IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 28, 2019, accepted July 6, 2019, date of publication July 11, 2019, date of current version August 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2928365

Reliable Multiservice Delivery in Fog-Enabled VANETs: Integrated Misbehavior Detection and Tolerance

XIAOMEI ZHANG[1], CHEN LYU[2], (Member, IEEE), ZHICAI SHI[1], DONGMEI LI[1], NEAL N. XIONG[3], (Senior Member, IEEE), AND CHI-HUNG CHI[4]

[1]School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China
[2]Department of Computer Science and Technology, Shanghai University of Finance and Economics, Shanghai 200083, China
[3]College of Intelligence and Computing, Tianjin University, Tianjin 300350, China
[4]Data61, Commonwealth Scientific and Industrial Research Organization (CSIRO), Sandy Bay, TAS 7005, Australia

Corresponding author: Chen Lyu (lyu.chen@mail.shufe.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802252 and Grant 61702319, and in part by the Shanghai Sailing Program under Grant 17YF1405500.

ABSTRACT Vehicular ad hoc networks (VANETs) in which vehicles act as the mobile nodes provide a wide variety of services, such as audio and video surveillance. However, such networks suffer from an important problem of service delivery reliability as the network performance degrades significantly in the presence of misbehaving vehicles. Most of the existing works either assume that vehicles' misbehaviors are constant or ignore heterogeneous traffic for multiservice (a mix of video, voice, and data traffic). In this paper, we investigate the problem of trust-based multiservice delivery via integrated misbehavior detection and tolerance for fault-aware VANETs. To model the effects of time-varying misbehaviors, modern fog computing could help to analyze and to store related data in VANETs while evaluating the dynamic trust weights based on attribute parameters of each vehicle. Then, we incorporate these weights into our service delivery framework that integrates trustworthy vehicle selection for misbehavior detection and uses differential resource allocation to achieve misbehavior tolerance. We present a multi-path selection criterion based on the trust evaluation and design a trust-aware heterogeneous traffic allocation algorithm over multiple routing paths. Finally, our scheme is evaluated using extensive simulations where we show that (i) approximately $12\% - 40\%$ higher successful service delivery can be achieved by our routing algorithm at the expense of acceptable delay loss compared to other three routing protocols; (ii) our trust-aware traffic allocation algorithm can gain $10\% - 20\%$ higher effective network utility and better fairness than that of the baseline solution; and (iii) the integrated scheme significantly improves both effective utility ratio and the path-usage proportion by comparing it with only routing scheme and only traffic allocation scheme.

INDEX TERMS Vehicular ad hoc networks, misbehavior detection, misbehavior tolerance, misbehavior dynamics, multiservice.

I. INTRODUCTION

The Vehicular Ad-hoc Networks (VANETs), as a sub-type of Intelligent Transportation Systems (ITSs) [1], [2], can provide efficient traffic monitoring, accident avoidance, infotainment and transport efficiency which are referred to as various types of traffic streams having quality of services (QoS) requirements. Most of services have to be forwarded to the destination via multi-hop routing using vehicles as mobile relays. In practical wireless environment, VANETs may suffer lots of security threats which cause many types of misbehaviors. Maintaining an acceptable level of service degradation for VANETs in the presence of misbehaving nodes is an open issue [3].

VANETs support vehicle-to-vehicle and vehicle-to-infrastructure communications through short range communication means. The lack of adequate physical protection make vehicles vulnerable to be captured and becomes an insider-misbehaving node. In recent literatures, as summarized in [4], various efficient defense schemes assume that the

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Maaz Rehan.

misbehaviors are traditional and constant in VANETs. Nevertheless, in order to evade misbehavior detection, there may exist inconsistent behaviors [5]: the normal (misbehaving) vehicles become misbehaving (normal) vehicles under uncertain attacks, random attacks, or mobile attackers. Traditional security components cannot counter smart misbehaviors with dynamic factors in VANETs. There are two types of defense approaches designed to protect VANETs: *detection*, such as misbehavior detection, and *tolerance*, such as utilizing diversity (multi-radio [6], multi-channel [7] and multi-path [8]). When smart attackers exist, it becomes difficult to mark all misbehaving vehicles since the detection-based approaches may receive fake alert and have incorrect detection results. On the other side, although fault tolerance can improve reliability to certain extent, the network performance degrades significantly when insider adversaries launch persistent attack as channels or paths may be disrupted. Hence, it is necessary to integrate misbehavior detection and tolerance both of which could coordinate and complement each other.

As an important component of misbehavior detection, trust evaluation in VANETs has been extensively studied for recognition of misbehaving vehicles [9]. The trust weight of a vehicle can be estimated by a tremendous amount of generated vehicular data: data from intrinsic aspect and data from extrinsic aspect, which is usually discussed in big data era [10]. Similar to cloud, fog in linkage with VANET provides data collection, analysis and trust management. Fog computing chooses its fog nodes from mobile vehicles, RSUs and base stations by the roads which are with capacity of computing and massive storage. Applying to features of fog computing into practice, researchers have proposed many outstanding works in providing the trustworthiness of any querying vehicle [11]. Nevertheless, few of existing works consider the dynamics of factors in real environments. In fact, the impact of misbehaviors is time-varying at each vehicle because of random, opportunistic and mobile attacks. In this paper, we propose a fog computing enabling misbehavior effect-based approach, which captures the dynamics of misbehaviors. At a given time, the states of trusted vehicles are identified by collecting the aforementioned factors and then are modeled as random processes. According to the stochastic model of being trusted, the fog estimates trust weight that is a statistical evaluation of trusted state over the time and helps the routing protocol to choose relay vehicles both in route discovery and maintenance phase.

Due to the uncertainty and time-variability of misbehaviors, malicious nodes may avoid being identified as attackers and preserve themselves under misbehavior detection [12]. Therefore, the misbehavior tolerance can be applied to maintain network performance in the presence of malicious nodes. The majority of misbehavior tolerance techniques make use of network redundancy [6]–[8]. Accordingly, we present a trust aware multipath routing protocol (TMP) for misbehavior tolerance. Our protocol explicitly utilizes the existing statistics to select trusted candidates and paths in the route discovery phase. Likewise, a relay node is discarded when it becomes untrusted while our misbehavior detection still works during route maintenance phase.

In order to make effective use of multi-path routing [13], the VANET must has the ability to provide an intelligent traffic allocation among multiple routing paths while considering the potential misbehavior of vehicles. Most of existing fault-aware resource allocation approaches are widely used for solving network utility maximization (NUM) problems subject to reliability constraints [14]. However, the total utility maximization of flows, which travel along the paths with different effect of misbehaviors, may cause extreme unfairness among actual-receive rate of each flow at the destination. A key reason is that the traditional NUM formulation is unable to make dynamical adjustments based on conservative assumptions. Paraskevas et al. apply "trust" concept into the NUM formulation for avoiding allocating more traffic through paths with high proportion of misbehaving nodes. Even though this pioneer work has made advances in dealing with performance and security tradeoff, the existing NUM based resource allocation approaches cannot deal with fair rate allocation for different types of traffic streams [15]. In our work, we generalize the NUM approach to obtain a new problem formulation, which considers the optimization of different utilities and incorporates the notion of trust into the utility-based NUM formulation. Especially, our trust-based NUM can allocate rates for fault-aware multipath VANETs to achieve better network performance and utility fairness among multiple types of services.

In this paper, we investigate the reliable multiservice delivery that can minimize performance degradation for VANETs in adversarial environments. In order to achieve this goal, we apply a trust evaluation-based approach, which integrates misbehavior detection and tolerance. Misbehavior detection is achieved by means of trust evaluation, while misbehavior tolerance is achieved by means of routing and traffic allocation for multi-source-multi-path system. The trustworthiness of each vehicle is evaluated according to both extrinsic and intrinsic factors, and is provided by the vehicular fog computing. Then we model the stochastic state of being trusted along the time and present a novel metric Trust Weight (TW) for each vehicle. The TW results can be queried for reliable routing schemes or be delivered to the source for traffic allocation algorithms. We introduce an enhanced, trust aware version of the multipath routing protocol that considers the misbehavior dynamics and incorporates these trust metrics into routing path selection problem. Meanwhile, the notion of trust is combined with the utility-based NUM problem that allocates traffic appropriately for meeting QoS requirements among different services. We propose a cross-layer traffic allocation algorithm for the trust aware NUM problem with contention constraints to minimize performance degradation including utility loss and fairness loss in VANETs. The extensive comparative evaluation first shows that our routing algorithm could achieve $12\% - 40\%$ higher packet delivery ratio with an acceptable communication overhead and delay compared to other three routing algorithms. Next, we illustrate the advantage of the trust aware NUM in effective network utility and fairness over the traditional NUM solution without considering misbehavior of untrusted vehicles. Finally, we show the effectiveness of our proposed routing protocol combined with our traffic allocation algorithm for VANETs in adversarial environments.

Our solution presents a novel approach that combines misbehavior detection and tolerance using dynamic misbehavior evaluation for VANETs. The main contributions of this paper are summarized as follow:

1) We design a trust based multiservice delivery framework that integrates misbehavior detection and tolerance in fog-enabled VANETs. The vehicular fog computing acts as a computation and store server to provide trust weights, which model stochastic state of being trusted by statistical factors uploaded by each vehicle.
2) We present a trust-aware multipath routing protocol, TMP, with respect to trust weights. It seeks to discover a set of relay nodes and routes that can satisfy trust requirements; it then maintains these requirements in the process of the transmission.
3) A distributed cross-layer optimization algorithm is proposed for the trust-aware NUM problem to be friendly with different types of services. Especially, our trust aware traffic allocation (TTA) algorithm can achieve lossy utility max-min fairness among multiple services of different QoS requirements.

The rest of this paper is organized as follows. In section II, we present our network model and fog assisted VANETs architecture. In Section III, we propose our trust evaluation, our trust aware multipath routing protocol and our trust ware traffic allocation algorithm. The performance evaluation is provided in Section IV. In section V, we summarize a survey of related work. Section VI concludes the paper and presents some future work.

II. SYSTEM MODEL

A. NETWORK MODEL

1) THE FUNDAMENTAL MODEL OF THE VANET

The VANET is a type of ad hoc networks which are self-organizing and decentralized. In city environment, cars move in a particular range or a regular pattern [16]. During a short period of time, the movement ranges and trajectories of the vehicles are fixed. VANETs are required to provide multiple services, such as intelligent transportation monitoring, entertainment, target tracking, to vehicles anytime and anywhere. In order to forward services, lots of moving vehicles need to act as the source nodes, relay nodes and destination nodes. A complete service delivery always contains different nodes, which select the next hop to receive and send packets, and allocate resource for each service.

