Hindawi
Security and Communication Networks
Volume 2018, Article ID 7608198, 12 pages
https://doi.org/10.1155/2018/7608198

Research Article

Towards a Novel Trust-Based Multicast Routing for VANETs

Hui Xia,[1,2] **San-shun Zhang**,[1] **Ben-xia Li**,[1] **Li Li**,[1] **and Xiang-guo Cheng**[1]

[1]*College of Computer Science and Technology, Qingdao University, Qingdao 266071, China*
[2]*Department of Computer Science and Technology, Shandong University, Qingdao 266237, China*

Correspondence should be addressed to Hui Xia; xiahui@qdu.edu.cn

Received 12 June 2018; Revised 20 August 2018; Accepted 5 September 2018; Published 1 October 2018

Guest Editor: Chunqiang Hu

The Intelligent Transportation System (ITS) is an important application area of the Cyber-Physical System (CPS). To further promote effective communication between vehicles, vehicular ad hoc networks (VANETs) have been widely used in the ITS. However, the communication efficiency in VANETs is not only affected by the external environment but also more vulnerable to malicious attacks. In order to address the above-mentioned issues, we propose a novel trust-based multicast routing protocol (TMR) to defend against multiple attacks and improve the routing efficiency. In the proposed trust model, direct trust is calculated based on Bayesian theory and indirect trust is computed according to evaluation credibility and activity. The fuzzy logic theory is used to fuzzify the direct and indirect trust values, and then the total trust value of the node is obtained by defuzzification. With the help of the obtained trust values, malicious vehicle nodes are eliminated in the processes of route establishment and route maintenance, and finally, the network establishes trusted and efficient routes for data delivery. Comprehensive simulation experiments show that our new protocol can effectively improve the transmission rate of data packets at the expense of a slight increase in end-to-end delay and control overhead.

1. Introduction

As a combination of computation processes and physical processes, cyber-physical systems (CPS) organically integrate cyber systems and physical systems from environmental perception [1]. To monitor road conditions, reduce traffic accidents and improve transportation safety, researchers have applied CPS to the smart transportation system to form the Transportation Cyber-Physical System (T-CPS) [2]. With the popularity of wireless communication technology and mobile computing, the vehicular ad hoc network (VANET) is assumed to be a significant component for both safety and infotainment applications in T-CPS. VANET mainly adopts a vehicle-to-vehicle (V2V) communication mode, where participating vehicles and other neighboring vehicles are allowed to exchange data by the wireless transceiver, and if necessary, packets can be routed via adjacent vehicles to destinations outside the communication range. Drivers can make correct decisions by exchanging information about each other's driving intentions while driving. Emergency vehicles can warn cars to take prompt evasive actions, thereby providing an emergency passage. Vehicles can adjust routes in time according to congestion alerts issued by the traffic monitoring system. In the research on VANET, data distribution is regarded as one of the most critical processes, which mainly depends on efficient routing protocols [3]. In order to meet the different requirements of traffic users, the routing protocols for VANET should have specific constraints, such as a lowering of the end-to-end delay and packets loss when forwarding packets. So far, researchers have proposed routing protocols to ensure reliable data transmission and information exchange between vehicles, which are roughly divided into two categories (geography-based and topology-based) according to different networking methods [4].

Compared with the static or low-speed moving nodes in the traditional wireless network, the VANET node moves faster and unpredictably, which leads to frequent changes of network topology. Besides, owing to the unique features of VANET itself, such as its dynamism, complexity, and uncertainty, the difficulty of routing protocol design in VANET is increased still further. On the other hand, the VANET routing protocol is more vulnerable to threats due

to the lack of infrastructure and the self-organization of the network. Malicious vehicles may incorrectly forward and even drop packets, or divert packets towards the wrong relay nodes, preventing data from reaching their destination nodes. Furthermore, vehicles colluding in the network may also falsely improve their reputation, or maliciously slander trusted vehicles, thereby interfering with the assessment of node trustworthiness. If the reliability of the data cannot be adequately assessed, the driver may make wrong judgments based on malicious information received from misbehaving vehicles, resulting in severe traffic jams. To solve the routing security problem, cryptography-based and trust-based security mechanisms have been proposed [5–8]. The former focuses on the integrity of the data but does not identify malicious entities within the network [7]. On the contrary, the trust-based security mechanisms are widely used in dealing with internal attacks from malicious entities [8, 9]. However, how to design a secure and efficient routing protocol on the basis of the trust model is still a tremendous challenge in VANET.

Therefore, in this paper, we first design a novel trust model based on fuzzy logic theory to compute the trust value of vehicles by direct trust and indirect trust. Then, a secure multicast routing protocol based on the trust model is presented to deal with multiple attacks (e.g., black attack, grey attack, slander attack) from malicious vehicular nodes. The main contributions of this paper are as follows:

(1) In the calculation of trust values of nodes, various influencing factors affecting the trust are fully considered. Also, the time decay function is used to ensure that the node's recent performance is given higher weight in the trust calculation.

(2) The fuzzy logic theory is used to fuzzify the value of the real decision factor, fuzzy inference is performed according to fuzzy inference rules, and the final trust value of the node is obtained after defuzzification.

(3) We integrate trust models into routing protocols and design a secure multicast routing protocol to achieve reliable and secure communication from multiple sources to multiple destinations. Furthermore, we give detailed descriptions of the data structure and packet format, route discovery process and route maintenance process.

