A Hybrid Heuristic Trust Evaluation Model with Emergency Message Dissemination in VANETs

Ali Abbas

College of Information Technology, Al-Furat Al-Awsat Technical University, Technical Institute, Samawa, Iraq;
ali.abbas.isa@atu.edu.iq.

Abstract:

Vehicular ad hoc network (VANETs) is the highly trending technology which is able to provide high security and efficiency for maximum of the applications of intelligent transmission systems (ITS). The kinds of notes which are present in the vehicular network are roadside units (RSU), vehicles, signals which are present in the traffic areas and so on. Due to high speed mobility of the vehicles data transmission is interrupted which results in frequent link failure at the time of data transmission. Due to such drawback the emergency data transmission is disturbed and as well the data malfunction occurs. To overcome such drawbacks in this article a hybrid heuristic trust evaluation model with emergency message dissemination (HTEDV) is developed. The major categories of this model are the effective network model and trust evaluation model. With the presence of such process the data transmission ratio and data generation.

1. Introduction

In the present decade the VANETs have emerged in people's missions in a gradual manner [1-5]. It is a new kind of mobile communication which consists of all the safety applications in a significant manner that helps to reduce roadside traffic accidents [6-10]. This technology is mainly used to perform critical information transmission among any two devices in the environment. The devices perform vehicle based communication and infrastructure based communication [11-14].

Nowadays this technology changes the way people travel and it consists of certain characteristics [15-18] which are highly unique and it causes certain drawbacks in the network [19-22]. The characteristics of vehicles which are in the VANET communication are high speed and random ability with rapid change in topology which becomes not suitable for centralized management architecture of the network [23-27]. Many researchers proposed certain methodologies to increase the network accuracy and efficient data transmission at the time of high mobility and rapid topology changes among the vehicles at the time of data transmission [28-31]. But still the network needs improvement in terms of cost efficient resources and effective trust management [32-35]. And as well correctness of interaction information among the devices with a perfect time period needs to get improvised to maximize the scalability of the network [36-38]. These are the major drawbacks which are identified in the vehicular communication [39-40] and in order to overcome such flaws in this article hybrid heuristic trust evaluation model with emergency message dissipation is introduced and the major contribution of this article is described below.

2. Related Works

In [41], implemented VANET which is essential for traffic efficiency and safety but faces security challenges including Man-in-the-Middle (MiTM) attackers. MARINE a novel trust model efficiently identifies and revokes credentials of MiTM attackers showing significant improvements in simulations with 35% MiTM attackers but the disadvantages is high delay. In [42], author enabled vehicle communication with Road-Side Units (RSUs) in VANET were the proposed BMLT-SA, a blockchain-based Sybil attack detection mechanism using HTM, VTM, and DTM among RSUs and validated through simulations and the disadvantage is high delay. In [43], Location Based Service (LBS) in VANET jeopardizes vehicle location privacy. Our proposed blockchain-enabled trust-based scheme, using Dirichlet distribution, ensures cooperation only among trusted vehicles, effectively preserving location privacy with minimal time delay.

In [44], explains VANETs to improve road safety through an Intelligent Transportation System (ITS) and this framework suggests a Neuro-fuzzy-based trust system for accurate and computationally efficient detection of fake messages and drawback is high delay. In [45], introduce features like platooning for an improved driving experience

in VANET. CETVSP, ensures trust in lead vehicles and efficient message relay with minimal computational expense and proven secure against user attacks but the disadvantages are high overhead. In [46], demonstarted Smart vehicles in Vehicular Ad-hoc Networks (VANET) which communicates road dangers for safety, this method's Conditional Distinguishable Pseudo Identities (CDPD) scheme is to address dubious warning messages, ensuring security and privacy but the disadvantage here is high power consumption.

In [47], shares traffic events for improved driver safety in VANET, an incentive-based trust system using the "Byzantine fault-tolerant Paxos algorithm and game theory", demonstrating effectiveness in simulations with the high overhead. In [48], preserving location-based service (LBS) in VANET for query privacy is crucial. Our efficient mechanism using cryptographic constructs like OT extension and ring-LWE scheme that ensures privacy for user queries, location server content and vehicle location, here the disadvantages are high packet loss. In [49], designed the Malicious Vehicles Identification and Trust Management (MAT) algorithm ensures security through key exchange and special nodes that prevents the attacks and improving group lifetime, cluster stability, and vehicle location accuracy with high power consumption. In [50], explains Securing VANET is challenging due to dynamic vehicle movements and wireless vulnerabilities. This paper proposes a "Dual Authentication (DA)" algorithm to counter various VANET attacks and introduces a novel trustworthiness evaluation scheme with a high delay as drawback.

