A Trustworthiness of Traffic Data and Mobile Nodes using VANET

M. Magesh Babu*, J. Vishnu Priya**, K.Vimala***, V. Vithya**** & P. Yuvarani Mangalam*****

*Assistant Professor, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
E-Mail: deivam_bmmb{at}yahoo{dot}co{dot}in
**UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
***UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
*****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.

***Abstract*—**Vehicular ad hoc networks (VANETs) have the potential to transform the way people travel through the creation of a safe interoperable wireless communications network that includes cars, buses, traffic signals, cell phones, and other devices. 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. 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 trustworthy, and node trust, which is defined as how trustworthy the nodes in VANETs are. 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. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. The effectiveness and efficiency of the proposed ART scheme is validated through 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 trustworthiness.

***Keywords*—**Privacy; Security; Trust Management Scheme; Trustworthiness; VANETs.

***Abbreviations*—**Attack-Resistant Trust (ART); Quality-of-Service (QoS); Vehicular Ad Hoc Networks (VANETs); Wireless Fidelity (WiFi); Wireless Local Area Network (WLAN).

I. INTRODUCTION

VEHICULAR Ad-hoc Networks (VANETs) are a special form of wireless networks made by vehicles communicating among themselves on roads. The conventional routing protocols proposed for Mobile Ad-hoc Networks (MANETs) work poorly in VANETs. As communication links break more frequently in VANETs than in MANETs, the routing reliability of such highly dynamic networks needs to be paid special attention. To date, very little research has focused on the routing reliability of VANETs on highways. In this paper, we use the evolving graph theory to model the VANET communication graph on a highway. The extended evolving graph helps capture the evolving characteristics of the vehicular network topology and determines the reliable routes preemptively. This paper is the first to propose an evolving graph-based reliable routing scheme for VANETs to facilitate Quality-of-Service (QoS) support in the routing process. A new algorithm is developed to find the most reliable route in the VANET evolving graph from the source to the destination. We demonstrate, through the simulation results, that our proposed scheme significantly outperforms the related protocols in the literature [Engoulou et al., 1; Kakkasageri & Manvi, 2].

II. VANETs STRUCTURE

Vehicular networks are expected to utilize various wireless access technologies in its communications, such as Dedicated Short-Range Communications (DSRC, 5.9GHz), which was developed in response to highly dynamic environments in order to grant transferring data at high rates, such signals can reach up to 1000 M. Some of other wireless technologies are Worldwide Interoperability for Mobile Access (Wi-MAX),

cellular systems, Wireless Local Area Network (WLAN) and Wireless Fidelity (WiFi). The nodes are equipped with particular devices to enable the communications between each other in a wireless manner, any node in ad hoc networks can commonly act as either a host which inquiries data or a router which forwards data. Correspondingly, there are two types of nodes in VANETs [Sharef et al., 3].

Vehicles: Which represents the mobile nodes, this type of nodes equipped with several devices such as: On Board Unit (OBU), an OBU composed of wireless transmitter and receiver units that mounted on a vehicle and responsible for the communications with other nodes in the network. Other installed devices are Event Data Recorder (EDR) and Tamper Proof Device (TPD). The EDR stores critical data about vehicles such as speed, position, time, transmissions and receives messages, trip details, etc. The EDR acts as a black box in an aero plane, the stored data is useful especially in post-accident analysis, since it provides data about the vehicle before, during and after the accident, which give an accurate and reliable picture of accidents reasons. Whereas the TPD holds secret information such as cryptographic material, driver identity, in addition to carrying out cryptographic operations by processing, signing and verifying the exchanged messages. The vehicles also supplied with different sensors to collect data to process/share it depending on its importance [Al-Sultan et al., 4].

RSU: Which represents the fixed infrastructure nodes (base stations), it plays as a router or gateway among vehicles themselves and between vehicles and external networks like the internet. As the range of ad hoc network is relatively limited to short distance, the RSUs can extend the range by re-distributing the information to forward it to other OBUs. The RSUs are deployed along the roadsides and can be connected to backbone networks to furnish different network applications and services. Vehicular Ad Hoc Networks have mainly two types of communications: Vehicular to Vehicular communications (V2V), and Vehicular to Infrastructure communications (V2I - I2V), see figure 1. In the first type, vehicles communicate directly with other vehicles by exchanging messages with each other. Whereas in the latter, the communications are done between vehicles and fixed infrastructures (i.e. RSUs). The communications could be either in a single hop or multi-hop manner, depending on the distance between the intended nodes. The RSUs also can communicate with each other to form Infrastructure to Infrastructure communications (I2I). These communications can be utilized to build efficient applications that enable safe and comfort transportation for passengers [Raya & Hubaux, 5].

From figure 2, we find that the sensor in a vehicle detects an accident ahead, and then it reports this accident to the system. Therefore, the traffic alert shown in figure 2 is true.