The remainder of this paper is organized as follows. Section 2 discusses recent works in the literature. We describe in detail a trust model in Section 3. In Section 4, we propose a trust-based multicast routing protocol. The experimental results are shown in Section 5. Finally, Section 6 presents concluding remarks and directions for future research.

2. Related Works

A routing protocol is the premise of effective operation for VANET. Slavik et al. [10] presented the Distribution-Adaptive Distance with Channel Quality (DADCQ) protocol which could select forwarding nodes based on the distance method. The decision threshold function is created to determine the decision threshold value and avoid the influence of node density, spatial distribution pattern, and wireless channel quality. Li et al. [11] proposed a novel intersection-based routing with QoS support for VANET, which composed of terminal intersection selection process, network exploration process and optimal routing path selection process. To minimize the end-to-end delay, Togou et al. [12] developed a distributed routing protocol called Stable CDS-Based Routing Protocol (SCRP). Before sending data messages, the protocol computes end-to-end delay of entire routing path based on the weight of each road segment. A cooperative volunteer protocol was proposed for VANET in [13] to broadcasting warning messages to emergency vehicles in Non-Line of Sight (NLOS) conditions. Moreover, the context-aware system is established to collect data and detect NLOS situations. To respond quickly to emergencies and prevent further accidents, Mezher et al. [14] designed a multimedia multi-metric map-aware routing protocol. The real maps with SUMO are utilized to create a realistic scenario, and the REVsim tool is exploited to choose a right forwarding node. In [15], the authors improve the existing ant colony optimization protocol using the concept of fuzzy logic, in which the validity of link is calculated by bandwidth, received signal strength metric and congestion metric.

With the increasingly prominent problem of route security, several schemes based on trust management have been proposed to deal with malicious attacks in VANET. Marmol et al. designed a proposal based on trust and reputation infrastructure for VANET in [16], which can precisely identify malicious or selfish nodes to prevent the spread of false or bogus messages. In [17], an event-based reputation system (EBRS) was proposed for defending against the conspired Sybil attacks. EBRS can detect and suppress the propagation of false messages employing reputation and trusted value of events. The probabilistic and deterministic approaches are used together to assess trust in [18]. The former computes the trust level of vehicles by using collected information, while the latter measures the trust level based on distances calculated. Sun et al. [19] presented a trust evaluation model based on membership cloud model for VANET. The goal of cloud model precisely describes the uncertainty of the trust relationships. Besides, they compute the cloud droplets and the aggregated trust values using trustworthiness and algorithm. Dahmane et al. [20] introduced a weighted probabilistic and trust-aware strategy to ensure that the most reliability relay nodes are selected in multi-hop communications. The authors in [21] proposed a security framework that consists of a hybrid trust model and a misbehaviour detection system, to detect malicious vehicles.

In recent years, some researchers have integrated the trust model into routing protocols and proposed many trust-based secure routing protocols. Based on the intersection-based routing protocol GyTAR, Bouali et al. developed a novel secure routing protocol S-GyTAR in [22]. The protocol monitors vehicles by cluster-based mechanism and evaluates trust value by a reputation-based scheme. A trusted routing protocol based on GeoDTN+Nav is proposed in [23], primarily, Bayesian trust management model and opportunistic routing forwarding models are used to establish security paths. Kerrache et al. [24] demonstrated a trust-based routing protocol, named TROUVE, to find the shortest and safest routing to a destination by the distribution of dishonest nodes in VANET.

Gazdar et al. [25] established distributed trust computing framework for VANETs, which employed the direct experience to calculate neighbors' trust value and utilized a tier-based approach to alleviate malicious behaviours. Given the authority levels of nodes, Yao et al. [26] developed a weight-based dynamic entity centre trust model. Furthermore, they also integrate the model into the routing protocol GPSR to enhance the security and improve the data delivery rate.

However, these above-mentioned researchers have not comprehensively investigated how to manage trust in vehicle ad hoc networks in a holistic manner. Besides, those mechanisms can introduce excessive routing overhead. Moreover, so far as we know, there are fewer security protocols for multicast which consider the concept of trust.

3. Trust Model

In this section, we describe our trust model in detail. The trust model in this paper contains two parts: the calculation of node trust and the calculation of path trust. The node's trust is determined by two trust factors: direct trust and indirect trust. And the path's trust is determined by the trust values of all the nodes on the path. Moreover, in this paper, we introduce a novel method to synthesize a relevant node's trust value.

3.1. Calculation of Node Trust. We introduce the sliding window mechanism to make sure that the latest interaction period can take a greater weight in the calculation of node trust.

3.1.1. Direct Trust. This latest period T can be divided into t time periods, that is, $T = \{T_1, T_2, T_3, \ldots, T_t\}$. It is assumed that in each period T_i, node A can monitor n_i times the forwarding behaviors of node B. The packet-forwarding ratios of node B in time period T_i are $v_{n_i} = \{v_{n_1}, v_{n_2}, v_{n_3}, \ldots, v_{n_i}\}$. We set a threshold ($L$) for the packet-forwarding ratio, if there are m_i times higher than the threshold L, and then the number below L is n_i-m_i. We make use of the Bayes theorem to reduce the error in computing the reputation of a specific node, which is calculated by combining the previous reputation level and likelihood function (i.e., the posterior probability in Bayes theorem is equal to the prior probability multiplied by the adjustment factor). Beta distribution conforming to the binomial distribution has the property of the conjugate prior. Applying the beta distribution to the Bayes theorem, if the prior probability satisfies the Beta distribution and the binomial distribution function denotes the likelihood function, then the final posterior probability is also satisfied the Beta distribution. In this way, we can keep the form of prior probability and posterior probability constant, and give both the prior probability and the posterior probability clearly physical meanings, separately.

