International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 19
August 2018

A Novel Predictablevehicular Ad Hoc Networks by Using Trustworthiness Evaluation-Based Routingprotocol

S.N.Neelima & C.H.Sudarsan Raju
[1] *M.Tech student, Department of ECE, BIT Institute Of Technology, Hindupur.*
[2] *Associate Professor, Department of ECE, BIT Institute Of Technology, Hindupur.*

Abstract--- *Vehicle networks (Vehicular Ad hoc Networks, VANETs) are considered similar to Online Social Networks (OSNs). There are many predictable elements in social networks. Incompletely predictable vehicular ad hoc networks is a type of networks where vehicles move in a certain range or just in a particular tendency, which is very similar to some circumstances in reality. In addition to the traveling path of a vehicle, the trustworthiness of it is also crucial in several field of today daily life. It is significant that the algorithm for calculating the vehicle's trustworthiness should be able to fully express attributes of the vehicle and the relationship among attributes.*

Index Terms— ***Incompletely Predicable Networks, VANETs, Trustworthiness Evaluation, Routing Protocol, Self-Configured Networks.***

1. INTRODUCTION

Vehicular Ad-Hoc Networks, (VANET), are a particular kind of Mobile Ad Hoc Network, (MANET), in which vehicles act as nodes and each vehicle is equipped with transmission capabilities which are interconnected to form a network. The topology created by vehicles is usually very dynamic and significantly non-uniformly distributed. In order to transfer information about these kinds of networks, standard MANET routing algorithms are not appropriate (Lee *et al.*, 2010b).

The availability of navigation systems on each vehicle makes it aware of its geographic location as well as its neighbours. However, a particular kind of routing approach, called Geographic Routing, becomes possible where packets are forwarded to a destination simply by choosing a neighbour who is geographically closer to that destination. With the rapid growth of vehicles and roadside traffic monitors, the advancement of navigation systems, and the low cost of wireless network devices, promising peer-to-peer (P2P) applications and externally-driven services to vehicles became available. For this purpose, the Intelligent Transportation Systems (ITS) have proposed the Wireless Access in Vehicular Environments (WAVE) standards that define an architecture that collectively enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications (ITS, 2012). According to architectures of network, VANET can be divided into three categories, the first of which is the Wireless Wide Area Network (WWAN) in which the access points of the cellular gateways are fixed in order to allow direct communication between the vehicles and the access points. However, these access points require costly installation, which is not feasible. The second category is the Hybrid Wireless Architecture in which WWAN access points are used at certain points while an ad hoc communication provides access and communication in between those access points. The third and final category is the Ad Hoc V2V Communication which does not require any fixed access points in order for the vehicles to communicate. Vehicles are equipped with wireless network cards, and a spontaneous setting up of an ad hoc network can be done for each vehicle (Li and Wang, 2007). This study will focus on studying ad hoc V2V communication networks, which are also known as VANETs. The purpose of VANET is to allow wireless communication between vehicles on the road including the roadside wireless sensors, enabling the transfer of information to ensure driving safety and planning for dynamic routing, allowing mobile sensing as well as providing in-car entertainment. As VANETs have unique characteristics which include dynamic topology, frequent disconnection of the networks, and varying environments for communication, the routing protocols for traditional MANET such as Ad hoc On-demand Distance Vector (AODV) (Perkins and Royer, 1999) are not directly usable for VANETs. Researchers have developed a variety of efficient routing protocols for VANETs including Greedy Perimeter Stateless Routing (GPSR) (Karp and Kung, 2000); Greedy Perimeter Coordinator Routing (GPCR) (Lochert *et al.*, 2005); and GpsrJ+ (Lee *et al.*, 2007). The current issue, however, is

that the range of the wireless sensors on vehicles is limited to a few hundred meters at most and the traffic conditions in a vehicular urban environment often change dynamically. Other than that, VANET routing protocols also face other problems including the issue of unstructured roads, the difference in the sizes of the intersections in a certain area, the sharp curves of the roads, uneven slopes, and other obstacles such as large buildings, traffic lights, trees, and sign boards. As it is impractical to spend excessively on rebuilding or restructuring the existing roads in urban environments, a routing protocol for the purpose of a larger distance of data communication in one-to-one and one-to-many transfers specifically for VANETs need to be developed.

RELATED WORK

Theodorakopoulos et al: [45] define the trust evaluation process as a path problem in a direct graph. They claim that their method is robust to current attacks. A graph based trust evaluation is also contained where its methodologies and challenges when applied to the case of online social networks are explained.