The VANET can be represented by an undirected graph $G(\mathcal{V}, \mathcal{L}, \mathcal{C})$. We denote the node set as $\mathcal{V} = \{1, 2, \ldots, V\}$ and the logical link set as $\mathcal{L} = \{1, 2, \ldots, L\}$. We mean each logical link as two vehicles that are in the transmission range of each other. $\mathcal{C}$ is denoted as the set of capacity c_l over $l \in \mathcal{L}$, and $\mathcal{C} = \{c_1, c_2, \ldots, c_L\}$.

WLANs and mobile ad hoc networks are always based on contention access protocol in the MAC layer. IEEE 802.11p-based VANETs also adopts the classic interference-limited protocol with random multiple access scheme [17]. In the assumption, every vehicle acts as a partner of other vehicles in this multihop network. However, due to the interference, there exists contention when two nodes transmit data over the same channel at the same time. A wireless node (vehicle) at the MAC layer follows random-access-based MAC protocol which describes when a transmission is successful. The successful transmission of link l is based on the transmission persistence probability. In a contention graph [18], let ω be the maximal clique in which only one link can be active in a time slot. ω_l is denoted as the set of maximal cliques containing link l, $\mathcal{L}(\omega_l)$ is denoted as the set of links which coexist with link l in the maximal clique. Assuming that each link l transmits data with a probability q_l, the successful transmission probability of link l can be expressed as $\prod_{j\in\mathcal{L}(\omega_l)\setminus\{l\}}(1 - q_j)$.

2) MULTIPLE SERVICES

The VANET meets the demand for multiple services or tasks, such as video, voice and data. Similar to the paper [15], the multi-services under our consideration are categorized into two classes. One common service is data collecting from the interested vehicles. For example, collision warning data sent to the neighboring vehicles, so that data can be analyzed further in order to make decisions. This class of services is referred to as elastic data flow which has a (strictly) concave increasing utility function. Another class of services is real-time, such as video monitoring and tracking by cameras in automatic driving scenarios. Different from the elastic data flow, it is referred to as inelastic flow whose utility function is convex but not (strictly) concave. In practical intelligent transportation systems, service delivery schemes should have the ability to handle a mix of elastic and inelastic flows and provide a good performance balance for different services.

3) ADVERSARY MODEL

We make the following assumptions on the misbehaviors of vehicles in VANETs:

1) In order to maximize its attack strength, a misbehaving node may not drop data packets during the initial stage. Instead, it increases its attack rate after misbehavior detection. Some adversaries generate virtual nodes to help attracting nodes to route through them. Thus, various misbehaviors contain failures from different types of factors.
2) We consider malicious node that can launch random attacks, opportunistic attacks and mobile attacks. Inconsistent behaviors may exist when misbehaving nodes alter their on and off status of attack in a probabilistic way. Hence, the performance of multiservice delivery is affected by the probabilistic and

time-varying impact of misbehaving nodes in many cases.

B. FOG ASSISTED VANETs ARCHITECTURE

In order to estimate the impact of probabilistic misbehaviors by each vehicle, a computing center is demanded for collecting data, analysis and distributing Trust Weights (TW). In this section, a fog assisted VANET architecture is explored that collects, stores and analyzes a massive amount of information to estimate trustworthiness of each vehicle. Similar to [19]. the architecture of proposed scheme for fog assisted VANETs are presented in Fig. 1. There exists the following participants in the proposed system, i.e., vehicles traveling on the roads, some stationary RSUs and fog servers.

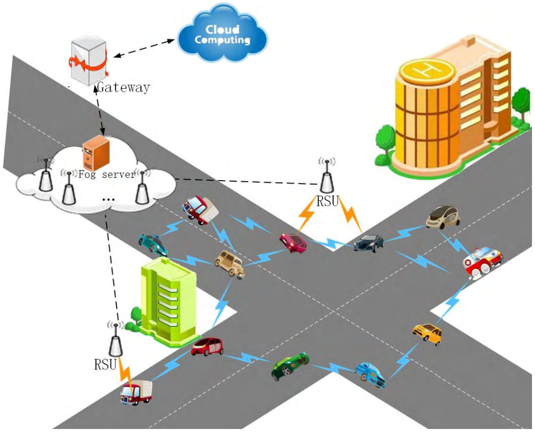


FIGURE 1. A fog-enabled VANETs structure.

Vehicles: The vehicles can be considered as a set of mobile nodes that can communicate in two scenarios: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). Our VANET architecture follows a hybrid architecture involving wireless local area networks or cellular and ad hoc networks. The vehicles in our architecture can relay information as partners for neighboring vehicles using short-range communication means of IEEE 802.11p. Besides, the long-range communication means (such as cellular networks) are equipped in vehicles and remote access services to cover large area and enormous amount of vehicles. For the vehicles without the long-range communication means, a vehicle can request for some services from proper units alongside the road (such as nearby roadside unites, RSUs) that can improve connectivity to passing vehicles. Vehicles can be classified as being Source Vehicles, Candidate Vehicles and User Vehicles.

1) Source Vehicles: Some vehicles in our VANET are possible to become source vehicles who delivery the services to the destination nodes through multiple paths. With the assistant of the fog, each source constructs routing paths to the destination node and chooses available paths based on the impact caused by the misbehaving nodes. Meanwhile, the source incorporate the misbehavior impact in the traffic allocation problem among the multiple routing paths.
2) Candidate Vehicles: All the neighboring vehicles within the transmission range can be regarded as candidate vehicles once they drive nearby the relay vehicle until they are chosen to join the routing and delivery process.
3) User Vehicles: From the list of candidate vehicles, each relay vehicle first upload this set to the fog. After obtaining the candidate set, the fog calculates the trustworthiness of each candidate to help the up-stream node or the source making decision of routing and traffic allocation. Our scheme can filter user vehicles from candidate vehicles according to their trustworthiness.

RSUs: They are wireless communication equipment that act as routers to exchange data. In order to cover large region, RSUs are deployed in the interaction of roads and act as fog devices; meanwhile, they help the vehicles connecting with each other. The attributes of vehicles will be uploaded to RSUs which can be used to the necessary computing in coverage areas.

Fog servers: Fog servers provide powerful storing and computational capability. They can gather information from fog nodes and calculate the trust weights for vehicles. The Fog server serves as a trusted third part to perform fair evaluation of trust weights. This mitigates the negative impacts caused by different criteria for the trustworthiness evaluation process. Moreover, the Fog server can provide compute and storage services to vehicles but reduce the latency compared to the cloud server.

III. TRUST BASED FRAMEWORK OF INTEGRATED MISBEHAVIOR DETECTION AND TOLERANCE

The detailed trust based framework is presented in this section. We first give an overview of our trust based framework of integrated misbehavior detection and tolerance. The process of trust evaluation is presented to judge the trust weight of every vehicle. Then we illustrate the integration of misbehavior detection and tolerance scheme composed by the trust-aware routing protocol and trust-aware traffic allocation algorithm among multi-services.

A. OVERVIEW

The proposed routing and traffic allocation algorithms utilize the fog server to evaluate the trust weights of every vehicle. The trust weights are calculated in terms of faulty behavior factors upload by each vehicle and its neighbors. We assume that the vehicles information can be acquired, transmitted, stored and analyzed through Internet to Vehicles [10]. In the route discovery and maintenance, the source finds or reroutes multiple paths to the destination node according to the trust records of intermediate nodes. Trust weights for the different paths should be incorporated to our traffic allocation algorithm in each source node. As given in Fig.2, the process of framework is as follows:

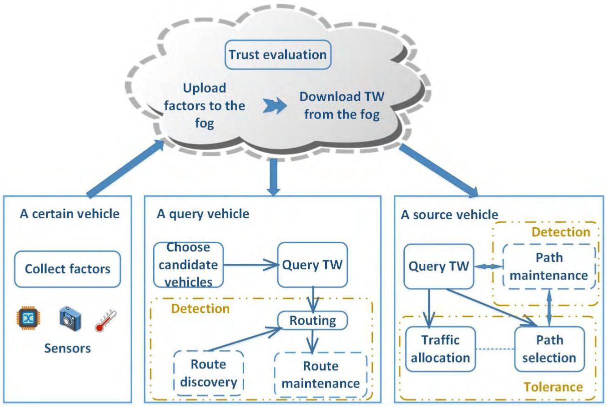


FIGURE 2. **Fog oriented integration misbehavior detection and tolerance.**

1) TRUST EVALUATION

due to the effect of the misbehaviors on the multiservice delivery, the vehicle uploads all the required information including its's own factors and the monitored misbehavior factors of its neighbor vehicles. The fog collects, stores and analyzes these data of vehicles' historical behaviors. Accordingly, the trust weight of each vehicle can be estimated in terms of statistical factors, which directly provided by itself and/or indirectly collected from its neighbors, consisting of remaining fuel, engine failures, numbers of accident, reputation verifications, and RSS pattern attributes.

2) TRUST-AWARE MULTIPATH ROUTING PROTOCOL (TMRP)

we combine TW metric with hop count information to help TMRP select the available paths. TMRP can find multiple paths based on modified AOMDV routing protocol. During the route discovery phase, a vehicle queries the TW values of its candidates for next hop from the fog and updates the TW value when it receives the RREP massage from next hop. In order to find path failure in the route maintenance phase, we utilize TW value to monitor failures on a link. After multiple paths being found, the source can maintain and detect TW of all paths in the path selection phase and the path maintenance phase according to trust weights from the fog.

3) TRUST-AWARE TRAFFIC ALLOCATION (TTA)

to capture the effect of the misbehaviors on throughput, trust weights should be cooperated into the network traffic allocation process. Multiple routing paths are constructed by many hops from the source node to its destination node. With the help of the trust estimation from the fog, the source node receives the trust weights of nodes on its routing paths and computes the end-to-end trust value over each path. For multiple services, a utility function is used for each source to describe how much QoS benefit that source receives by the allocated traffic. Then TTA algorithm maximizes the total utilities of actual effective traffic to ensure that trusted paths will get higher utility and achieve utility fairness among different services.

4) INTEGRATION OF MISBEHAVIOR DETECTION AND TOLERANCE

our architecture integrates misbehavior detection and tolerance by means of trust evaluation, route discovery, route maintenance and traffic allocation during the multiservice delivery process. By placing the trust evaluation, malicious behaviors can be effectively detected and marked. Then nodes with low trust weights are detected by the trust evaluation and avoided in the routing phase. Since random and dynamic misbehaviors exist, probabilistic misbehaving nodes may also join in the multiservice delivery and our scheme can tolerant them to certain extent through path selection and traffic allocation over multiple routing paths. Meanwhile, when some inside node starts launching attacks, the path maintenance can detect its trust value and eliminate it from routing paths.