In [51], improves public transport safety and efficiency in VANET yet face security challenges this compares trust and cryptography applications to address VANET security requirements, and the disadvantages are high packet loss. In [52], demonstrated the Internet of Vehicles drives the development of VANETs routing algorithms by addressing security challenges in multi-hop communications through a concise and secure algorithm based on accumulating trust and the drawback is high overhead. In [53], developed Intelligent Transportation System (ITS) relies on VANET facing security challenges in Location Based Service (LBS). The proposed BTLB-PP system enhances VANET security and privacy efficiently as validated by simulations with the disadvantages of high delay. The earlier model analysis with its merits and demerits are discussed in table 1.

3. Proposed HTEDV Model:

This HTEDV model is mainly designed to provide trust management among the vehicles in the network. The core modules are effective network construction, trust evaluation model and its analysis. Figure 1 depicts the structure of the suggested model.

3.1 Network Model

- Vehicles: This is a representation of the network's primary users, intelligent vehicles (IVs). Each IV has a distinctive blockchain into consideration, a set of both private and public keys, and is capable of cryptographic V2V and V2I transactions.
- RSUs: These are the traffic handling system units that connect IVs to roadside infrastructure wirelessly. It functions in the IV-compatible 5.9 GHz DSRC band, offering extremely low latency—a prerequisite for high-speed activities. In addition, RSUs are in charge of registering and removing IV registrations, which entails providing them with certificates for authentication and canceling them. Additionally, they serve as DrivMan's Certificate Authority (CA). This certificate lacks a genuine identity, nevertheless it possesses an IV public key, a crypto fingerprint (CID), and a date of expiration. This protects the vehicle's anonymity because actual identities may be found by examining activities taken with any public key.

3.2 Trust Evaluation Model:

Here we introduce a Horizontal Trust Management (HTM) method that allows any vehicle to get information about other nodes connected to the same RSU. After compiling all of the information that was given by other cars, the vehicle utilizes a Local Machine Learning (ML) method to separate those around it into two distinct categories: Normal Nodes (NN) and Malicious Nodes (MN). We investigate the performance of three machine learning algorithms: "Random Forest (RF), K-Nearest Neighbors (KNN), and Support Vector Machine (SVM)" to

find the best LML approach. We select the one that is more suited for our procedure based on the outcomes of its implementation. At first, we assume that the RSUs in the VANET are the ones issuing the timestamp-containing digital signatures. Subsequently, the signature is received simultaneously by all vehicles linked to the same RSU. Vi records the infrastructure signatures for every car it is linked to, together with the time and RSU. The following format will be used for this signature:

$$sig(V_i) = (I \qquad (1)$$

Every time a vehicle Vi receives a signature, it creates a new vector V by adding its ID, designated IDV i, GPS location, $P_{V_i}(T)$, and velocity, $Spd_{V_i}(T)$, to the received data. I defined ECTV as follows:

$$VECT_{v_i} = \qquad (2)$$

When linked to many RSUs, every node records a brief history of its trajectories as it moves. An historical vector H_{V_i} is created from the vectors $VECT$ that the vehicle V_i generates:

$$H_{V_i} \qquad (3)$$

HTM consists of three primary phases:

4. Simulation Environment: The HTEDV network structure is constructed in the software Ns3 and to generate the real time traffic models which are present in the densely populated area sumo mobility generator is used with open street map software. The parameters which are taken into consideration for the result analysis are data delivery ratio, network throughput, routing overhead, energy efficiency and energy consumption. The obtained results are compared with certain earlier methodologies such as LTMM [51], BSRA [52] and BTLD [53] and as well the input parameters which are present in this simulation experimentation are given in table 2.

4.1 Packet Delivery Ratio: It is the calculation of the data which is generated in the source vehicles and it gets successfully transmitted to the destination within the predefined time slots. Utilizing the trust management system which is present in the HTEDV helps to increase the delivery ratio of the vehicles. In figure 2 the delivery ratio calculation of the HTEDV given and it is compared with the other works like LTMM, BSRA and BTLD. This research proves that the HTEDV achieves around 10% better data delivery ratio when compared with the other methods.

