/ Literature survey:

A.In this proposed ART scheme is presented in details. The ART scheme addresses two types of trustworthiness in VANETs, data trust and node trust [1]

A.Preliminaries In general ,the trust worthiness of a node Nk can be defined as a vector Θ k =(θ(1) k ,θ(2) k ,...,θ(n) k), in which θ(i) k stands for the

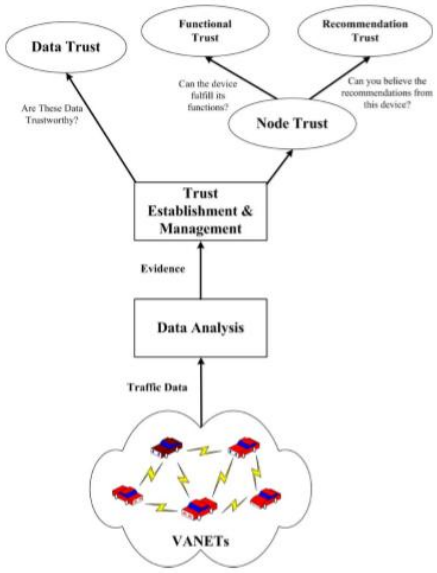


Fig. 2. Overview of the ART scheme.

i-th dimension of the trustworthiness for the node Nk. Each dimension of the trustworthiness θ(i) k corresponds to one or a certain category of behaviour (s) B(i) k (such as packet forwarding or true recommendation sharing), and θ(i) k can properly reflect the probability with which the node will conduct B(i) k in an appropriate manner[1].θ(i) k can be assigned any real value in the range of [0,1], i.e., ∀i∈{ 1,2,3,4,...,n}, θ(i) k ∈[0,1].The higher the value of θ(i) k , the node Nk is more likely to conduct B(i) k properly. Each dimension of the trustworthiness θ(i) k for the node Nk is defined as a function of the misbehaviors M(i) k that are related to B(i) k and have been observed by the neighbors of the device Nk. Different dimensions of the trustworth in easy correspond to different functions, and the selection of different functions should coincide with the basic features of M(i) k , such as severity of the outcome, occurrence frequency, and context in which they occur. In particular, the

trustworthiness of a device is represented in a vector Θk =(θ(1) k ,θ(2) k), and each element in the vector stands for functional trust and recommendation trust, respectively[1]. In the future, if it is necessary to introduce new element to the trust vector,the new element can be added easily.

B. Scheme Overview The ART scheme is composed of two phases, namely data analysis and trust management. The schematic diagram of the ART scheme is depicted we first collect traffic data from VANETs for data analysis[2]. Second, we summarize the findings from the data analysis as evidences for trust management schemes to evaluate the trustworthiness. The details of the evidence combination are presented in Section IV-C. Then these evidences will be used to assess the trustworthiness of data and nodes. The trust worth in ess of nodes further consists of functional trust and recommendation trust. The details of the evaluation of trust recommendation using collaborative filtering are provided in Section IV-D.

C. Evidence Combination Evidence combination is very important for the proposed ART scheme.Because some of the traffic data are not reliable[6],it is critical to find an evidence combination technique to properly fuse together multiple pieces of evidence in presence of both trustworthy and untrustworthy data. Thus, it is necessary to combine multiple pieces of evidences so that both data trust and functional trust can be properly evaluated

Proposed System:

The unique security and privacy challenges posed by VANETs include integrity (data trust), confidentiality, non repudiation, access control, real-time operational constraints/demands, availability, and privacy protection. The trustworthiness of VANETs could be improved by addressing holistically both data trust, which is defined as the assessment of whether or not and to what extent the reported traffic data are dependable, and node trust, which is defined as how reliable on nodes in VANETs are. In this system, an attack-resistant trust management scheme (ART) is proposed for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. The data trust is checked by sending and collected from multiple vehicles, node trust is based on two dimensions (i.e) functional trust and reference trust, that indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively[3]. The successful and effectiveness of the planned ART scheme is validated from beginning to end extensive experiments. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced. We also implement trust based credit model, which combines all details like data trust, functionalities trust and node trust in a VANET group based on that it will make communication among wide network

Modules:

1. Trans receiver

It consists of Transmitter as well as receiver configuration, which act as a VANET node.
An electronic button allows the transmitter and receiver to be linked to the same satellite dish, and prevents the transmitter output from destructive receiver.