B. TRUST EVALUATION

In this section, we present a mechanism which can not only evaluate individual node trust value, but can also derive individual node trust weight and a path trust metric according to statistical trust values.

1) TRUST VALUE

Modern vehicles have been equipped with enormous types of sensors which generate massive data referred to as Big Data from sensing the status of roads and vehicles [10]. The huge amount and various types of data generated by vehicles can be divided into two groups: data from intrinsic aspect and data from extrinsic aspect. Data from intrinsic aspect that directly collects the vehicle information such as numbers of violation, engine parameters, numbers of accident, mileage, velocity, etc. Data from extrinsic aspect refers to the information about the relationship with other vehicles or the environmental conditions, e.g., distance between vehicles and neighboring ones, warning notice, blind spots, trajectory, road map, etc. The principle component analysis (PCA) approach is a common data analysis method that decrease dimensions of multi-variable space. In the big data era of vehicles, we can use PCA approach to perform the trust value in terms of vehicle ''big data'' which is a multi-variable data table.

The trust value of each vehicle is determined by the extrinsic and intrinsic factors which are denoted as $f_1, f_2, \ldots, f_c$. Based on trustworthiness, we evaluate the node-misbehaving state and get the estimation of TW metric for each node and each path. Each eigenvalue e_i of f_i, $i \in \{1, 2, \ldots, c\}$, can be computed through utilizing PCA approach. If $\sum_{j=1}^{p} e_j / \sum_{j=1}^{c} e_j$ is close to 1, all the c factors can be instead by these p factors. Then we can obtain the trust value for each vehicle: $T = \sum_{i=1}^{p} b_i f_i$, where $b_i = e_i/(\sum_{j=1}^{m} e_j)$ is the contribution rate of each factor.

Extrinsic factors we select as follows: RSS pattern f_1 and reputation f_2 which are observed by neighboring vehicles. Intrinsic factors we select as follows: numbers of violation, engine failure, numbers of accident and mileage. f_3, f_4, f_5, f_6 represent the reciprocal of these four parameters, respectively. In practical situations, once a factor equals to 0, we set $f = 2$ to avoid that its denominator is 0.

a: RSS PATTERN

some physical measurements are used in VANETs to estimate the position of a vehicle in terms of the received signal strength (RSS) value. However, malicious vehicles may generate Sybil nodes which send forged RSS value to interfere the detection. Each vehicle observes the its neighbors' RSS time series which is data points over time. As shown in [20], sybil nodes have very similar RSS time series patterns. The fog collects the RSS time series and compares the resemblances between two series. We use the distance function D(PA,PB) to express the similarly between Pattern A (PA) and Pattern B(PB). The Euclidean distance can be calculated as follows:

$$D_{Lp}(PA, PB) = (\sum_{i=1}^{T}(pa_i - pb_i)^2)^{1/2}, \tag{1}$$

where T is measurement period time and pa, pb are the i^{th} element of pattern PA and PB.

In order to eliminate the interference caused by malicious nodes which adjust the transmission power of sybil nodes purposefully, RSS values can be preprocessed:

$$RSS'_i = \frac{RSS_i - \mu}{3\sigma}, \tag{2}$$

where μ and σ are the mean and standard deviation of RSS_i.

Each vehicle A compare the similarly of the RSS pattern with its neighbors $N_1, N_2, N_k, \bigvee N_i, N_j \in N(A)$:

$$D'_{Lp}(PN_i, PN_j) = \frac{D_{Lp}(PN_i, PN_j) - D_{Lp}min}{D_{Lp}max - D_{Lp}min}, \tag{3}$$

where $D_{Lp}max$, $D_{Lp}min$ are the maximum and minimum values of all D_{Lp}. The value of $D'_{Lp}(PN_i, PN_j)$ is between [0, 1]. If the value is closer to 0, two RSS patterns are more similar; while the value is closer to 1, two RSS patterns are less similar. The RSS pattern of Vehicle B is as follows:

$$f_1 = min_{j \in N(B)} D'_{Lp}(PN_j, PN_B). \tag{4}$$

b: REPUTATION

we define the reputation parameters as the forwarding ratio correctly of node B. Its upstream node can monitor the reputation parameters of one vehicle. For example, each vehicle A observes that how many packets actually delivered over link (A, B) and how many valid packets pass the error detection procedure. Then the reputation value $r(A, B)$ calculated by Vehicle A is given by the ratio of valid number to total number and then uploaded to the fog. If Vehicle A wants to evaluate the receiver node B over link (A, B), the reputation value r calculated by Vehicle A is given in the following equation:

$$r_{A,B} = \frac{NT_{A,B}}{NT_{A,B} + ND_{A,B}}. \tag{5}$$

Here, r is the reputation of vehicle B which directly observed by vehicle A, NT is the number of data packets forwarded, and ND is the number of packets discarded or disrupted by Vehicle B. Fog calculates the reputation parameter of the receiver node B. Let $N(B)$ denote as the set of Vehicle B's transmitter nodes, $| N(B) |= n$, the reputation of Vehicle B can be computed as follows:

$$f_2 = \frac{1}{n} \sum_{j \in N(B)} r_{j,B}. \tag{6}$$

We take an example to describe our trust value evaluation process. There are ten vehicles $v_1, v_2, \ldots, v_{10}$ and six factors $f_1, f_2, \ldots, f_6$ mentioned above, as shown in Table 1. The six eigenvalues of principle components are depicted in Fig. 3. We can see that the first three principle components can instead of all the components since $\sum_{j=1}^{3} e_j / \sum_{j=1}^{6} e_j = 0.91168$.

TABLE 1. Example of six parameters of ten vehicles.

	f_1	f_2	f_3	f_4	f_5	f_6
v_1	0.804732	0.94	1	2	2	0.07945
v_2	0.826423	0.95	0.5	1	2	0.081031
v_3	0.816405	0.91	1	0.5	2	0.071667
v_4	0.025161	0.885	2	0.2	1	0.085821
v_5	0.039058	0.91	1	0.5	0.5	0.09973
v_6	0.702646	0.75	0.5	0.33	0.3333	0.08331
v_7	0.604298	0.47	0.125	0.5	0.125	0.07889
v_8	0.715631	0.7	0.5	0.333	0.3333	0.073744
v_9	0.764781	0.83	0.3333	0.33	0.5	0.086573
v_{10}	0.853462	0.72	0.125	0.25	0.3333	0.087512

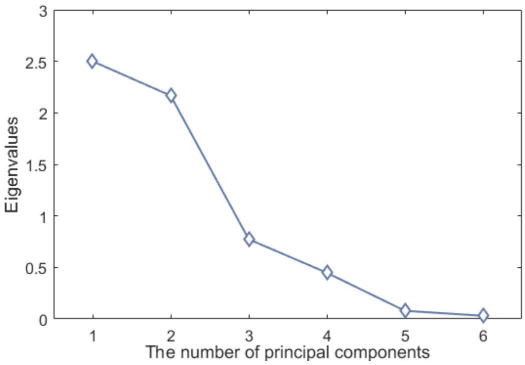


FIGURE 3. The six eigenvalues of principal components.

The trust value of each vehicle can be obtained in Fig. 4. The trust values of v_4, v_5 and v_7 are less than 0.6. The values of RSS pattern v_4, v_5 are close to 0 so that there are at least two vehicle have similar patterns. It means that v_4, v_5 are very likely to be sybil nodes. Meanwhile, v_7 with $f_2 = 0.47$ launches dropping packets, receiving a quite low trust value after the evaluation. Therefore, our trust evaluation process can detect various misbehaviors of vehicles effectively.

2) TRUST WEIGHT AND PATH TRUST METRIC

In order to capture the uncertainty of misbehaviors, we present a novel metric Trust Weight (TW), which is a statistical estimating of being trusted state along the time.

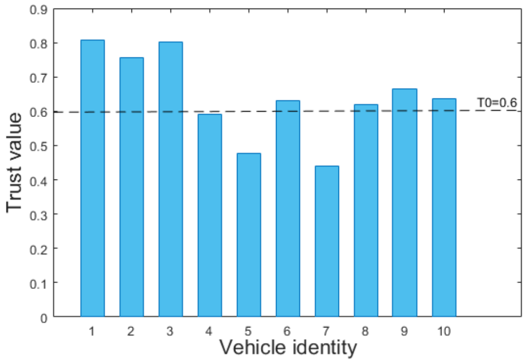


FIGURE 4. The trust values of six vehicles.

A heuristic is motivated by determining whether the node is in a trustworthy state. Applying the condition in which the trust value is above a certain threshold, we can detect various types of misbehaviors. We define the TW which is the time that nodes spend in trustworthy state per unit time.

Definition 1: The trust weight denoted by TW_i is the fraction of time during period $[t, t + t_s]$ for which the node i is in the trustworthy state where trust value $T_i(t') < T_0$, $t' \in [t, t + t_s]$.

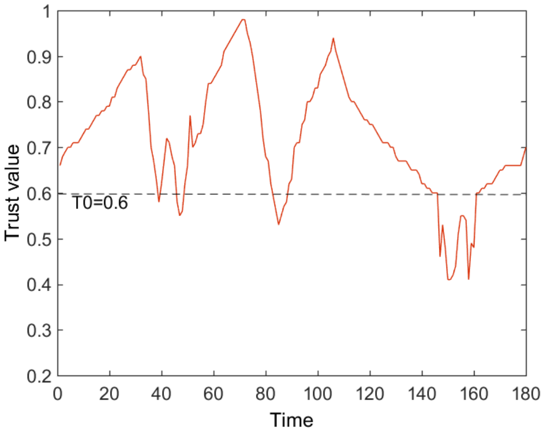


FIGURE 5. The trust values during a period.

We show an example of converting the trust values on a node (as drawn in Fig. 5) into the trust weight with T_0 being 0.6 (as plotted in Fig. 6).

In traversing the path R_s, the source s queries TW of each node in path R_s from the fog and then computes the end-to-end path trust metric. Once the estimations of node trust weight and path trust metric are obtained, we can cooperate the statistical misbehavior information into routing path selection and traffic allocation. The path trust metric can be formulated as

$$\mathcal{TW}_s = \prod_{i\in R_s} TW_i. \tag{7}$$

C. TRUST-AWARE MULTIPATH ROUTING PROTOCOL

In this section, we introduce trust aware version of enhanced AOMDV routing protocol. A trust-aware multipath routing protocol based on trust weights called TMRP is presented, combining TW with hop count information in selecting next hop.