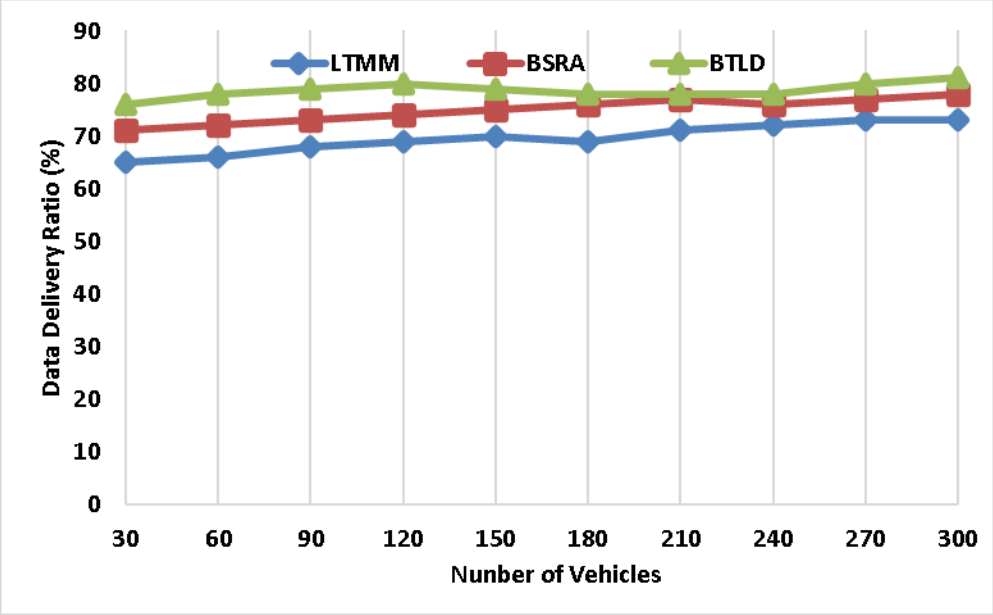

Figure 2 - Packet Delivery Ratio

4.2 Network Throughput: It is defined as the calculation of the amount of data produced in the source vehicles at a particular time period. The data generated by all the vehicles in the cumulative form represents the throughput calculation. In figure 3 throughput calculation is performed among the HTEDV and the earlier methods like LTMM, BSRA and BTLD. From the results it shows the HTEDV achieved maximum throughput which is around 100 kbps higher than the other methods.

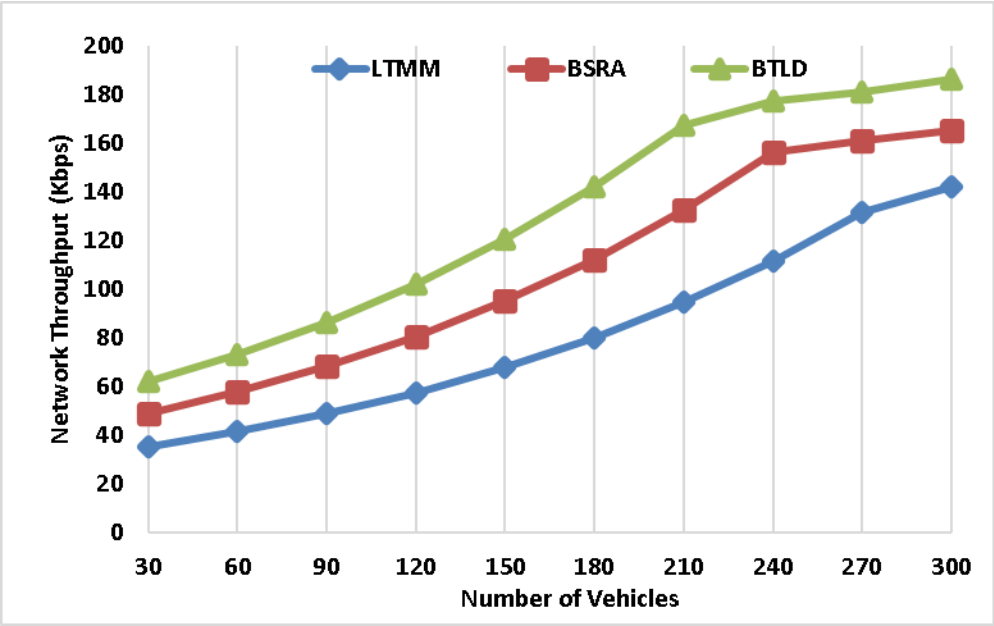

Figure 3 - Network Throughput

4.3 Routing Overhead: It is defended as the calculation of the number of data packets which get forwarded back to the source without reaching the destination. In order to provide high flexibility among the vehicles reduction of routing overhead is very essential. In figure 4 the calculation of routing overhead is shown and the performance of the HTEDV is much lower than the earlier works like LTMM, BSRA and BTLD. With the presence of the trust management system the transmission ratio of the HTEDV is high and that leads to reduce the overhead which is around 300 packets lower than the other methods.