Jiang et al: [47] present a user-domain-based trusted acquaintance chain discovery algorithm to take advantage of potential relationships in on-line social networks. In fact vehicle networks are also a type of social networks, the work mentioned by Jiang et al: is worthy of reference. There have been many trust models that are worthy of reference being presented for other fields in recent years. Although not designed specifically for routing protocols in vehicle networks, these trust models and methods have a certain reference value.

Mohsenzadeh et al: present a fuzzy mathematics based trust evaluation model for cloud computing according to records of interaction between cloud entities. Simulation experiments show that the proposed model can effectively identify malicious entities, and assist the system to correctly make security decisions.

Wang et al: [55] present a reputation management scheme for pseudonym-enabled VANETs. Two types of reputations are defined, which are named as the service reputation and the feedback reputation. Reputation accumulation algorithms are designed based on the information entropy and the majority rule. They claim that their scheme is robust against the tactical attack and can preserve privacy against the reputation link attack during pseudonym changes

2. EXISTING SYSTEM

❖ After having an appropriate algorithm to compute the vehicle trustworthiness, a robust center for big data collection, analysis and trustworthiness distribution is also demanded. As is well known, the most important features of cloud computing are distributed computing and mass storage.

❖ Applying the features of cloud computing into practice, researchers have proposed many outstanding schemes and protocols in their own fields. It is agood choice to use the cloud to collect, store and analyze attribute parameters to provide the trustworthiness of any vehicle to the nodes querying for the vehicle's trustworthiness

Disadvantage

❖ Although many protocol shave been proposed for vehicle networks, some open issues, such as network feature utilization and trustworthiness evaluation, etc., have not yet been resolved.

❖ From one side, relationships among different time stamp sand positions in the same vehicle are not fully used as the important information for routing search.

❖ In traditional routing protocols, routing situations at each moment are usually considered separately. However, the continuity of vehicle movement in time is ignored.

❖ On the other side, there is no way to completely avoid the current trustworthiness mechanism from providing false or unfair trustworthiness value.

❖ In a trusted scheme or mechanism, its own trustworthiness value is mainly given by the node itself, or decided by team members.

3. PROPOSED SYSTEM

❖ In this paper, we proposed a trustworthiness evaluation based routing protocol (TERP). The

trustworthiness of every vehicle is taken into consideration, which is obtained through the attribute parameters of the vehicle and is provided by the cloud. The cloud is used in order to host the vast amount of historical big data related to vehicle activities, on which the trust evaluation is based.

❖ The cloud server acts as a trusted third part to provide fair trustworthiness evaluation. This avoids problems caused by different criteria for the evaluation of vehicle trustworthiness. At the same time, the cloud server can also reduce the calculation and storage overhead of each vehicle terminal.

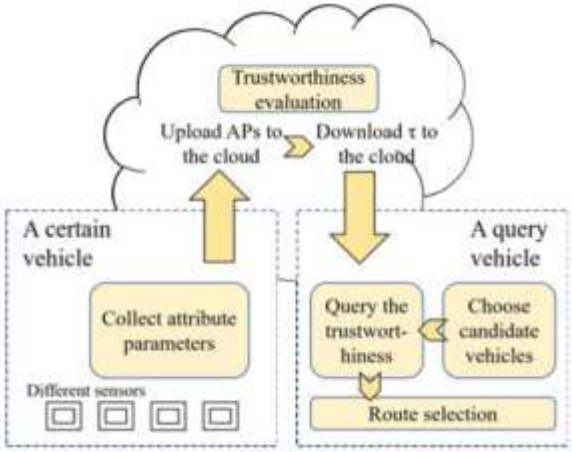
ADVANTAGES OF PROPOSED SYSTEM:

❖ A balanced node utilization ratio is defined

❖ A fair trustworthiness evaluation is proposed

❖ A method for value re-excavation from known information is presented.

SYSTEM ARCHITECHTURE



4. IMPLEMENTATION

System Model

In this work we focus on a two-dimensional torus topology. This topology is found in several nodes. Each node can directly communicate with the compute nodes of adjacent boards by means of wireless links, compute nodes are expected to communicate intensively with each other. Hence, the efficiency of routing has a significant influence on the overall performance. we focus on the topology of a single board, i.e., on a regular torus mesh network with m rows and n columns. we focus on unicast communication where one sender communicates with one receiver over one or more intermediate nodes (forwarders). Each node can be a sender, forwarder, or receiver. Receivers issue acknowledgments to inform the sender about the successful delivery of data packets. These end-to-end acknowledgments are routed through the network as data packets.