2. TCP

Transmission control protocol is the responsibility for communication .The Transmission Control Protocol (**TCP**) is one of the main protocols of the Internet protocol suite. Its originated in the original network performance in which it complement the Internet Protocol (IP). consequently, the entire suite is commonly referred to as **TCP**/IP.
It determines how to break application data into packets that networks can deliver, sends

packets to and accepts packets from the network layer, manages flow control, and cause it is meant to provide fault less data transmission handle retransmission of dropped or distorted packets and acknowledgement of all packet that arrived.

3. CBR (Constant bit rate):

Constant bit rate (**CBR**) is used in telecommunications, describing to the quality of service. Compare with variable bit rate. When searching for codes, CBR encoding means the rate at which a codec's output data should be constant.

The problem of not allocating enough data for complex sections could be solved by choosing a high bitrate to ensure that there will be enough bits for the entire encoding process, though the size of the file at the end would be proportionally larger.

4. Trust value generation

It gives the data trust, node trust, functional trust and recommendation trust for each communication.

5. Trust based credit value assigner

It receives all trust values and assign a credit value for a particular node and communication.

6. Data and traffic analyzer

It analyze the size and content of the data and traffic in the network.

The traffic data from network traffic study help in:

- Understanding and evaluating the network utilization
- Download/upload speeds
- category, amount, origin and destination and content/data of packets

Result Analysis:

The result analysis gives us the knowledge about how the system works , this assumption is done by actually fixing a device inside the car to get the transmission of signals .

Considering the number of vehicles moving on the road and Fig.3 tells us about the less number of vehicles denoting the blue colour on the road .The next yellow colour in Fig.4 ,denotes the medium number of vehicles on the road ,as well as the green colour in Fig 5,Which denotes the larger number of vehicles on the road .The (Fig 6)denotes the vehicles meeting with an accident with the red colour .According to Ns2 module a collision has occurred .The network which is set next to the road gets the accident alert and send it to server and then these signals (Fig.7)are been sent to the other vehicles coming in that path. After reciving the alert message in vechiles coming in that path ,they change their direction (Fig.8),means take another route to reach their destination, which is denoted by the violet colour in the output .

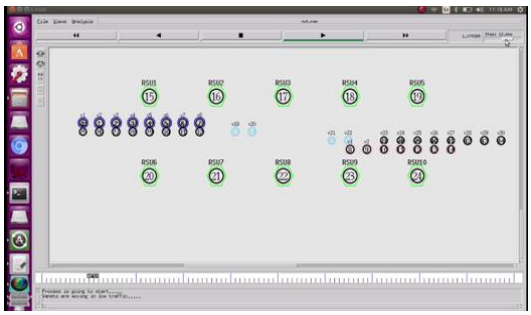


Fig.3 denoting the less number of vehicles passing

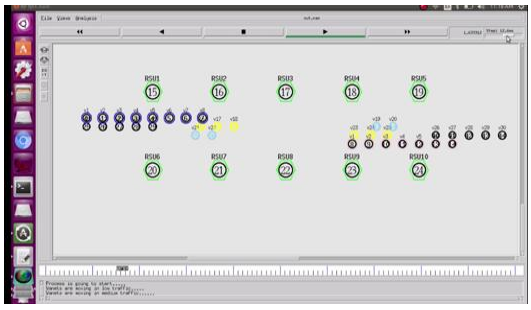


Fig .4 denoting the medium number of vehicles passing.

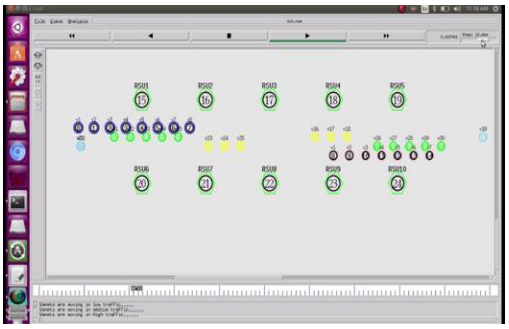


Fig.5 Denoting the larger number of vehicles passing .

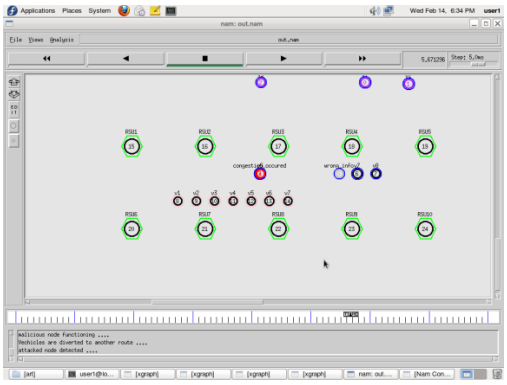


Fig 6.Collision occurred on the road .