4.4 Energy Efficiency: It is the calculation of residual energy or reminding energy which is measured at the end of the simulation of the vehicular network. To maximize the lifetime of the network it is very essential to achieve maximum energy efficiency among the vehicles. In figure 5 the calculation of energy efficiency is performed between the HTEDV and the earlier works like LTMM, BSRA and BTLD. From the given result it is understood that the HTEDV produces maximum energy efficiency which is around 150 joules higher than the other methods.

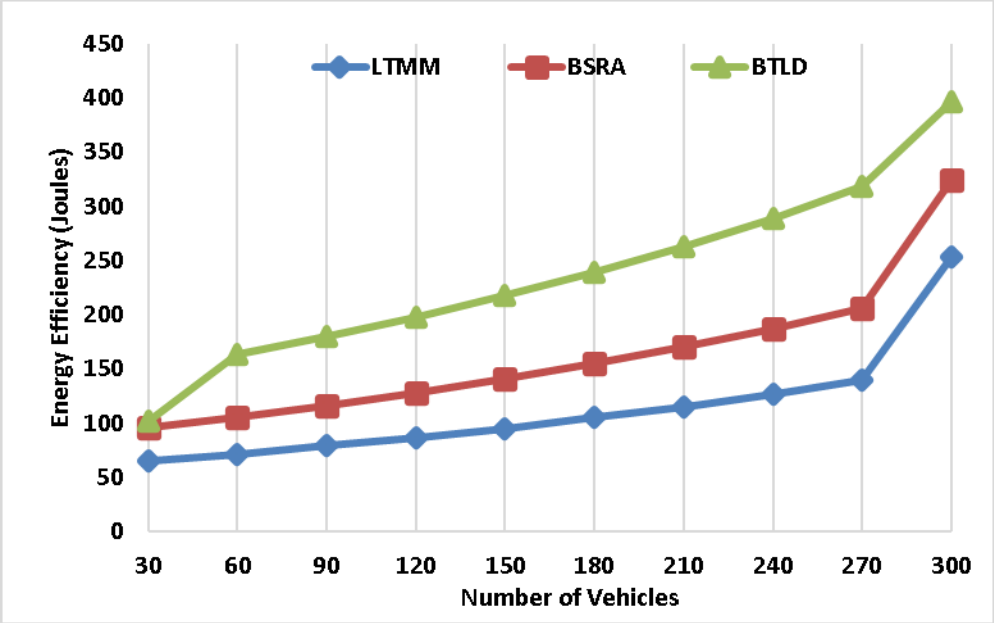

Figure 5 - Energy Efficiency

4.5 Energy Consumption: It is the amount of energy which is utilized among the vehicles at the time of high speed data transmission. Through the trust management system the communication among the vehicles is standardized so that the HTEDV produces much lower energy to perform the communication. In figure 6 the consumption calculations of the HTEDV is described and it is compared with the other methods like LTMM, BSRA and BTLD. From the result it is shown that the HTEDV produces very lower energy consumption which is around 70 joules lower than the earlier methods.