In this paper, the last reputation vector denotes the prior probability and the current reputation vector represents the posterior probability. At this moment, the binomial distribution function can be used as the adjustment factor. The general form of the Beta distribution function is $\beta(a, b) = x^{a-1}(1 - x)^{b-1}/B(a, b)$, where $B(a, b)$ is a normalization constant which is used to ensure that the total probability is 1. We set $B(a, b) = \int_0^1 x^{a-1}(1 - x)^{b-1}dx$, where x satisfies $[0, 1]$. We assume that $R_{i\text{-}1}$ represents the value of the $(i\text{-}1)^{\text{th}}$ reputation evaluation vector according to the Beta distribution, and then the calculation of the posterior probability is $R_i = (f_i(x)/\int_0^1 f_i(x)R_{i-1}dx)R_{i-1}$. In this paper, two mutually independent events that conform to binomial distribution are taken as whether the forwarding rate is higher than the threshold value L, then it can obtained $f_i(x) = C_{n_i}^{m_i} x^{m_i}(1 - x)^{n_i - m_i}$. The reputation evaluation vector sequence of node A to B is $R_n = \{R_1, R_2, R_3, \ldots, R_t\}$. As mentioned above, if $R_{i\text{-}1} \sim beta(a_{i\text{-}1}, b_{i\text{-}1})$, then $R_i \sim beta(a_{i\text{-}1} + m_i, b_{i\text{-}1} + n_i\text{-}m_i)$. Then the values $a_1 = m_1$, $b_1 = n_1\text{-}m_1, \ldots, a_i = a_{i\text{-}1} + m_i$, $b_i = b_{i\text{-}1} + n_i\text{-}m_i$. Therefore, at the beginning t_0, we can set $a_0 = b_0 = 1$, $R_0 \sim beta(1, 1)$. One of the trust metrics t_d in the T_i time period can be computed and updated by using the expectation of beta distribution. The calculation equation is shown as follows:

$$t_d = \frac{a_i}{a_i + b_i} \quad (i \geq 1) \tag{1}$$

The direct trust of node B from the point of view of node A should also be affected by their interaction time and the total amount of packets forwarded. Therefore, we can use two metrics to describe the above-mentioned conditions, i.e., the time attenuation factor and the total amount of packets forwarded factor. The equation for calculating the direct trust is shown as follows:

$$dt_{AB} = \frac{\sum_{i=1}^{t} \rho^{t-i} M_{AB}^{i}}{M} * t_d \tag{2}$$

where $M = \sum_{i=1}^{t} \rho^{t-i}$, ρ^{t-i} $(0 < \rho < 1)$ denotes the time attenuation function, and M_{AB}^{i} denotes the amount of packets forwarded by node B for node A during the T_i period. The greater the amount of packets forwarded is, the higher the confidence of the obtained trust value will be. When there is no direct interaction between nodes A and B, the value of dt_{AB} is set to 0.5.

3.1.2. Indirect Trust. The indirect trust factor is crucial in the calculation of node trust. If node A and node B have no historical interactions, node A can still calculate the trust value of node B based on gathering other nodes' trust recommendations of node B. In this paper, two kinds of trust recommendation metrics (i.e., recommendation credibility and activity factor) are used to calculate the indirect trust of a specific node.

(1) Recommendation Credibility. Some malicious nodes do not discard or modify packets, while maliciously defaming other trustworthy nodes. This type of attack is also called a bad-mouth attack or slander attack. In order to resist these attacks, we can calculate the recommendation credibility of the recommended nodes. It is assumed that $\{j_1, j_2, j_3, \ldots, j_r\}$ are the neighbors of node j which have interactions with node i [27]. We can also divide the interaction period into $N * T_t$ $(N >= 1)$ time periods during which node i interacts with

any recommender. The direct trust of node j_l within the time period T_k is $dt^k_{ij_l}$ ($1 <= k <= N$) evaluated by node i, and the direct trust of j_l is $dt^k_{jj_l}$ evaluated by node j. Then, after the N-th interaction, the degree of deviation of node j for the trust evaluation of node j_l is calculated using the following equation:

$$tr_{ijj_l} = \sum_{k=1}^{N} \rho^{N-k} \left(1 - \left|dt^k{}_{jj_l} - dt^k{}_{ij_l}\right|\right) \tag{3}$$

Supposing the number of common nodes is r, these nodes interact with both node i and node j. Then compared with node i, the total degree of deviation of node j for trust evaluation is as follows:

$$tr_{ij} = \frac{\sum_{l=1}^{r} tr_{ijj_l}}{r} \tag{4}$$

We can suppose that there are R nodes that interact with j's neighbors. The greater the value of R is, the more accurate the obtained trust value will be. Then the recommendation credibility of node j is as follows:

$$tr_j = \frac{e^{-1/R} \sum_{i=1}^{R} tr_{ij}}{R} \tag{5}$$

where $0 < e^{-1/R} < 1$, and this metric is used to adjust the number of nodes on the evaluation of trust. The greater the value of R is, the closer it is to 1. We can also obtain a higher recommendation credibility value for node j. Moreover, we set an acceptable threshold for the recommendation credibility REC_THRESHOLD. If the node's recommendation credibility is lower than this threshold, the recommended information supplied can be ignored.