Path Selection

To prevent problems of routing algorithms like deadlocks or livelocks, we use the Odd-Even-Turn-Model as a basic path selection method. This model restricts the movements of a packet to certain allowed turns depending on the coordinate sof the node that takes the routing decision. These restrictions prevent cycles in the routing path and thus livelocks to occur.

Locally Evaluated Trust (LET)

Metric In our approach, each node locally rates the trustworthiness of its four neighboring nodes (north, east, south, and west) by evaluating the delivery of previously sent packets. This implies that LET does not apply to a whole path but only to adjacent nodes. Before transmitting a packet, the sender and each forwarder consider their locally computed trust values to select the next node on the path. The range for the trust value can be arbitrary. For the sake of simplicity, we let the LET range between 0 (untrusted) and 1 (trusted). A trust value of 0.5 indicates a neutral rating that is also used as the initial value of the metric. Updates of the LET are triggered by local observations of the nodes. For each sent packet, the sender logs the identifier of the packet, the time of transmission, and the identifier of the neighbor that was selected as successor.

Attacker Model

In this work, we consider only active attackers. Active attackers can, modify or drop packets (data packets as well as acknowledgments), delay their transmission or replay formerly sent packets. The presence of these attackers can thus be detected using quantitative metrics. For instance, an increase in the average data delivery latency might hint at the presence of an attacker who delays packets. Passive attackers only observe the data transmitted. However, as long as an attacker only observes, it is not possible to recognize the attack. possible to describe it in a metric. The confidentiality of the data can, however, be enforced through end-to-end

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 19
August 2018

encryption. We therefore assume the use of end to-end encryption and do not further discuss passive attacks. We further assume that appropriate security measures like digital signatures are in place that enable nodes to verify the origin and validity of received packets. Hence, modified packets can be recognized and will be discarded so that a modification implies a packet loss as well. Therefore, we do not explicitly distinguish between modification and dropping of packets in the following. The sender recognizes the loss of a packet if a data transmission is not acknowledged within a pre-defined time interval (timeout). Since it is not possible to distinguish whether the data packet or the acknowledgment was lost, both cases are treated as the same. The delay of a transmission can also cause the detection of a packet loss, but when the acknowledgment eventually reaches the sender, this false detection can be corrected. The replay of acknowledgments to conceal an attack is not possible since we assume that the acknowledgment is digitally signed by the receiver and contains a unique reference to the acknowledged data packet. An active attacker can also affect network availability by flooding the network with useless traffic (denial of service). The LET metric considers the trustworthiness of nodes and is not designed for this type of attacks. Thus, it is not helpful to prevent or detect them. We leave the consideration of denial of service attacks to future work.