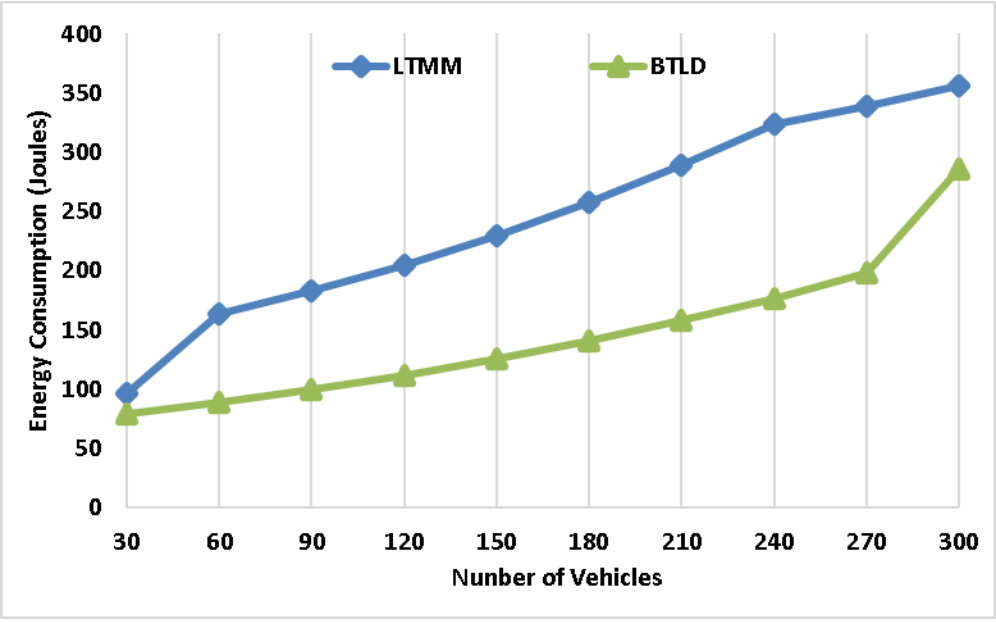

Figure 6 - Energy Consumption

5. Conclusion:

The aim of this proposed HTEDV model is to attend effective communication among the devices which are present in the vehicular network. For that purpose efficient trust evaluation and emergency message dissemination model is concentrated

6. References:

[1] A. H. Abbas, A. J. Ahmed, S. A. Rashid, M. A. Jubair, N. F. Abdulsattar, H. S. Mansour, and M. I. Habelalmateen, "Hybrid ANT Based Continuous

[2] M. K. Hasan, M. M. Ahmed, N. F. Wani, A. H. Abbas, L. M. Alkwai, S. Islam, A. K. M. A. Habib, and R. Hassan, "Dynamic load modeling for bulk load-using

[3] A. H. Abbas, A. J. Ahmed, and S. A. Rashid, "A Cross-Layer Approach MAC/NET with Updated-GA (MNUG-CLA)-Based Routing Protocol for VANET Network,"

[4] H. S. Mansour, M. H. Mutar, I. A. Aziz, S. A. Mostafa, H. Mahdin, A. H. Abbas, M. H. Hassan, N. F. Abdulsattar, and M. A. Jubair, "Cross-Layer and Energy-Aware AODV

[5] A. H. Abbas, H. Mansour, and A. Al-Fatlawi, "Self-Adaptive Efficient Dynamic Multi-Hop Clustering (SA-EDMC) Approach for Improving VANET's Performance,"

[6] M. A. Jubair, S. A. Mostafa, D. A. Zebari, H. M. Hariz, N. F. Abdulsattar, M. H. Hassan, A. H. Abbas, F. H. Abbas, A. Alasiry, and M. Turki-Hadj, "A QoS Aware Clus

[7] M. I. Habelalmateen, A. J. Ahmed, A. H. Abbas, and S. A. Rashid, "T

[8] S. A. Rashid, M. I. Habelalmateen, A. J. Ahmed, A. H. Abbas, M. A. Jubair, M. H. Hassan, A. Abdulhadi, S. Hammed, and L. Audah, "Congestion Aware Genetic Q-

[9] A. H. Abbas, A. J. Ahmed, S. A. Rashid, N. F. Abdulsattar, M. H. Hassan, M. A. Jubair, and M. I. Habelalmateen, "Predictive Hybrid Routing with

[10] A. H. Najim, A. H. Abbas, K. Al-sharhanee, and H. M. Hariz, "Reinforcement Learning-based Topology-Aware Routing Protocol with Priority Scheduling for Internet of Drones in Agriculture

[11] A. H. Alwan, A. A. Aziz, M. A. Jubair, A. H. Abbas, M. H. Hassan, S. Alheejawi, N. F. Abdulsattar, A. S. Mustafa, and M. I. Habelalmateen, "Monitoring the Impact

[12] Mostafa, S.A., Mustapha, A., Ramli, A.A., Jubair, M.A., Hassan, M.H., Abbas, A.H. (2021). Comparative Analysis to the Performance of Three Mobile Ad-Hoc Network Routing Protocols in Time-

[13] M. H. Hassan, M. A. Jubair, A. H. Abbas, A. J. Ahmed, S. A. Rashid, M. H. Mutar, H. S. Mansour, A. Ali, and M. I. Habelalmateen, "AODV based Crow Search Algorithm