(2) Activity Factor. The metric H can be defined as the activity factor. If the number of neighbors of a specific node is G, and the number of neighbors that have recently interacted with this node is F, then we can calculate roughly the activity factor of this node using the following equation, $H = F/G$.

Finally, we can obtain the indirect trust of a specific node B as follows:

$$re_B = \frac{\sum_{j=1}^{F} tr_j dt_{jB} M_{jB}}{\sum_{j=1}^{F} tr_j M_{jB}} * H_B \tag{6}$$

Sections 3.1.1 and 3.1.2, respectively, calculate the node's direct trust and indirect trust. It is difficult to find an accurate mathematical model to integrate these two factors. Yet the ability to close the gap between imprecise human reasoning and the computational logic of fuzzy logic makes it especially attractive for the trust evaluation of the nodes.

3.1.3. Synthesis of Node Trust. The fuzzy logic model used in this paper is similar to the traditional fuzzy logic system which contains the following four steps: (1) transform the true value variable into a fuzzy set by a fuzzifier; (2) design fuzzy IF-THEN rules; (3) ue the fuzzy inference engine combined with fuzzy IF-THEN rules to derive the node's degree of trustworthiness; (4) use a defuzzifier to convert the fuzzy trustworthiness output into the real trust value.

First of all, we divided the two fuzzy trust factors into two levels, that is, great and small.

Definition 1 (input or output range). $0 \le dt \le 1$, $0 \le re \le 1$. The closer the value is to 1, the greater the input is. The output degree of node's trust is divided into four levels: fully trustworthy (ft), overall trustworthy (ot), generally trustworthy (gt), untrustworthy (ut).

Definition 2 (node trust value). The trust value of a node $0 \le$ trust ≤ 1. The closer the value is to 1, the higher the trustworthiness of the node is. Then these member functions are defined using triangular membership functions as follows:

$$small(x) = \begin{cases} \dfrac{0.6 - x}{0.6} & x \in (0, 0.6) \\ 0 & x \in (0.6, 1) \end{cases} \tag{7}$$

$$great(x) = \begin{cases} 0 & x \in (0, 0.4) \\ \dfrac{x - 0.4}{0.6} & x \in (0.4, 1) \end{cases} \tag{8}$$

$$ft(t) = \begin{cases} \dfrac{t - 0.6}{0.4} & t \in (0.6, 1) \\ 0 & t \in (0, 0.6) \end{cases} \tag{9}$$

$$ot(t) = \begin{cases} \dfrac{t - 0.4}{0.2} & t \in (0.4, 0.6) \\ \dfrac{0.8 - t}{0.2} & t \in (0.6, 0.8) \\ 0 & \text{others} \end{cases} \tag{10}$$

$$lt(t) = \begin{cases} \dfrac{t - 0.2}{0.2} & t \in (0.2, 0.4) \\ \dfrac{0.6 - t}{0.2} & t \in (0.4, 0.6) \\ 0 & \text{others} \end{cases} \tag{11}$$

$$ut(t) = \begin{cases} \dfrac{0.4 - t}{0.4} & t \in (0, 0.4) \\ 0 & t \in (0.4, 1) \end{cases} \tag{12}$$

The x in (7) or (8) represents the dt or re value of a specific node. The t in (9)~(12) denotes the trust value of this node. Input fuzzy set membership functions and output fuzzy set membership functions can be shown in Figure 1.

Because of the subjective characteristic of trust, the node is more inclined to believe in the empirical value based on the direct interactions between it and other nodes. Therefore the fuzzy IF-THEN rules we designed should ensure that the dt value takes a higher weight in the calculation of node's trust values. According to this, we set the four fuzzy IF-THEN rules as follows:

(1) IF dt is great AND re is great, THEN the node is fully trustworthy.

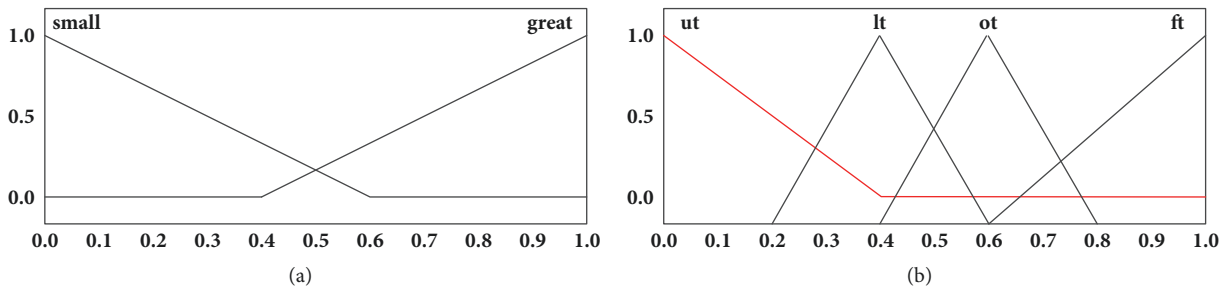


Figure 1: Membership functions: (a) input fuzzy set membership functions; (b) output fuzzy set membership functions.