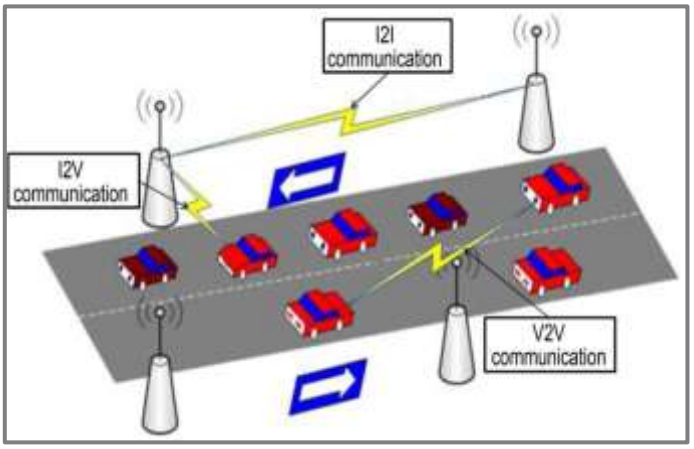

Figure 1: VANET's Communication

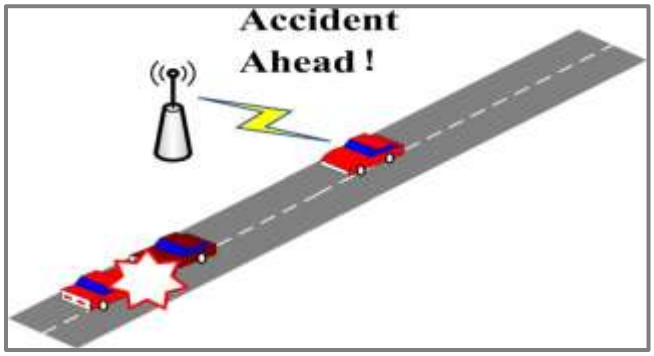

Figure 2: Traffic Alert

III. TRUST ESTABLISHMENT AND MANAGEMENT IN AD HOC NETWORKS

The main purpose of trust management is to assess various behaviors of other nodes and build a reputation for each node based on the behavior assessment. The reputation can be utilized to determine trustworthiness for other nodes, make choices on which nodes to cooperate with, and even take action to punish an untrustworthy node if necessary [Lin & Song, 6].

In general, the trust management system usually relies on two sorts of observations to evaluate the node behaviors. The first kind of observation is named as *first-hand* observation, or in other words, direct observation. First-hand observation is the observation that is directly made by the node itself, and the first-hand observation can be collected either passively or actively. If a node promiscuously observes its neighbors' actions, the local information is collected passively [Angwin & Valentino, 7].

In contrast, the reputation management system can also rely on some explicit evidences to assess the neighbor behaviors, such as an acknowledgement packet during the route discovery process. The other kind of observation is called second-hand observation or indirect observation. Second-hand observation is generally obtained by exchanging first-hand observations with other nodes in the network. The main disadvantages of second-hand observations are related to overhead, false report and collusion [8; Douceur, 9; Hu et al., 10].

IV. MODULES

- Back-bone nodes at intersection.
- Packet forwarding.
- Message queuing and retrieval
- Back-bone nodes at road segment [Nait-Abdesselam et al., 11].

4.1. Back-bone Nodes at Intersection

Back-bone nodes of this kind are of three types, namely, stable, primary, and secondary back bones. A stable back-bone node is selected from the stream of vehicles waiting at the intersection during red traffic signal. Among the waiting vehicles, the vehicle closest to the intersection declares itself as the stable back bone [Buchegger & Le Boudee, 12].

4.2. Packet Forwarding

A back-bone node is always preferred. This is because back-bone nodes can maintain the communication history and store packet in the absence of a forwarder at the intersection. A forwarding node checks its neighbor list to probe the available back-bone nodes. It compares the packet forwarding time with the staying time of each back bone node. If the forwarding node is moving, it prefers stable back-bone nodes as the forwarder [Yau & Mitchell, 13].

4.3. Message Queuing and Retrieval

The stable back-bone nodes take the responsibility of packet buffering. In the absence of a suitable forwarding node, the packet is stored in a stable back-bone node. On availability of a forwarding node in the desired direction, packet is retrieved and forwarded. The stable back-bone nodes maintain the database of all communications with a timestamp. They store source and destination addresses along with the time of arrival of packets [Mejri et al., 14].

4.4. Back-Bone Nodes at Road Segment

The part of a road segment longer than the transmission range is devoid of nodes, it can be noticed by the nodes present at the periphery of the void region. Nodes closest to the void region from both directions declare themselves as back-bone nodes. These backbone nodes are termed as "void-guard" back-bone nodes. The purpose of a "void-guard" back-bone node is to inform the presence of a void region to the neighboring back-bone nodes stationed at intersections.

V. EXISTING SYSTEM

- Traffic Estimation and Prediction System (TrEPS).
- Validation and Evidence combination algorithm.

5.1. Disadvantage

- Traffic information are not secured.
- Short range.
- TrEPS may encounter confusing or even conflicting traffic information reported by multiple sources.