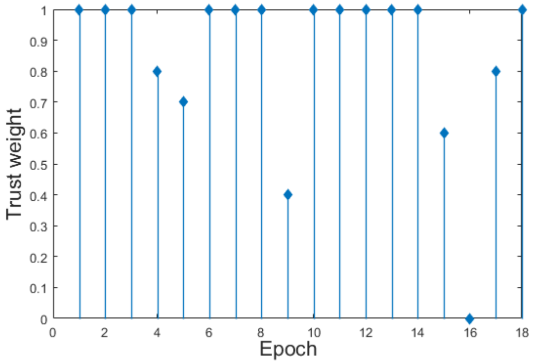


FIGURE 6. Estimation of TW.

1) ROUTING DISCOVERY

In AOMDV routing table, each routing entry maintains three fields: destination address, next hop and last hop. We add two fields (hop_count, $trust\_weight$) in the routing entry. The hop_count is designed to store the value of hop counts and the $trust\_weight$ will record the trust weight of this path in route request (RREQ) messages. We set TMRP as a priority-based route discovery method, which uses the candidates' TW to decide their priority. The fog can provide the record of trust weights of candidate nodes. The node with high trustworthiness has higher probability to be chosen into the routing path. The routing discovery procedure of enhanced AOMDV is shown in Algorithm 1.

Algorithm 1 Routing Discovery Procedure

```
for each node $i$ do
    insert TW of neighbors into RREQ;
    broadcast RREQ;
end for
for each node $i$ in the path do
    receive $Source\_ID$ and $RREQ\_ID$ from RREQ;
    if $RREQ\_ID$ is in the processed list then
        drop RREQ;
    else
        get values from ($hop\_count$, $trust\_weight$) in RREQ;
        if $trust\_weight > TW_0$ then
            forward RREQ;
        else
            drop RREQ;
        end if
    end if
end for
```

2) ROUTE MAINTENANCE

TMRP uses route error (RERR) and route reply (RREP) to maintain and update the routing table entries in each node.

In route maintenance phase, TW is utilized to discriminate misbehavior on a link along the routing path.

With the help of trust estimation from the fog, misbehavior dynamic information on each can be noticed timely to its neighbor nodes. When TW of some misbehaving node becomes lower than TW_0, fog will notice all its neighbor nodes. Then the neighbor nodes broadcast RERR massages for any route traveling through this misbehaving node. The upstream hops of the path could research another next hop in order to avoid this misbehaving node. In the same way, when TW of the probabilistic misbehaving nodes get higher than TW_0, the potentially interrupting link may be reutilized.

3) PATH SELECTION AND MAINTENANCE

Our routing protocol utilizes route discovery to get a set of paths from source and destination nodes. If the path trust weight is above a threshold, the path is identified as available; the source can deliver services along it. Anytime it is identified as an unavailable path, the protocol reroutes to repeat the discovery procedure and discard the misbehaving node.

The set of paths is considered an effective method to increase service delivery rate in VANETs. Because the probability of at least one path arriving at the destination node is improved based on the guarantee of the path set. Using multipath selection is a misbehavior tolerance way to improve the network performance. Meanwhile, the misbehavior detection still works since an available path may become an unavailable path in terms of the probabilistic path weight. When this occurs, the source node will have to start a new routing discovery procedure.

Different from AODV and AOMDV, our TMRP adds two fields (*hop_count*, *trust_weight*) in the routing entry. Therefore, our protocol can make good use of the upstream nodes in the path to control RERR broadcast hops. When a link is broken, a RERR packet is delivered back to the source node to notify the error. Since the TMRP has recorded routing paths, the broadcast frequency of RERR can be also controlled. Therefore, our trust-aware multipath routing protocol can achieve lower overhead than AODV and AOMDV when the broken links exist in the routing path.

D. TRUST-AWARE TRAFFIC ALLOCATION

In the precious section, we introduce the trust-aware multipath routing protocol for the VANET. To make effective utilizing of multiple routing paths, each source node must be able to allocate traffic intelligently across the routing paths while considering the potential impact of mibehaviors on service delivery. In this section, we present a trust-aware traffic allocation algorithm to generate the optimal effective rate control among multiple services.

1) SYSTEM ANALYSIS

Consider the VANET which has multiple sources and multiple routing paths. The related symbols are described and listed in Table 2. TW_i is denoted as the time fraction during which node i act as a trusted node. Moreover, the path trust value $\mathcal{TW}_{s,n}$ is indicated as the time proportion of good behaviors over the path $R_{s,n}$, which denotes the ratio of actual effective traffic flow at the destination node. We denote $\mathcal{TW}^i_{s,n}$ as the sub-path trust value along sub-path $\mathcal{R}^i_{s,n}$. We incorporate the statistical trust weight into the link capacity constraint condition. Due to the contention set conception described in Sec. II, the capacity constraint of effective flow rate over a link (i,j) can be represented as follows:

TABLE 2. The meaning of symbols.

Symbol	Expression	Description
$\mathcal{S}$	$\{1, 2, ..., S\}$, and $S \subseteq \mathcal{V}$	The set of sources
k_s	$s \in \mathcal{S}$	The number of available paths or routes from the source s to destination
$\mathcal{R}_{s,n}$	1 (the path passes through l) or 0(otherwise)	The set of links used by source s on its path n
$\mathcal{R}^i_{s,n}$	1 (the path passes through l) or 0(otherwise)	The set of links along the sub path from source s to the intermediate node i of $\mathcal{R}_{s,n}$
$\mathcal{R}_s$	$[\mathcal{R}_{s,1}, \mathcal{R}_{s,2}, ..., \mathcal{R}_{s,k_s}]$	The set of all the available paths of source s
$\mathcal{R}$	$[\mathcal{R}_1, \mathcal{R}_2, ..., \mathcal{R}_S]$	$L \times K$ routing matrix over all the paths
$x_{s,n}$		The rate of source s on the path $\mathcal{R}_{s,n}$
x_s	$\sum_{n=1}^{k_s} x_{s,n}$	The total source s rate
F_s	$[x_{s,1}, ..., x_{s,k_s}]^T$	The set of all path rates of source s
M_s	$M_s < \infty$ and $s \in \mathcal{S}$	The maximum flow data rates of s
m_s	$m_s \geq 0$ and $s \in \mathcal{S}$	The minimum flow data rates of s
$U_s(x_s)$	$s \in \mathcal{S}$	Continuous, strictly increasing and non-negative utility function of x_s
Q_s	$(s \in S(i,j)) \bigwedge(\mathcal{P}_{s,n} \in \mathcal{P}_s) \bigwedge((i,j) \in \mathcal{P}_{s,n})$	Flow of path $\mathcal{R}_{s,n}$ over link (i,j)

$$\sum_{Q_s} \mathcal{TW}^i_{s,n} x_{s,n} \leq c_{(i,j)} q_{(i,j)} \prod_{d \in \mathcal{L}(\omega_{(i,j)}) \setminus \{(i,j)\}} (1 - q_d). \quad (8)$$

In order to support multiple services referring to elastic and inelastic traffic, we will use the utility based traffic allocation scheme designed by Wang et al. [16]. This traffic allocation scheme is not only be friendly with elastic traffic but also be applicable inelastic traffic. We define a non-negative utility $U_s(x_s)$ to cater for multiple services with different QoS performance, where $x_s \in [m_s, M_s]$. This utility function is no need to be strictly concave so that it can models both elastic traffic and inelastic traffic. Then a ''pseudo utility'' can be defined as

$$\mathcal{U}_s(x_s) = \int_{m_s}^{x_s} \frac{1}{U_s(y)} dy, \quad m_s \leq x_s \leq M_s. \quad (9)$$

Now considering the statistical trust weight and applying the pseudo utility function in Network Utility Maximization (NUM) problem:

Problem 1:

$$\max \sum_{s \in S} \left(\int_{m_s}^{\sum_{n=1}^{k_s} \mathcal{TW}_{s,n} x_{s,n}} \frac{1}{U_s(y)} dy \right)$$

$$s.t.: \sum_{Q_s} \mathcal{TW}^i_{s,n} x_{s,n} \leq c_{(i,j)} q_{(i,j)} \prod_{d \in \mathcal{L}(\omega_{(i,j)} \setminus \{(i,j)\})} (1 - q_d)$$

$$m_s \le \sum_{n=1}^{k_s} x_{s,n} \le M_s$$

$$0 \le \sum_{(i,j)\in\mathcal{L}(\omega_{(i,j)})} q_{(i,j)} \le 1. \tag{10}$$

We can see from Problem 1 that $\mathcal{U}'_s(x_s) = \frac{1}{U_s(x_s)}$ and $\mathcal{U}' > 0$. Therefore, the utility function $\mathcal{U}_s(x_s)$ is continuous, increasing and strictly concave. The above problem is also a convex optimization problem after replacing the utility function.

2) TTA ALGORITHM

We use a change of variables $\tilde{x}_{s,n} = log(x_{s,n})$ and $\tilde{F}_s = [e^{\tilde{x}_{s,1}}, \ldots, e^{\tilde{x}_{s,k_s}}]$. The Problem 1 is turned to Problem 2:

Problem 2:

$$\max \sum_{s\in S}\Big(\int_{m_s}^{\sum_{n=1}^{k_s}\mathcal{TW}_{s,n}e^{\tilde{x}_{s,n}}} \frac{1}{U_s(y)}dy\Big)$$

$$s.t.:\ log\sum_{Q_s}\mathcal{TW}^i_{s,n}e^{\tilde{x}_{s,n}} - \log c_{(i,j)} - \log q_{(i,j)}$$

$$-\sum_{d\in\mathcal{L}(\omega_{(i,j)\setminus\{(i,j)\}})} \log(1-q_d) \le 0$$

$$m_s \le \sum_{n=1}^{k_s} e^{\tilde{x}_{s,n}} \le M_s$$

$$0 \le \sum_{(i,j)\in\mathcal{L}(\omega_{(i,j)})} q_{(i,j)} \le 1. \tag{11}$$

By applying Karush-Karush-Tucker(KKT) theory [21], we can derive:

$$\lambda_{(i,j)}(t+1) = [\lambda_{(i,j)}(t) - \tau\Big(\sum_{d\in\mathcal{L}(\omega_{(i,j)\setminus\{(i,j)\}})} \log(1-q_d(t))$$

$$+ \log q_{(i,j)}(t) + \log c_{(i,j)}$$

$$- \log\Big(\sum_{Q_s}\mathcal{TW}^i_{s,n}e^{\tilde{x}_{s,n}(t)}\Big)]^+, \tag{12}$$

$$q_{(i,j)}(t) = \frac{\lambda_{(i,j)}(t)}{\sum_{k\in\mathcal{L}(\omega(i,j))}\lambda_k(t)}, \tag{13}$$

where $\lambda_{(i,j)}$ is the Lagrangian multiplier for the Lagrangian function of Problem 2, $q_{(i,j)}$ is the link attempt rate. The traffic allocation algorithm adopts the similar second-order algorithm in [21].