(2) IF dt is great AND re is small, THEN the node is overall trustworthy.

(3) IF dt is small AND re is great, THEN the node is generally trustworthy.

(4) IF dt is small AND re is small, THEN the node is untrustworthy.

The membership functions and rules given above are just a set of instances. They can be revised as needed. If the input and output sets can be more reasonable, the evaluation result could be more objective.

The output fuzzy set is calculated by the fuzzy inference engine, and we define some required operators before building the engine. Then we apply the centroid calculation method to defuzzify the output fuzzy node trust value and finally get the true trust value of a node. The centroid calculation equation is shown as follows:

$$trust_B = \frac{\int_0^1 tf\,(t)\,dt}{\int_0^1 f\,(t)\,dt} \tag{13}$$

where $f(t)$ is the final expression of the trust value through fuzzy reasoning. We test several sets of trust values and get the results in Table 1.

We put four kinds of combination, i.e., $dt = 0.5$, $re = 0.4$; $dt = 0.4$, $re = 0.5$; $dt = 0.6$, $re = 0.4$; $dt = 0.5$, $re = 0.8$, into the fuzzy logic system to get the trust values of the node in Figure 2. We can figure out that the value of dt has a greater influence on the calculation of node's trust value than re through analysing a large number of results.

Figure 3 shows the distribution of trust values of a specific node for different input combination of dt and re. From the trend in the curvature of this graph, apparently we can see that when the dt value of the node is more than 0.4, as the dt value increases, the trust value of the node increases rapidly.

3.2. Calculation of Path Trust. The credibility of a routing path should also be assessed. In this paper, we use the metric 'path trust' (PT) to evaluate the above content. The path trust value is closely related to the trust value of each intermediate node on the path [28]. We refer to the barrel theory and take the node trust value which has the lowest credibility as the path trust value. For example, suppose that there are n nodes on the path, the source node is S, and the destination node is D. Then the path trust value PT_{SD} is calculated as follows: $PT_{SD} = \min\{trust_S, \ldots, trust_D\}$.

4. Applying Trust Enhancement to Multicast Routing

In this section, we apply trust enhancement to the standard multicast ad hoc on-demand distance vector routing protocol (i.e., MAODV [29]). We call this new trust-based routing protocol as multicast trust-based ad hoc on-demand distance vector routing protocol (i.e., MTAODV). Any node in the network can calculate its neighbor's trust value, and it can select a trustworthy routing path for data delivery.

4.1. Trust-Based Route Discovery. Three new fields are added to the original RREQ messages (i.e., Table 2) of MAODV that are reverse path trust, required path trust, and malicious node address. The initial value of reverse path trust is 1. If a node wants to join the multicast group but has no valid route, it will broadcast a J_flag RREQ message. The reverse path is built when the RREQ message comes to the reply node. A node that is close to the required node denotes the upstream node. In contrast, it is a downstream node if it is close to the reply node. The node that receives the message can calculate the trust value of the sending or forwarding message node [30, 31]. This relevant node trust value will be used to compare with the path trust value, and the reverse path value will be updated to the smaller one. However, if the node trust value is smaller than the required path trust, the J_flag RREQ message will not be forwarded further.

One new field (i.e., average trust value, ATV) is added to the original RREP messages (i.e., Table 3) of MAODV. Assume that a selected routing path contains n nodes, and then the average trust value can be calculated using the following equation:

$$ATV = \frac{\sum_{i=1}^{n} trust_i}{n}, \tag{14}$$

where $trust_i$ is the trust value of any node on the path. The multicast group member who has received the J_flag RREQ message will reply with the RREP to the source node. The forwarding route is built when the source node receives the message. When there is more than one path from the source node to the destination node, the source node should activate one of them. The traditional MAODV protocol stipulates that the shortest one is selected as a priority [32]. In MTAODV, the trust factor is the most important. So the destination node will choose a path that has the greatest average trust value

Table 1: The inference results of node's trust values.