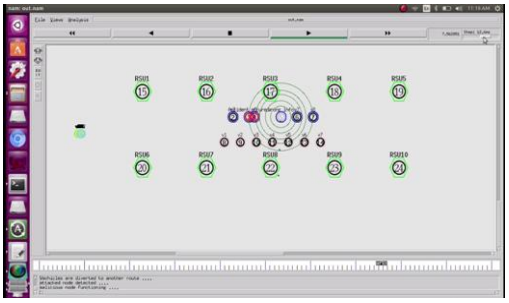


Fig.7 When collision (accident) occurs the network receives the signal and passes the accident alert to the vehicles coming in that path.

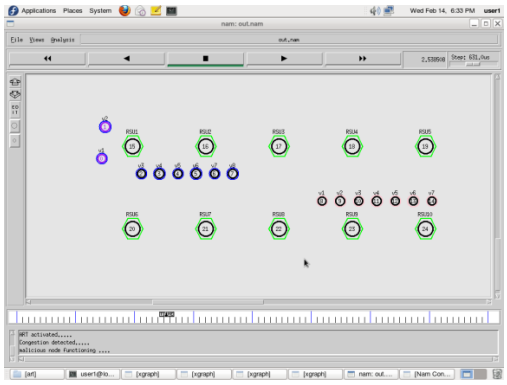


Fig 8.vehicles changing their in paths after the alert message

Graphical Result:

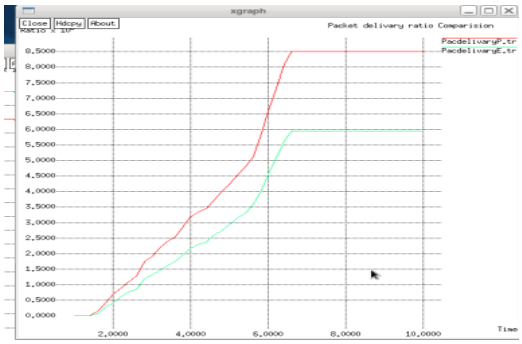


Fig.9 this graph is a comparison between old and new throughput .

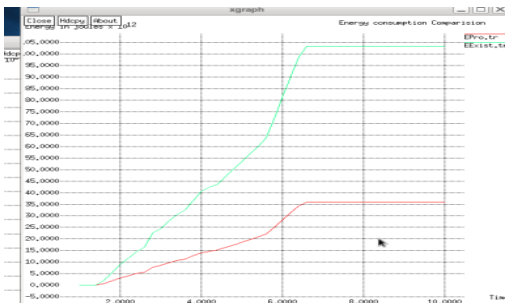


Fig.10 this graph denotes the comparison between old and ne energy.

Conclusion:

In this paper, an attack-resistant trust management scheme named ART is proposed to evaluate the trustworthiness of both traffic data and vehicle nodes for VANETs. In the ART scheme, the trustworthiness of data and nodes are modeled and evaluated as two

separate metrics, namely data trust and node trust, respectively. In particular, data trust is used to assess whether or not and to what extent the reported traffic data are trustworthy. On the other hand, node trust indicates how trustworthy the nodes in VANETs are b.To validate the proposed trust management scheme, extensive experiments have been conducted, and experimental results show that the proposed ART scheme accurately evaluates the trustworthiness of data as well as nodes in VANETs, and it can also cope with various malicious attacks.

References

[1] Wenjia Li, Houbing Song "Attack-Resistant Trust(ART)Management Scheme for Securing Vehicular Ad Hoc Networks" 2016

[2] R. K. Rout, "A survey on object detection and tracking algorithms," Ph.D. dissertation, 2013.

[3] C. Stauffer and W. E. L. Grimson, "Learning patterns of activity using real-time tracking,"

Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 22, no. 8, pp. 747–757,

2000.

[4] A. Yilmaz, O. Javed, and M. Shah, "Object tracking: A survey," Acm computing surveys

(CSUR), vol. 38, no. 4, p. 13, 2006.

[5] C. Stauffer and W. E. L. Grimson, "Learning patterns of activity using real-time tracking,"Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 22, no. 8, pp. 747–757, 2000.

[6] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," Vehicular system.