TTA algorithm: We assume that the links do not changed within a time slot but be independently altered over different time slots. On each time slot t, Algorithm 2 lists out the trust-aware traffic allocation over multiple paths for multi-service.

For the VANET, a distributed traffic allocation solution is practical for its property of reducing the implementation complexity. As analyzed in Algorithm 2, our approach only requires each link update (actually performed by each router) to compute the transmission probability of links. The source rate is allocated update according to the transmission probability of the routing path embedded in the feedback signal.

Algorithm 2 Trust-Aware Traffic Allocation Algorithm

```
• MAC:
  At each time t = 1, 2, ..., each link $(i, j)$:
    1) Aggregates flow rates $x_{s,n}(t)$ and $\tilde{x}_{s,n}(t)$ for all
       paths $R_{s,n}$ that contain link $(i, j)$;
    2) Updates the link attempt rate by using (13);
    3) Computes a new lagrangian multiplier by formula (12);
    4) Decides the maximum attempt rate:
         $q_s^{r*}(t) = max_{i=1,2,\ldots,n_s} q^r_{s,i}(t).$        (14)
• Traffic allocate:
  At each time t = 1, 2, ..., each source $s$:
    1) Each source receives $q^r_{s,i}(t) = \sum_{(i,j)\in p_{s,i}} q_{(i,j)}(t)$
       from the network for all its paths $R_{s,i}$;
    2) Receives $q_s$ from its packet headers of all its paths
       $R_{s,n}, n = 1, \ldots, n_s$;
    3) Updates the source rate $x_s(t+1)$:
         $x_s(t+1) = [\frac{1}{U_s(q_s^{r*}(t))}]^{M_s}_{m_s};$        (15)
    4) For the paths $p_{s,i}$ without maximum attempt rate,
       updates the path flow rate over $p_{s,i}$:
         $x_{s,i}(t+1) = [x_{s,i}(t) - \varsigma(q_s^{r*}(t) - q^r_s(t))]^+, \varsigma > 0$
                                                                  (16)
    5) For any path $p_{s,j}$ having maximum attempt rate,
       updates the path flow rate over $p_{s,j}$:
         $x_{s,i}(t+1) = [x_{s,i}(t+1) - \sum_{i\neq j} x_{s,i}(t+1)]^+.$ (17)
• Routing:
  At each time t = 1, 2, ..., each source $s$: over the chosen
  link, transmit traffic for the destination node according
  to the rate computed by the traffic allocation updates.
```

Clearly, our traffic allocation algorithm run the link update procedure and the source update procedure locally. In each iteration, the algorithm has a time complexity of $O(hk)$ if a VANET has h links and S sources with k routing paths.

IV. PERFORMANCE EVALUATIONS

In this section, we first present simulation results to compare the performance of AODV, AOMDV, QoS aware multipath routing protocol MPQP [22] and our proposed TMRP routing protocol. Then we show the effectiveness of TTA for multiple services, by comparing it with the UNUM approach [19] based on same link contention constraints. Lastly, we show the advantage of our integrated misbehavior detection and tolerance approach over only misbehavior detection approach for VANETs in adversarial environments.

A. SIMULATION SETTINGS AND TRUST EVALUATION

To evaluate our proposed scheme and other compared protocols, we have conducted comprehensive experiments using

OPNET and C++ simulator. Protocols are run on a PC machine with an Intel(R) Core(TM) i5-6600 of 3.3 GHz and 16GB main memory.

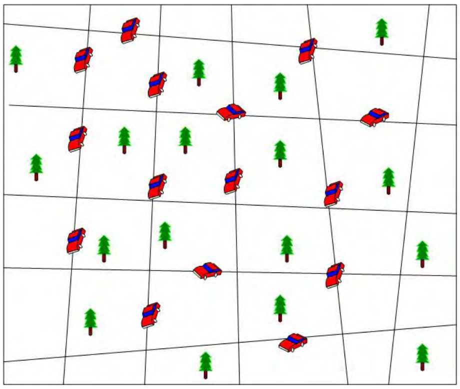


FIGURE 7. Simulation scenario.

TABLE 3. Parameter values in simulations.

Parameter	Value
Number of nodes	100
Map size	$1000m \times 1000m$
Mobility model	Described by IPNs
Propagation model	Two-ray ground reflection path loss model, Ricean fading model
Link capacity	c_l = 1Mbps
MAC	IEEE 802.11p
Number of sources	8
Percentage of misbehaving nodes	$0 \sim 0.5$
Maximum data rate	M_s = 1Mbps
Minimum data rate	m_s = 0Mbps
Step size	$\tau = 0.1$
Transmission power	$P_t = 1mW$
Interference Transmission power	$P_j = 1mW$
Path-loss constant	$\rho = 2.5 \times 10^{-4}$
Path-loss exponent	$\nu = 2.7$
Receiver noise	$N = 10^{-10}mW$
Node speed	$0 \sim 20m/s$
Simulation steps	1000

In the simulation environment, as shown in Fig. 7, the topology consists of 100 vehicles (nodes) randomly deployed in a square area of 1000m × 1000m. We place two RSUs (fog nodes) and one server node (a fog server) that is utilized to calculate the trust weight of every vehicle in the network. Our mobility model and traffic model are incorporated into the simulator [23]. The access of each vehicle arrives following a Poisson distribution. Over an observation period, the neighbor group is maintained among vehicles that move in a certain range and with a certain speed between $0 \sim 20$ meters/sec. We use IEEE 802.11p as the Media Access Control (MAC) protocol which also employs the classic un-slotted CSMA/CA protocol [17]. In order to reflect the effects by the diffraction of signals in practical road environments, we apply the Two-ray Ground Reflection propagation model and Rician distribution to simulate lossy channels [28]. For simulation convenience, there are 8 source vehicles that send data to the destinations. The link capacity is set to be $1Mbps$. Each result is based on 1000 iterations.

In section III, we show that trust weight evaluation process with different misbehaviors should be provided. Accordingly, our VANET consists of well-behaved nodes and misbehaving nodes. We simulate sybil attacks by randomly setting 4 malicious nodes each of which generates 3-6 Sybil nodes. Well-behaved vehicles forward 10 packets/s over Control Channel, but the malicious vehicle should broadcast 10n packets/s if it creates n virtual vehicles. In addition, we consider other misbehaving nodes that drop data packets with a varying probability Pr under continuous time model. As the Dos attacks also lead to the packet dropping, Pr can be set as the packet dropping probability of the vehicle under DDos attackers. We assume that each parameter Pr is equal to $e^{-\xi s}$, where s is the signal to interference and noise ratio (SINR) $s = \rho P_t d_{tr}^{-\nu} / (\rho \Sigma_j P_j d_{jr}^{-\nu} + N)$, N is the noise at the receiver node, d_{tr} is the distance from the transmitting node and the receiving node,and d_{jr} is the distance from each attacker to the receiving node [24]. If distance d_{tr} and d_{jr} are chosen as a continuous random parameter with time, Pr is also the a continuous random parameter. The proposed algorithms are simulated under various misbehaviors with the presence of increasing number of misbehaving nodes from 0% to 50% in the total numbers of vehicles. Table 3 lists these significant simulation parameters.

As in Section III, the fog server evaluates the trust weight of each vehicle in according to first three of their associated factors: RSS pattern, reputation and numbers of violation. We choose ten nodes to show their trust values in Fig. 8.

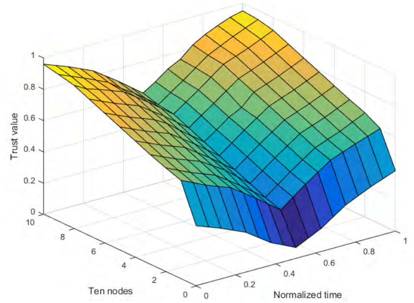


FIGURE 8. Trust value of ten nodes.

B. THE EFFECTIVENESS OF TMRP

To analyze the TMRP routing protocol, we use the following three metrics to compare three multipath routing protocols. The packet delivery ratio (PDR) is the proportion of the number of received data packets received successfully at the destination to the number of data packets delivered by the source. The overhead represents the fraction of the total number of control packets to the total number of data packets during the transmission. Average end-to-end delay indicates the transmission delay of delivering data packets successfully.

First we evaluate the effectiveness of TMRP in enhancing packet delivery ratio (PDR) under varied number of

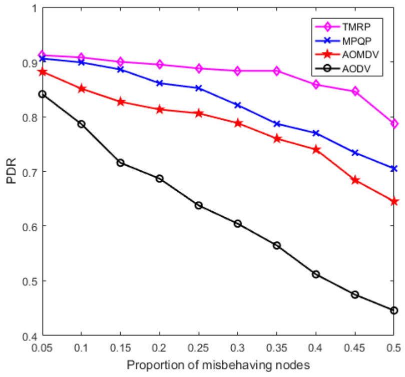


FIGURE 9. **Packet delivery ratio.**

misbehaving nodes. Viewed from Figure 9, PDR of TMRP is compared with that of other three routing protocols with the increasing number of misbehaving nodes. The delivery ratio in TMRP is always higher than that of other three protocols with the presence of misbehaving nodes. In addition, PDR in other three protocols degrades more sharply than that of TMRP as the proportion of misbehaving nodes increases. Since TMRP detects misbehaviors with the assistant of trust evaluation in fog, nodes can try more trustworthy next-hop to delivery packets and then deliver ratio is improved. Moreover, TMRP has a much higher probability in choosing the trustworthy path than that of other three protocols. MPQP also can choose more reliable paths in terms of reliability constraint. However, sybil nodes cannot be identified by MPQP so that the malicious behavior of them will lead to potential packet loss.