dt	*re*	*Trust*
0.9	0.3	0.6
0.3	0.9	0.4
0.6	0.4	0.464
0.5	0.8	0.562

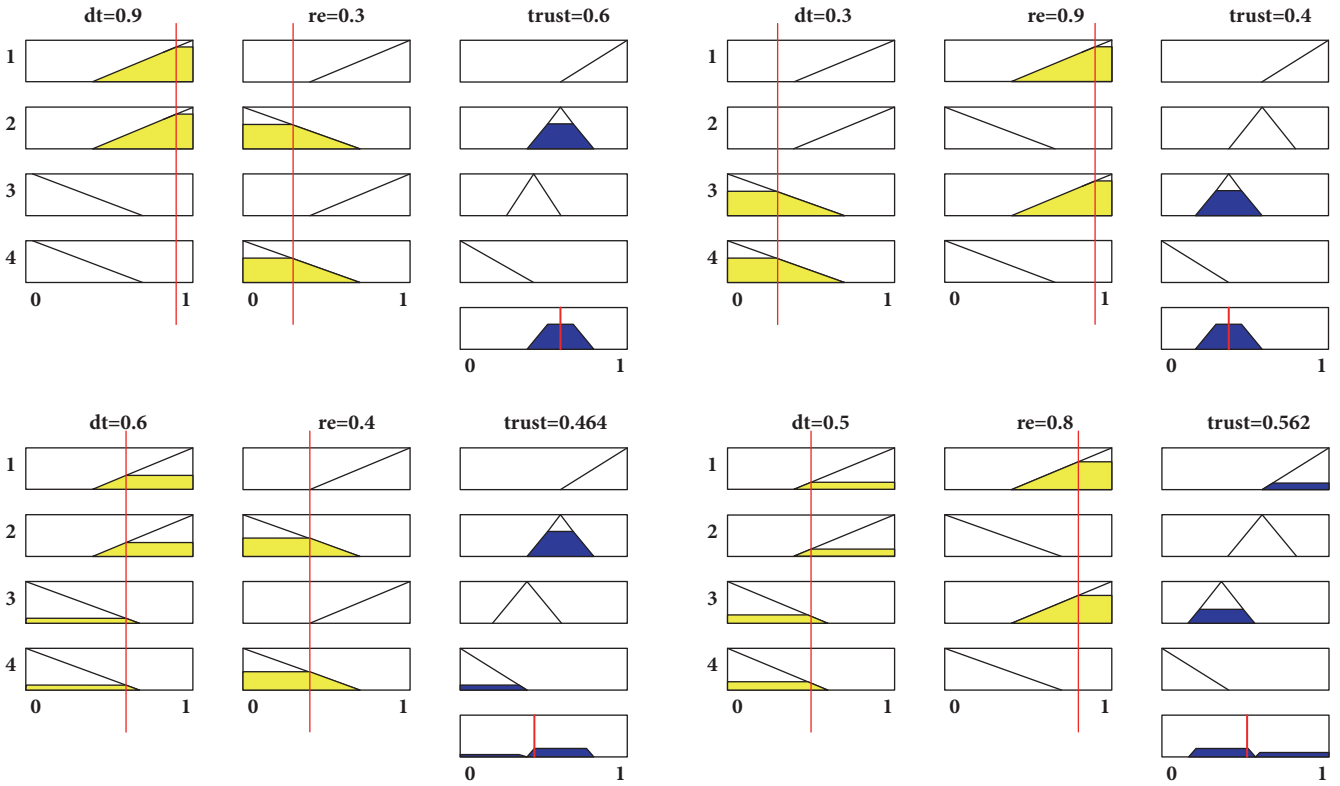


Figure 2: Node trust evaluation process.

Table 2: Enhanced RREQ message.

Dest_Addr
Dest_Seq
J_flag
R_flag
Originator IP Address
Originator Sequence Number
Lifetime
Reverse Path Trust
Required Path Trust
Malicious Node Address

Table 3: Enhanced RREP message.

Originator IP address
Dest_Addr
Dest_Seq#
R_flag
Mgroup_hop
Lifetime
Hop_Cnt
Average Trust Value

to send a MACT message. The path that has received the message is activated, and any node that has not received the message will delete the path of its cache.

4.2. Trust-Based Route Maintenance. Each multicast group member maintains a multicast routing table. In this paper, we put all the malicious node addresses in an array and place the array in a multicast routing table, as shown in the Table 4 'enhanced multicast routing table'.

After the multicast group is set up and the data is being transmitted, the upstream node can monitor the forward behaviors of the downstream node. If the downstream node is detected as a malicious node, the upstream node will unicast an RREQ message with this malicious node address (as shown in the Table 5) to the group leader. The group leader receives the message and replies with an RREP message to

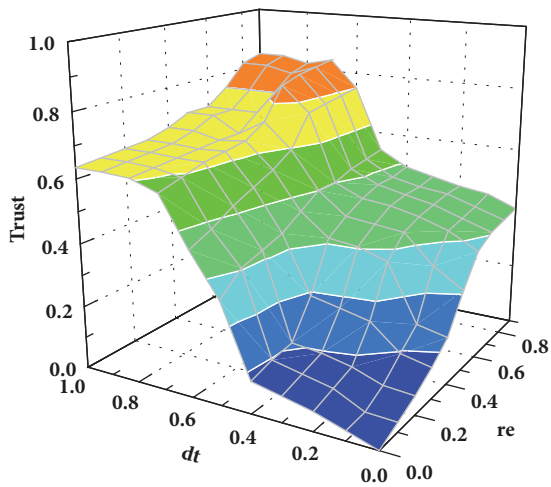


Figure 3: The surface of the node trust value.

Table 4: Enhanced multicast routing table.

Multicast Group IP Address
Multicast Group Leader IP Address
Multicast Group Sequence Number
Hop Count to Multicast Group Leader
Hop Count to next Multicast Group Member
Next Hops: Next Hop IP Address; Next Hop Interface; Link Direction; Activated Flag
{*MaliciousNode*$_1$ *Address*; *Malicious Node*$_2$ *Address*; *Malicious Node*$_3$ *Address*; }

that node. Then the group leader broadcasts a group hello message with the malicious node address to the entire network. A node that receives the message will record the malicious address in its multicast routing table. All multicast group members will disconnect from this malicious node and rediscover another route to the multicast group. The malicious node cannot be a group member until it recovers from the multicast routing table. It will recover from the multicast routing table after V_Threshold_time, and its trust value will be set to 0.5.

4.3. Restoration of Broken Branches. As shown in Figure 4, node S is the group leader. Supposing node B detects its downstream node C is a malicious node, it unicasts an RREQ message with this malicious node address (i.e., node C) to the group leader (i.e., node S). This group leader will reply with an RREP message to node B after it receives the RREQ message. Then the group leader broadcasts a group hello message with the malicious node address to the entire network. Each node in this network that receives the message will record the malicious address in its multicast routing table. All multicast group members in this multicast tree (i.e., node B and node

Table 5: Enhanced group hello message.