5. RESULTS ANALYSIS

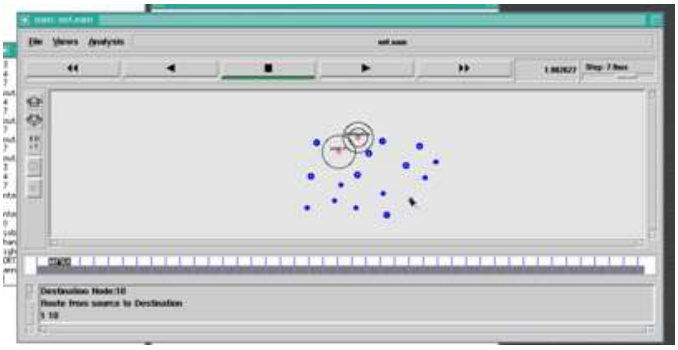


Fig 1: message transferring with TERP protocol

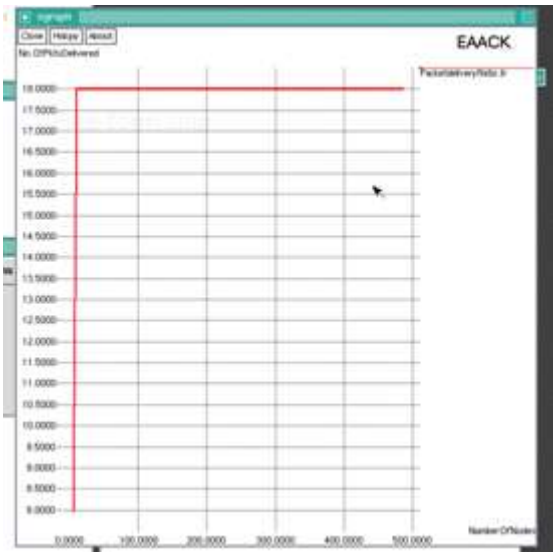


Fig 2 : packet delivery ratio

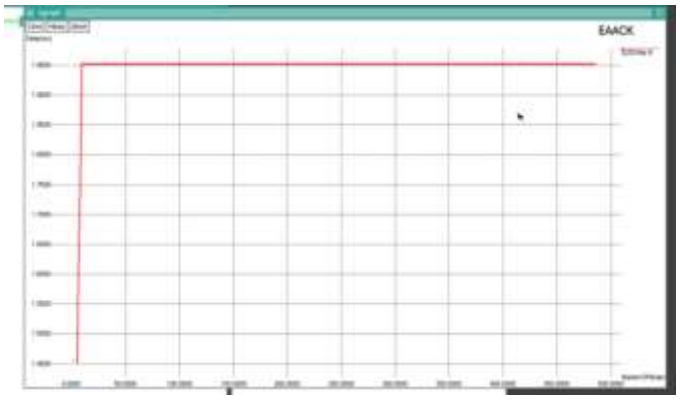


Fig 3: end to end delay

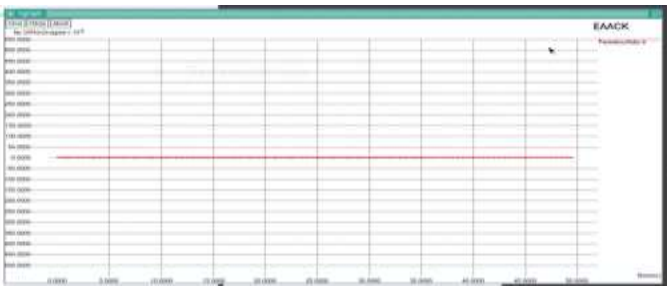


Fig 4 : packet loss ratio

6. CONCLUSION

In this paper, we proposed a novel routing protocol named trustworthiness evaluation-based routing protocol (TERP) for incompletely predictable vehicular ad hoc networks. Due to the inherent characteristics of this type of networks, it is particularly important to design a trusted route transmission method that is suitable for utilization in vehicle networks. For that reason, attribute parameters of vehicles are listed and sent to the cloud as the evaluation basis. By filtering according to transmission probabilities, candidate nodes are aggregated into a list and sent to the cloud. The cloud looks up and feeds back the latest trustworthiness evaluations of these nodes. Based on the trustworthiness provided by the cloud, nodes in the network perform the needed routing and packet delivery. An evaluation test has been implemented and showed that our evaluation process is feasible. Moreover, the simulation of the proposed new protocol indicates that TERP is able to maintain a high packet delivery ratio, with low overhead and end-to-end delay. In order to enhance the security method of the proposed protocol, in our future work, we suppose to propose a reliable and secure trustworthiness evaluation system and further improve the trustworthiness evaluation scheme by supporting also privacy and anonymity.

References

[1] J. Shen, C. Wang, A. Wang, X. Sun, S. Moh, and P. C. Hung, "Organized topology based routing protocol in incompletely predictable ad-hoc networks," Computer Communications, 2016, doi:10.1016/j.com com.2016.07.009.

[2] G. Ping, W. Jin, H. G. Xue, S. K. Chang, and J. U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," Journal of Internet Technology, vol. 15, no. 6, pp. 929–935, 2014.

[3] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," Journal of Internet Technology, vol. 16, no. 1, pp. 171–178, 2015.

[4] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, 2016, doi: 10.1109/JSYST.2016.2544805.

[5] J. Shen, H. Tan, S. Moh, and I. Chung, "Enhanced secure sensor association and key management in wireless body area networks," Journal of Communications & Networks, vol. 17, no. 5, pp. 453–462, 2015.

[6] M. B. Abdullahi and G. Wang, "A Lightweight Anonymous Ondemand Routing Scheme in Wireless Sensor Networks," in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, June 2012, pp. 978–985.

[7] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks," Journal of Network & Computer Applications, vol. 76, pp. 37–48, 2016.

Mr. Ch.Sudarsan Raju received Bachelor's Degree in Electrical and Electronics Engineering from SJMIT, Chitradurga, Karnataka and Master's degree in Digital Systems and Computer Electronics from JNTU, Anantapur. He is a life time member of Indian Society for Technical Education (ISTE).He is also a life time member of IMAPS. He is currently working as Associate Professor with Department of Electronics and Communication Engineering in BIT Institute of Technology, Hindupur. His research interests include wireless networks and Vehicular Ad Hoc and Sensor Networks.