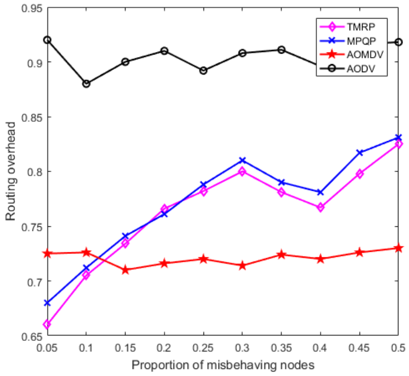


FIGURE 10. **Routing overhead.**

Figure 10 plots the protocol overhead of TMRP in comparison with three protocols. TMRP has lower overhead than that of AODV and MPQP but little greater than that of AOMDV. The overhead can be reduced in TMRP by introducing the fog since the trust weights are not exchanged between vehicles. TMRP only asks for the fog to deliver the trust weights, which decrease the number and the frequency of using broadcast packets. On the other hand, the route maintenance mechanism in TMRP will reroute the trustworthy paths if the misbehaving nodes are detected during the service delivery phase. In consequence, when the proportion of misbehaving nodes exceeds 12%, the maintenance overhead is increased so that the overhead of TMRP is more than that of AOMDV.

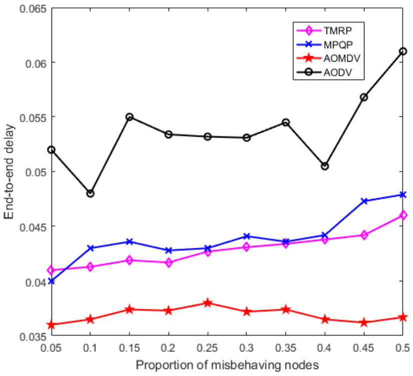


FIGURE 11. **End-to-end delay.**

The end-to-end delay of four protocols is shown in Figure 11. Observed from the figure, we can see that the delay of our proposed protocol ascends slowly with the increasing proportion of misbehaving nodes and is slightly lower than that of MPQP. That is because the trust evaluation in fog can help each vehicle to adopt next hop more quickly. However, the delay in AOMDV remains lower than that of our protocol. If some routing link becomes untrusted as the number of misbehaving nodes increases, TMRP will encourage other trustworthy link to join in routing, which results in raising the delay of packets. This result demonstrates that there is a tradeoff between successful delivery and delay. The main purpose of our protocol is improving the successful service delivery at the expense of acceptable delay loss.

C. THE EFFECTIVENESS OF TTA

In this subsection, we use simulation results to illustrate the advantage of the TTA over UNUM, with the same pseudo utility and contention constraints. In our VANET, we choose four sources which provide multiple services with different QoS requirements and have their utility function: $U_1(x_1) = \frac{1}{(1+e^{-2(x_1-4)})}$, $U_2(x_2) = \frac{log(x_2+1)}{log 11}$, $U_3(x_3) = \frac{1}{(1+e^{-2(x_3-6)})}$, $U_4(x_4) = 0.1x_4$. Figure 12 and Figure 13 plots the utility of effective rate received by the destination in UNUM and TTA, respectively. Figure 14 shows the effective utility ratio that is defined as the ratio of the utility of effective rates at the destination and the utility of original rates send by the source. We have the following observations from three figures: a) the utility of our algorithm is consistently higher than that of UNUM; b) The utility of sources in TTA are closer to each other than those in the UNUM approach, implying that TTA can achieve better utility fairness among sources; c) TTA can get higher the effective utility ratio and maintain an acceptable level of the utility degradation in the presence of misbehaving nodes.

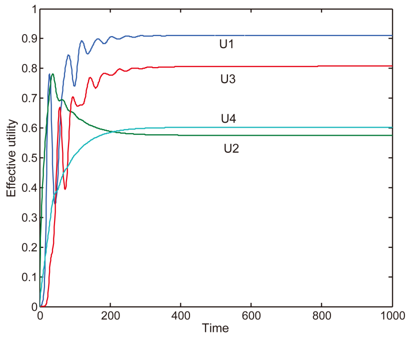


FIGURE 12. Effective utility in UNUM [19].

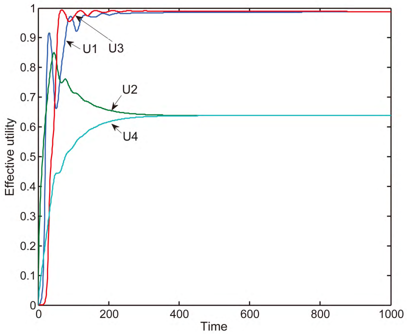


FIGURE 13. Effective utility in TTA.

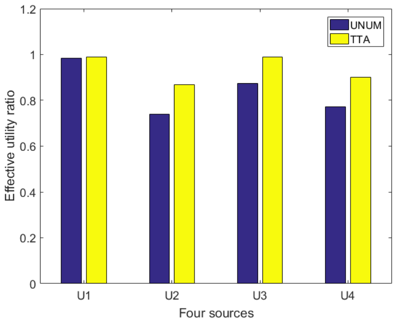


FIGURE 14. The comparison of effective utility ratio in UNUM and TTA.

The reason behind these three observations can be explained as follows: our proposed algorithm introduces the trust metric into the utility functions and constraints. Each source assigns its rate adaptively according to its actual received utility to compensate for utility loss which is caused by misbehaving nodes along the routing path. Furthermore, we design the trust based network utility maximization problem to determine the optimal tradeoff for each source dynamically, embodying the fairness objectives into the problem formulation. Hence, the considerable gains in network performance including utility fairness and effective utility are attained in our trust aware traffic allocation algorithm.

D. TMRP + TTA SCHEME

In this subsection, we demonstrate the effectiveness of our integrated misbehavior detection and tolerance scheme for

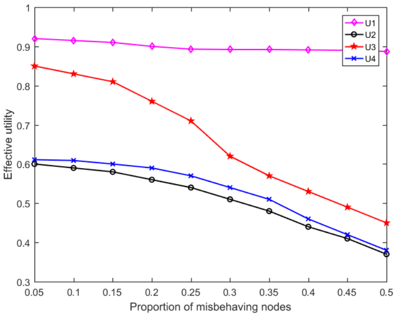


FIGURE 15. Effective utility in TMRP.

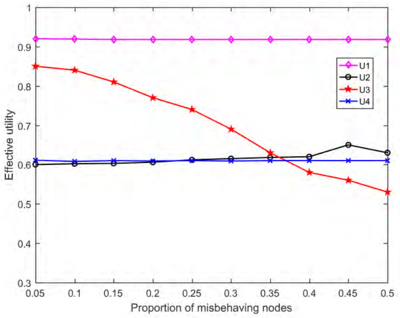


FIGURE 16. Effective utility in TMRP+TTA.

the VANET in the presence of misbehaving nodes. The proposed TMRP + TTA scheme is benchmarked against the scheme with only TMRP, in which it does not employ any resource allocation algorithm. Figure 15 and Figure 16 plots effective utility of two schemes under varied number of misbehaving nodes. Obviously, the effective utility of TMRP + TTA scheme can be significantly higher than that of TMRP scheme; and the superiority of TMRP + TTA scheme over TMRP scheme increases as the proportion of misbehaving nodes increases. The simulation results illustrate that the misbehavior tolerance is able to complement misbehavior detection by applying our integrated scheme. When dynamic misbehaviors exist, some faulty nodes cannot be detected by the detection-based approaches. The effective utility becomes lower when inside misbehaving nodes are present on routing paths. In our integrated scheme, we incorporate the effect of misbehaviors into NUM problem to adopt resource allocation dynamically so that our misbehavior tolerance is able to complement misbehavior detection.

We make further observation on effective utility of source 2 and source 4. As the number of hops increases, the effective utilities of source 2 and source 4 in TMRP + TTA scheme are closer to each other than those in TMRP scheme. This means better fairness can be achieved due to explicitly taking into account the utility loss in our integrated scheme.

Finally, the proposed TMRP + TTA scheme is benchmarked against the scheme with only TTA scheme, in which it only employ traditional multipath routing algorithm. In the figure 17, the reliable path usage proportion of

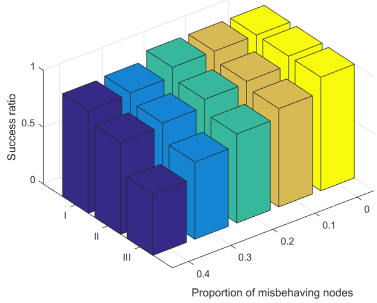


FIGURE 17. The comparison of TMRP and TMRP+TTA.

TMRP + TTA scheme and TTA scheme are plotted respectively. I- the percentage of scenarios where the network has reliable paths; II- the percentage of scenarios where TMRP + TTA scheme uses reliable paths; III- the percentage of scenarios where TTA scheme uses reliable paths. Figure 16 shows that TMRP + TTA scheme has a much higher ratio in using the reliable path successfully than TTA scheme. Using reliable paths to deliver service improves the utility gain of TMRP + TTA scheme. The result shows that the misbehavior detection also help complementing passive misbehavior tolerance in our integrated scheme.

V. RELATED WORK

A. TRUST EVALUATION IN VANETs

The misbehavior detection approach based on trust evaluation model in VANETs attracts much attentions due to its potential to maintain the network performance and satisfy the application QoS requirements [25]–[28]. Among all of the issues in trust evaluation technique, "how to manage the trustworthiness" and "how to evaluate the trustworthiness" have always been two hot topics.

1) FOG ENABLED VANETs

Li et al. [25] design an trust management scheme composing of data trust and node trust to cope with various misbehaviors in VANETs. The node trust is computed in terms of functional trust from itself and recommendation trust from other nodes. Accordingly, each node may obtain the local evidences by itself and transmit the external evidences to other nodes. Cheng et al. [26] propose a dynamic trust assessment including direct subjective trust assessment and direct objective trust assessment. The management is performed based on exchanging trust values among various vehicles. However, misbehaving nodes may drop, modify and even forge the values while relaying trustworthiness of other nodes in adversarial environments. To overcome these limitations, some trust based misbehavior detection approaches of utilizing "Vehicular Cloud Computing" have been studied for VANETs. But in this way, it is not practical to satisfy the requirements in delay using a centralized place.

As for the integration of cloud service and existing VANETs, the fog computing could provide distributed, heterogeneous platforms. Owing to support of fog nodes and fog servers, fog enabled VANETs can utilize enlarged and sufficient computation and storage resources to serve mobile vehicles. ([27]–[29]) Zhang et al. [29] design a computation offloading approach which utilizes the resource both of fog servers and vehicular terminals. A fuzzy trust model according to historical information and plausibility has been also presented in [11] to defend various types of threatens. In addition, the model chooses fog nodes as facilities to calculate the level of trust for VANETs.