Group Leader IP address
Multicast Group IP address
Multicast Group Sequence Number
U_flag
O_flag
Hop Count
Malicious Node Address

F as shown in Figure 4) disconnect from this malicious node. For instance, node F automatically sends a MACT message with P_flag to the upstream node to disconnect itself from node C. Then, node F rediscovers another route to the multicast group via performing the restoration of broken branches. Besides, since the malicious node information (i.e., node C) has been stored in the malicious node table of the network node, the RREQ message with J_flag (initiated by node F) reforwarded by node C will be ignored by the next hop. This mechanism can ensure that the malicious node can no longer join the tree or become the intermediate forwarding node.

We set {hello_interval $*$ (1 + allowed_hello_loss)} as the threshold time to detect branch disconnection, and use the hello message to detect the break. If a node does not receive a hello message from a neighbor within the time specified above, it can determine that the branch is broken. Once the branch disconnection is detected, the downstream node repairs the broken link. The downstream node broadcasts a RREQ message with J_flag until the message reaches any group member, in which the destination address in this message is set as the address of the group leader, the destination sequence number is set as the last acquired multicast group sequence number, and Mgroup_Hop is set as the number of hops to the group leader. Then the downstream node establishes a path to this specific group member to complete the link repair.

5. Experimental Results

5.1. Experimental Setup. We use the NS-2.35 simulator [33] to estimate the performance of MAODV [29], MTAODV, LWT-MAODV [20] and RBTM-MAODV [26] under different scenarios. The experimental parameters are set as shown in the Table 6 [34]. In a 1000$*$1000 square metre area, 40 nodes perform the random way model. There are two source nodes and eight destination nodes. The delivery ratio threshold L is set to 0.7 and the base of the time attenuation function is set to 0.9. We change the node maximum speed and the number of malicious nodes in the network, respectively. In the following scenarios, two simple types of routing attacks (i.e., grey-hole attacks and black-hole attacks) are launched by malicious nodes. In grey-hole attacks, data packets were selectively forwarded by malicious nodes at a rate of 45%, while in black-hole attacks, all data packets were dropped.

5.2. Performance Evaluation. The performance of the entire network is shown by the following three vectors: packet delivery ratio, end-to-end delay, and control overhead. The

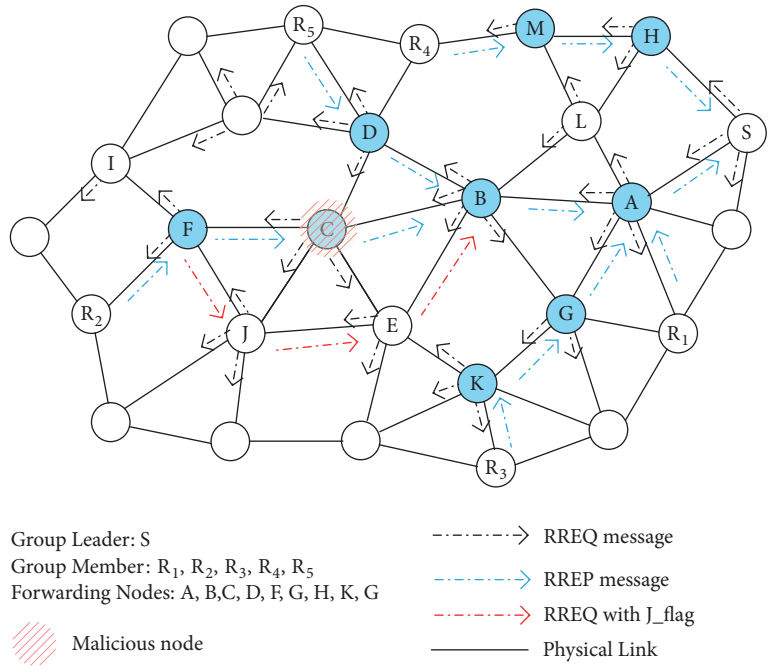


Figure 4: A simple example for restoration of broken branches.

Table 6: Network configuration parameters.

Parameter	Value
Simulation time	3000 s
Topology area	1000 m∗1000 m
MAC protocol	IEEE 802.11
Packet size	256 bytes
Node movement speed	5~30 m/s
Channel bandwidth	2 Mbits/s
Number of nodes	40
Source node	2
Destination node	8
Number of malicious nodes	0~10

packet delivery ratio represents the routing efficiency, and it is the fraction of the data packets that are received by the destination nodes compared to those sent by the source nodes. The end-to-end delay is the time used to receive all packets from the source node to the destination node. The control overhead is the ratio of the control bytes to the packet bytes in a network. Each experiment was repeated 30 times. The simulation results are shown in Figures 5 and 6.