VI. PROPOSED SYSTEM

- Attack resistance trust management scheme.
- Collaborative filtering algorithm.
- 3GEP algorithm.

6.1. Advantages

- Secured traffic data.
- Increased range.
- Speedy message passing.

6.2. Applications

- Time Utilization
- Route Diversions
- Active prediction

VII. OUTPUT

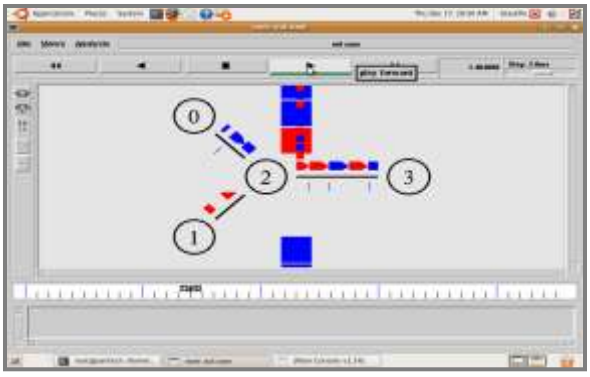

Figure 3: Simulated Output of NAM

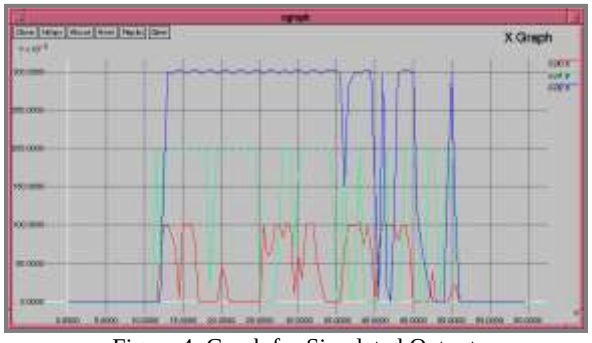

Figure 4: Graph for Simulated Output

VIII. CONCLUSION

Vehicular Ad Hoc Network is a promising research area that bodes for better transportation in future. 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 VANET's are.

REFERENCES

[1] R.G. Engoulou, M. Bellache, S. Pierre & A. Quintero (2014), "VANET Security Surveys", *Computer Communications*, Vol. 44, Pp. 1–13.

[2] M. Kakkasageri & S. Manvi (2014), "Information Management in Vehicular Ad Hoc Networks: A Review", *Journal of Network and Computer Applications*, Vol. 39, Pp. 334–350.

[3] B.T. Sharef, R.A. Alsaqour & M. Ismail (2014), "Vehicular Communication Ad Hoc Routing Protocols: A Survey", *Journal of Network and Computer Applications*, Vol. 40, Pp. 363–396.

[4] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti & H. Zedan (2014), "A Comprehensive Survey on Vehicular Ad Hoc Network", *Journal of Network and Computer Applications*, Vol. 37, Pp. 380–392.

[5] M. Raya & J.P. Hubaux (2007), "Securing Vehicular Ad Hoc Networks", *Journal of Computer Security*, Vol. 15, No. 1, Pp. 39–68.

[6] Y. Lin & H. Song (2006), "DynaCHINA: Real-Time Traffic Estimation and Prediction", *IEEE Pervasive Computing*, Vol. 5, No. 4, Pp. 65–65.

[7] J. Angwin & J. Valentino (2011), "Devries, Apple, Google Collect User Data", Apr. 2011. [Online]. Available: http://www.wsj.com/articles/SB10001424052748703983704576277101723453610

[8] Waze Mobile, Free Community-Based Mapping, Traffic & Navigation App. [Online]. Available: https://www.waze.com/

[9] J.R. Douceur (2002), "The Sybil Attack", *International Workshop on Peerto-Peer Systems, Ser. Lecture Notes in Computer Science*, P. Druschel, F. Kaashoek & A. Rowstron, Vol. 2429. Berlin, Germany: *Springer-Verlag*, Pp. 251–260.

[10] Y.C. Hu, A. Perrig & D.B. Johnson (2002), "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", *Proceedings of the 8th ACM Annual International Conference on Mobile Computing and Networking*, Atlanta, GA, USA, Pp. 12–23.

[11] F. Nait-Abdesselam, B. Bensaou & T. Taleb (2008), "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", *IEEE Communications Magazine*, Vol. 46, No. 4, Pp. 127–133.

[12] S. Buchegger & J.Y. Le Boudee (2005), "Self-Policing Mobile Ad Hoc Networks by Reputation Systems", *IEEE Communications Magazine*, Vol. 43, No. 7, Pp. 101–107.

[13] P.W. Yau & C.J. Mitchell (203), "Security Vulnerabilities in Ad Hoc Networks", *Proceedings of 7th International Symposium on Communication Theory and Applications*, Pp. 99–104.

[14] M.N. Mejri, J. Ben-Othman & M. Hamdi (2014), "Survey on VANET Security Challenges and Possible Cryptographic Solutions", *Vehicular Communications*, Vol. 1, No. 2, Pp. 53–66.