The fog computing is also a promoting technology for mobility support of the vehicular environment. The work in [28] has presented a improved geographic routing (IGR) which adopts the routing path based on the condition of vehicles and streets observed by fog nodes. Similarly, Noorani et al. utilize mobile vehicles, RSUs and base stations as referred as fog nodes to select the appropriate route for establishing V2V communication [30].

In this paper, we are motivated to propose a trust evaluation approach that measures the effect of misbehaving vehicles on service delivery using fog computing. With the utilization of fog computing, the amount of historical vehicular data can be hosted for storing and calculating the trust weight of each queried vehicle. Moreover, our presented fog enable VANET deploys fog servers and fog nodes (including mobile vehicles, RSUs and base stations) to track surrounding vehicles and record variations in their abnormal behaviors. Thus, fog computing is of convenience and capabilities for dynamic misbehavior monitoring and trust evaluation in VANETs.

2) TRUST EVALUATION MODEL

Due to the effect of the node-misbehavior on packet delivery, plenty of trust evaluation methods of dealing with the nodes' faulty behaviors have been studied. A trust aware relay selection for VANETs was proposed in [31] for evaluating the trust values in terms of four parameters that reflect the vehicles status. Hu et al. [32] develop a trust-based recommendation scheme which collects the feedback from vehicles for calculating trust scores. However, few of them consider the uncertainty in the misbehaving parameters in VANETs. Recent works has illustrated that the smart misbehaving nodes employ dynamic attack methods to decrease the proportion of being detected in wireless networks [22], [33]. Wu et al. [33] address dynamic ongoing attacks and unknown attacks which have dynamically changing features and mutable attributes. Mitchell et al. [34] propose a behavior based intrusion detection technique to cope with random and hidden attackers. In fact, the misbehavior dynamics and mobility usually lead to the time-variability in service delivery. To characterize the probabilistic and dynamic effect of misbehaviors, our work identifies the trusted state of each vehicle by collecting parameters, and then calculates trust metrics according to statistical results of trusted state along with time. This assumption can address both constant misbehviors and random misbehviors.

TABLE 4. Review of fault aware service delivery.

	Schemes	Methodology	Type of misbehaviors	Strong points	Weak points
Trust evaluation	ART[25]	Measures trust based on data trust and node trust	Faulty or malicious vehicles	Accurate evaluation	Ignore forgers and sybil nodes
	[26]	Measures trust based on social connections	Faulty vehicles	Low trust assessment error	Ignore forgers and sybil nodes
	WeiSTARS[31]	Evaluates trust based on vehicles' status	Faulty or malicious vehicles	High delivery ratios	Ignore dynamic attacks
	REPLACE[32]	Chooses platoon head based on reputation from users	Malicious attackers	Defends against various types of attacks	Ignore dynamic attacks
	UCON[33]	Combines intrusion detection and prevention	Ongoing malicious vehicles	Defends against novel attacks	Ignore time-variability of misbehavior
	IDRS[34]	Integrates intrusion detection and response	Malicious attackers	Defends against a range of misbehaviors	Ignore time-variability of misbehavior
Multipath routing	NC-RMR[39]	Constructs braided multipath routing	Faulty nodes	Guarantees reliability and E2E delay	Just study selfish behavior
	SDM[40]	Allocates traffic based on delay estimate	Faulty nodes	Minimizes the average delay	Just study selfish behavior
	[41]	Constructs multipath based on security limit	Node failures and intruder attacks	Improves four performance metrics	Ignore sybil nodes
	[43]	Determines multipath under throughput loss constraints	Single-link attacks	Guarantees network resilience	Ignore the misbehaving dynamics
	$MPTCP-La/E^2$[44]	Constructs multipath using cloud computing	Denial-of-service attacks	Optimize the energy usage	Ignore the misbehaving dynamics
	FMR[45]	Chooses reliable paths using erasure encoded fragment	Insider attackers	Improve data availability	Ignore the misbehaving dynamics
Resource allocation	[46]	Allocates rate based on E2E delay requirements	Faulty nodes	Improves end-to-end QoS	Unable to allocate rate dynamically according to the actual receive-resource
	[47]	Allocates resource under the negative effective of noise	Artificial noise	Achieves the optimal performance	Unable to allocate rate dynamically according to the actual receive-resource
	[15]	Controls rate for different types of traffic	None	Suitable for multiple services in wireline networks	Not consider misbehaving nodes
	[48]	Controls rate for a mix of elastic and inelastic traffic	Channel loss	Suitable for multiple services in wireless networks	Not consider misbehaving nodes

The existing works classify trust modeling in VANET context into three categories, namely data-based, identity-based and hybrid models. Approaches using data-based models evaluate the trustworthiness of a vehicle in terms of various information. A data-based trust model in [26] evaluates data reports to infer their validity using several decision logics. The authors in [35] proposed a data-based trust evaluation algorithm for calculating the vehicles's trustworthiness in many aspects, i.e., the type of the vehicle, remaining gasoline, mileage and vehicle accident numbers. By this method, it detects the non-trusted data reports or events from all the information. One main limitation of this method is that, if vehicles seek partners for cooperating with each other to delivery and share content, the data-based models will fail since they are unable to build trust relationships between vehicles. Identity-based models separate vehicles into trust and non-trusted, and forward packets through vehicles that have established a priori trust relations with each other. Zhang et al. [36] propose a security aware fuzzy enhanced reliable ant colony optimization routing protocol which identifies misbehaving vehicles and blocks them from participating the transmission. However, the trusted vehicles based on a prior relationship may launch abnormal behaviors under on-off attacks or dynamic attacks. [37] pointed out that a hybrid trust approach can take advantage of both data-based models and identity-based models, which update the trust metrics both according to attributes of every vehicles and message reports from trusted vehicles. However, the above-mentioned hybrid methods does not focus on applying misbehavior dynamics information for service delivery under adversarial environments. In this paper, we adopt the hybrid trust model and calculate the vehicle's trust metric using timely misbehavior dynamics information by taking both attributes of each vehicle and RSS reports from other vehicles into account. Thus, our approach not only defenses against stationary misbehaviors, but also addresses mobile attacks and uncertain misbehaviors.

B. MULTIPATH ROUTING

Multipath routing aims to improve network performance by increasing the probability of data delivery over more paths. A number of multipath routing protocols have been explored [38]–[41] in the literature. A braided multipath routing, NC-RMR, is presented in [34] to guarantee packet delivery reliability and meet the end-to-end delay constraint in WSNs. The authors in [40] cooperate the characteristics of self-similar traffic into a multipath routing algorithm which can reduce the delay and data loss rate. These works, nevertheless, study a particular misbehavior of selfishness in packet delivery. A intrusion-fault tolerant multipath routing scheme [41] is proposed for improve the network reliability under intruder attacks. Besides such direct misbehavior of disrupting transmission, the misbehaving vehicles delivery fake position information to their neighboring vehicles so that there will be misleading driving directions or bandwidth consumptions [42]. In comparison, our TMRP addresses a wider series of misbehaviors than these approaches through combining the intrinsic factors and the extrinsic factors of vehicles.

For defending against various misbehaviors, not only the failed node behaviors should be found, but also the certain malicious attacks are expected to be detected. The authors in [43]–[45] propose to exploit the multipath routing for misbehavior tolerance in networks with presence of both the failed node behaviors and the malicious attacks. Typically, the reliability metrics, combined with other traditional routing information, are utilized in making a next hop and a path selection. However, the above-mentioned multipath routing protocols ignore the misbehaving dynamics information under random attacks or mobile attacks. In this paper, we apply misbehaving dynamics parameters as routing metric to the multipath routing protocol design.

C. TRAFFIC ALLOCATION IN LOSSY NETWORKS

Due to interference and contention, wireless networks are typically lossy in packet delivery. Saad et al. [46] perform rate allocation with considering the lossy nature of wireless links. A noise aware resource allocation in [47] is designed for reliable data delivery in terms of noise metric in the presence of artificial noises. With the aim of maximizing network throughput, the authors [46], [47] use the QoS requirement as a constraint to allocate data traffic. On the other hand, the fairness among users will be broken due to the different lossy degree among users. In this paper, we incorporate trust metrics into both the objective function and the constraint conditions of NUM problem and then determine fair traffic allocation dynamically according to the actual loss in packet delivery.

Several works that discuss the traffic allocation among different types of services. Wang et al. [15] extend the utility function in NUM problem, namely UNUM, to be suitable for both elastic traffic and inelastic traffic. Jing et al. [48] merge the theoretical framework in [15] with a constraint setting for wireless sensor networks. As in [15], [48], we use the utility based traffic allocation theory which is friendly with various types of services. Furthermore, considering the existence of misbehaving nodes, we use trust weights in UNUM approach for VANETs to allocate fair traffic among multiple services in adversarial environments. A brief comparison of fault aware service delivery approaches is given in Table 4.

VI. CONCLUSION

In this paper, we focused on the problem of reliable multiservice delivery which integrates misbehavior detection and tolerance for VANETs in the presence of misbehaving vehicles. Due to the probabilistic characteristics of variable misbehaviors, it was particularly important to model the stochastic state of being trusted for each vehicle. For that reason, extrinsic factors and intrinsic factors of vehicles were listed and were sent to the fog as the evaluation basis of trust weight metrics. We provided a trust based multiservice delivery framework of integrating misbehavior detection and tolerance via trust evaluation, multipath routing and traffic allocation. Moreover, a trust aware multiple-path routing protocol, TMRP, introducing trust weight into the multipath routing algorithm was presented. We incorporated trust weight in the utility optimization problem to capture QoS requirements for multiservice and then proposed a traffic allocation algorithm that maintained network performance in adversarial environments.

Firstly, we simulated the effectiveness of our routing protocol to indicate that TMRP improves the packet delivery ratio, with acceptable overhead and end-to-end delay. Secondly, the results showed that our traffic allocation algorithm could gain network performance including higher utilities and better utility fairness among different services. Finally, we evaluated the effectiveness of TMRP combined with TTA scheme, proving that misbehavior detection and tolerance were able to be mutually complementary. For the future work, we suppose to investigate more sophisticated attacker models, and to evaluate our integrated approach in other network scenarios.

REFERENCES

[1] M. Xing, J. He, and L. Cai, "Utility maximization for multimedia data dissemination in large-scale VANETs," *IEEE Trans Netw. Service Manage.*, vol. 16, no. 4, pp. 1188–1198, Apr. 2017.

[2] J. Ni, X. Dong, K. Zhang, and X. Shen, "Privacy-preserving real-time navigation system using vehicular crowdsourcing," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.

[3] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, "Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols," *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1505–1518, May 2013.

[4] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[5] H. Feng, C. Li, and Y. Xu, "Invulnerability analysis of vehicular ad hoc networks based on temporal networks," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Oct. 2016, pp. 2198–2202.

[6] H. Cheng, N. Xiong, A. V. Vasilakos, L. T. Yang, G. Chen, and X. Zhuang, "Nodes organization for channel assignment with topology preservation in multi-radio wireless mesh networks," *Ad Hoc Netw.*, vol. 10, no. 5, pp. 760–773, Jul. 2012.

[7] H. Su and X. Zhang, "Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3309–3323, Jun. 2007.

[8] M. A. Salkuyeh and B. Abolhassani, "An adaptive multipath geographic routing for video transmission in urban VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 10, pp. 2822–2831, Oct. 2016.

[9] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[10] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018.

[11] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. Vargas-Rosales, M. K. Khan, and S. Goudarzi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017.

[12] Y. Gao, F. Villecco, M. Li, and W. Song, "Multi-scale permutation entropy based on improved LMD and HMM for rolling bearing diagnosis," *Entropy*, vol. 19, no. 4, p. 176, 2017.

[13] K. Yang, S. Ou, H.-H. Chen, and J. He, "A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3358–3370, Nov. 2007.

[14] J.-W. Lee, M. Chiang, and A. R. Calderbank, "Price-based distributed algorithms for rate-reliability tradeoff in network utility maximization," *IEEE J. Select. Areas Commun.*, vol. 24, no. 5, pp. 962–976, May 2006.

[15] W.-H. Wang, M. Palaniswami, and S. H. Low, "Application-oriented flow control: Fundamentals, algorithms and fairness," *IEEE/ACM Trans. Netw.*, vol. 14, no. 6, pp. 1282–1291, Dec. 2006.

[16] 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," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.

[17] D. Hu, J. Wu, and P. Fan, "On the outage probability of interference-limited multi-hop linear vehicular ad-hoc network," *IEEE Access*, vol. 6, pp. 75395–75406, 2018.

[18] L. Tan, X. Zhang, L. L. H. Andrew, S. Chan, and M. Zukerman, "Price-based max-min fair rate allocation in wireless multi-hop networks," *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 31–33, Jan. 2006.

[19] K. Kang, C. Wang, and L. Tao, "Fog computing for vehicular ad-hoc networks: Paradigms, scenarios, and issues," *J. China Universities Posts Telecommun.*, vol. 23, no. 2, pp. 56–65, Apr. 2016.

[20] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun. 2017, pp. 591–602.

[21] W.-H. Wang, M. Palaniswami, and S. H. Low, "Optimal flow control and routing in multi-path networks," *Perform Eval.*, vol. 52, nos. 2–3, pp. 119–132, 2003.

[22] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1864–1875, Jul. 2014.

[23] J. Shen, C. Wang, A. Wang, X. Sun, S. Moh, and P. C. K. Hung, "Organized topology based routing protocol in incompletely predictable ad-hoc networks," *Comput. Commun.*, vol. 99, pp. 107–118, Feb. 2017.

[24] P. Tague, D. Slater, G. Noubir, and R. Poovendran, "Quantifying the impact of efficient cross-layer jamming attacks via network traffic flows," Netw. Secur. Lab, Univ. Washington, Seattle, WA, USA, Tech. Rep., 2009.

[25] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[26] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652–663, Mar. 2019.

[27] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET-A survey," *IEEE Trans. Intell. Transp. Syst.*, to be published. doi: 10.1109/TITS.2019.2893067.

[28] T. Lu, S. Chang, and W. Li, "Fog computing enabling geographic routing for urban area vehicular network," *Peer-Peer Netw. Appl.*, vol. 11, no. 4, pp. 749–755, Jul. 2018.

[29] K. Zhang, Y. Mao, S. Leng, A. Vinel, and Y. Zhang, "Delay constrained offloading for mobile edge computing in cloud-enabled vehicular networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling*, Sep. 2016, pp. 288–294.

[30] N. Noorani and S. A. H. Seno, "Routing in VANETs based on intersection using SDN and fog computing," in *Proc. 8th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, Oct. 2018, pp. 339–344.

[31] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A weighted trust-aware relay selection scheme for VANET," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[32] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[33] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416–424, 2016.

[34] R. Mitchell and I. R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.

[35] X. Wen, L. Shao, Y. Xue, and W. Fang, "A rapid learning algorithm for vehicle classification," *Inf. Sci.*, vol. 295, pp. 395–406, Feb. 2015.

[36] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 1071–1078.

[37] A. M. Vegni and T. D. C. Little, "A message propagation model for hybrid vehicular communication protocols," in *Proc. 7th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Newcastle Upon Tyne, U.K., Jul. 2010, pp. 382–386.

[38] S. M. Zin, N. B. Anuar, M. L. M. Kiah, and I. Ahmedy, "Survey of secure multipath routing protocols for WSNs," *J. Netw. Comput. Appl.*, vol. 55, pp. 123–153, Sep. 2015.

[39] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks," *J. Netw. Comput. Appl.*, vol. 33, no. 4, pp. 422–432, 2010.

[40] D. Han and J. M. Chung, "Self-similar traffic end-to-end delay minimization multipath routing algorithm," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2121–2124, Dec. 2014.

[41] Y. Challal, A. Ouadjaout, N. Lasla, M. Bagaa, and A. Hadjidj, "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 34, pp. 1380–1397, Jul. 2011.

[42] A. S. Lal and R. Nair, "Region authority based collaborative scheme to detect Sybil attacks in VANET," in *Proc. Int. Conf. Control Commun. Comput. India (ICCC)*, Nov. 2015, pp. 664–668.

[43] P. P. C. Lee, V. Misra, and D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," *IEEE/ACM Trans. Netw.*, vol. 15, no. 6, pp. 1490–1501, Dec. 2007.

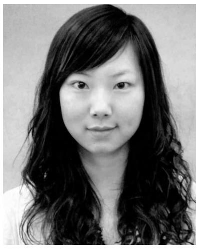
[44] Y. Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS-Aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE ACCESS*, vol. 5, pp. 21862–21872, 2017.

[45] P. M. Mohan, T. J. Lim, and M. Gurusamy, "Fragmentation-based multipath routing for attack resilience in software defined networks," in *Proc. IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, UAE, Nov. 2016, pp. 583–586.

[46] M. Saad, A. Leon-Garcia, and W. Yu, "Optimal network rate allocation under end-to-end quality-of-service requirements," *IEEE Trans. Netw. Service Manage.*, vol. 4, no. 3, pp. 40–49, Dec. 2007.

[47] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[48] J. Jin, M. Palaniswami, and B. Krishnamachari, "Rate control for heterogeneous wireless sensor networks: Characterization, algorithms and performance," *Comput. Netw.*, vol. 56, pp. 3783–3794, Nov. 2012.



XIAOMEI ZHANG received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2018. She is currently a Lecturer with the School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai. Her current research interests include wireless network security and distributed system security. Her publications include over 30 papers in scholarly journals and conference proceedings. She is a member of the Shanghai Computer Security (SCS).

CHEN LYU received the B.S. and M.S. degrees in telecommunications engineering from the Xidian University of China, Xi'an, China, in 2007 and 2010, respectively, and the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, in 2016. She is currently a Lecturer with the Department of Computer Science and Technology, Shanghai University of Finance and Economics, Shanghai. Her research interests include wireless security, applied cryptography, and security and privacy in online social networks.

ZHICAI SHI received the B.S. degrees from the School of Computer, Harbin Institute of Technology, China, in 1986, and the M.S. and Ph.D. degrees from the School of Control Science and Engineering, Zhejiang University, China, in 1996 and 2000, respectively. Since 2007, he has been with the School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, where he is currently a Professor. His research interests include identity authentication, privacy-preserving, and the analysis and design of the lightweight protocol.

DONGMEI LI received the M.S. degree from Zhejiang University, in 2001, and the Ph.D. degree from Shanghai Jiao Tong University, in 2018. She is currently a Teacher with the School of Electronic and Electrical Engineering, Shanghai University of Engineering Science. Her research interests include applied cryptography and information security, in particular, public key encryption, image encryption, and cloud computing security.

NEAL N. XIONG received the Ph.D. degrees from the Wuhan University (about sensor system engineering), and the Japan Advanced Institute of Science and Technology (about dependable sensor networks), respectively.

He is currently a Professor with the College of Intelligence and Computing, Tianjin University, China. Before he attended Tianjin University, he was with Northeastern State University, Georgia State University, Wentworth Technology Institution, and Colorado Technical University (full professor about five years) about 10 years. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory. He has published over 300 international journal papers and over 100 international conference papers. Some of his works were published in the IEEE JSAC, IEEE, or ACM transactions, ACM Sigcomm Workshop, the IEEE INFOCOM, ICDCS, and IPDPS. He has received the Best Paper Award in the 10th IEEE International Conference on High-Performance Computing and Communications (HPCC-08) and the Best Student Paper Award in the 28th North American Fuzzy Information Processing Society Annual Conference (NAFIPS2009). He has been the General Chair, the Program Chair, the Publicity Chair, a PC member, and a OC member of over 100 international conferences, and as a Reviewer of about 100 international journals, including the IEEE JSAC, the IEEE SMC (Park: A/B/C), the IEEE Transactions on Communications, the IEEE Transactions on Mobile Computing, and the IEEE Transactions on Parallel and Distributed Systems. He is serving as an Editor-in-Chief, an Associate Editor or Editor member for over 10 international journals, including an Associate Editor for the IEEE Transactions on Systems, Man and Cybernetics: Systems, an Associate Editor for the *Information Science*, the Editor-in-Chief for the *Journal of Internet Technology* (JIT), and an Editor-in-Chief for the *Journal of Parallel and Cloud Computing* (PCC), and a Guest Editor for over 10 international journals, including the *Sensor Journal*, WINET, and MONET.

CHI-HUNG CHI received the Ph.D. degree from Purdue University, West Lafayette, IN, USA. He is currently a Senior Principal Research Scientist of Data61 in CSIRO (Commonwealth Scientific and Industrial Research Organization), Australia. Before he joined CSIRO, he has been with industries, such as Philips Research Laboratory, USA, and IBM, Poughkeepsie, NY, USA, and universities, such as The Chinese University of Hong Kong, National University of Singapore, and Tsinghua University, for more than 20 years. He has published more than 260 international journal and conference papers and has edited ten books. He also holds six US patents. His research areas include cybersecurity, behavior modeling, knowledge graph, data engineering and analytics, cloud and service computing, social computing, the Internet-of-Things, and distributed computing.