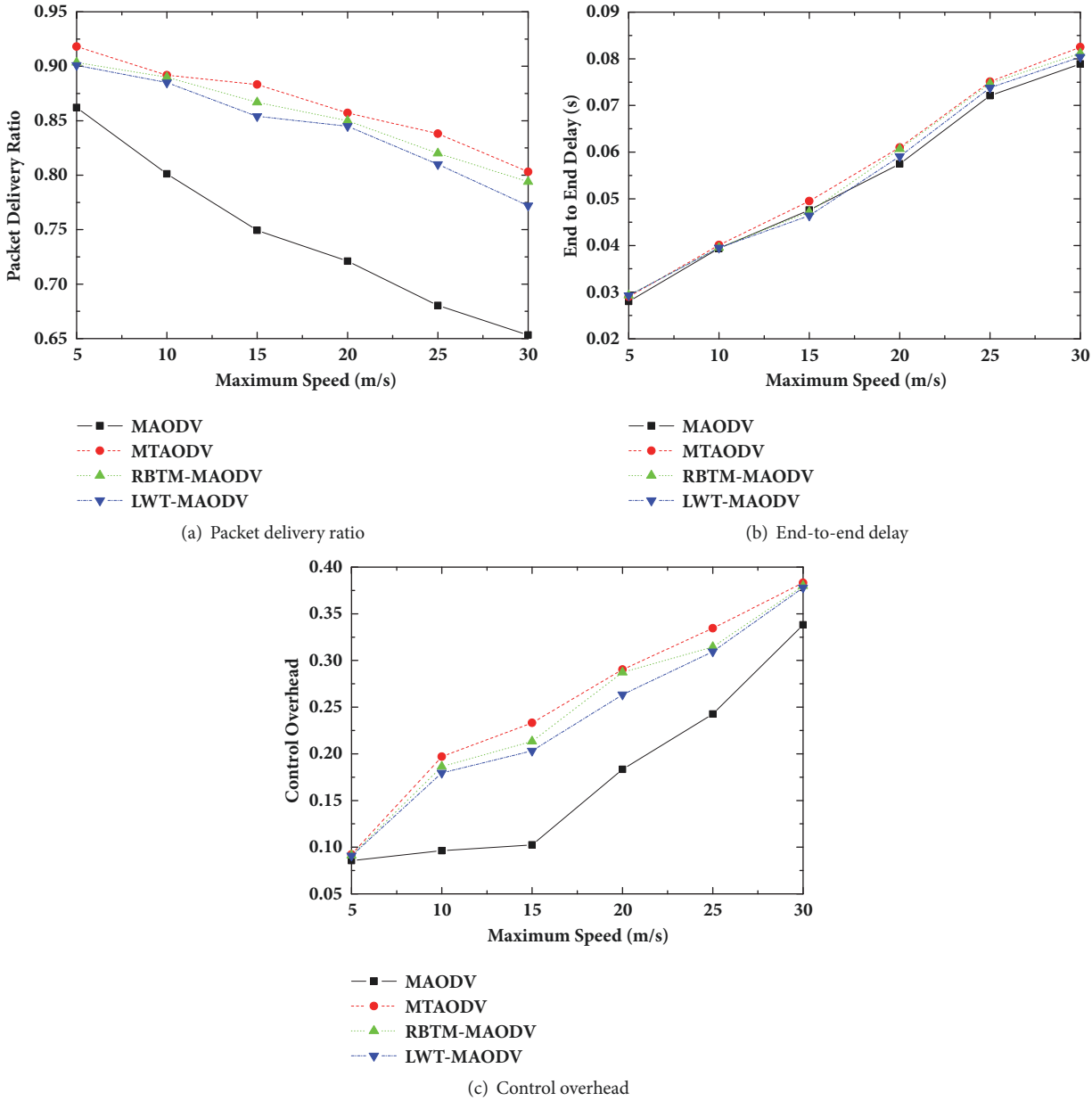
Test 1: Varying Node Maximum Speed. As shown in Figure 5(a), when there are three malicious nodes in the network, the packet delivery ratio is reduced by changing the network node maximum speed. The reason is that, with the nodes moving faster, the network topology changes more frequently, resulting in the probability of the packet transmission path being disconnected increases. The delivery ratio of MAODV declines sharply, while MTAODV, LWT-MAODV, and RBTM-MAODV perform more stable and the MTAODV performs better than the other two trust-based protocols. This figure shows that applying a trust model to a protocol can effectively exclude malicious nodes in the network. Compared with the other two trust models, using more trust metrics to calculate the trust value of nodes makes the MTAODV more effective.

Figure 5(b) shows that the end-to-end delay increases since the route linkage are susceptible to collapse. Along with the increase in node maximum speed, the end-to-end delay in MTAODV, LWT-MAODV and RBTM-MAODV is higher than MAODV. There can be several reasons: (1) These trust-based protocols choose a trusted path instead of the shortest one; (2) Once a malicious node is found on the path, the routing path will be broken. The network will subsequently perform the route maintenance operation, leading to an increase in the end-to-end delay.

Figure 5(c) shows that the control overhead in MTAODV, LWT-MAODV and RBTM-MAODV is relatively high compared with MAODV along with the increase in node maximum speed. The reason is that the enhanced trust-based protocol increases the computational complexity and requires more control packets. All the operations involving trust increase the control overhead.

Test 2: Varying the Number of Malicious Nodes. In the second experiment, we set the node maximum speed to 10 m/s.

Figure 6(a) illustrates that when the number of malicious nodes increases, the packet delivery ratios reduce in the four protocols. The larger the number of malicious nodes, the greater the hop count of the trusted route will be. This results in a notable decrease in the packet delivery ratio. The MAODV decreased significantly while the other



(a) Packet delivery ratio

(b) End-to-end delay

(c) Control overhead

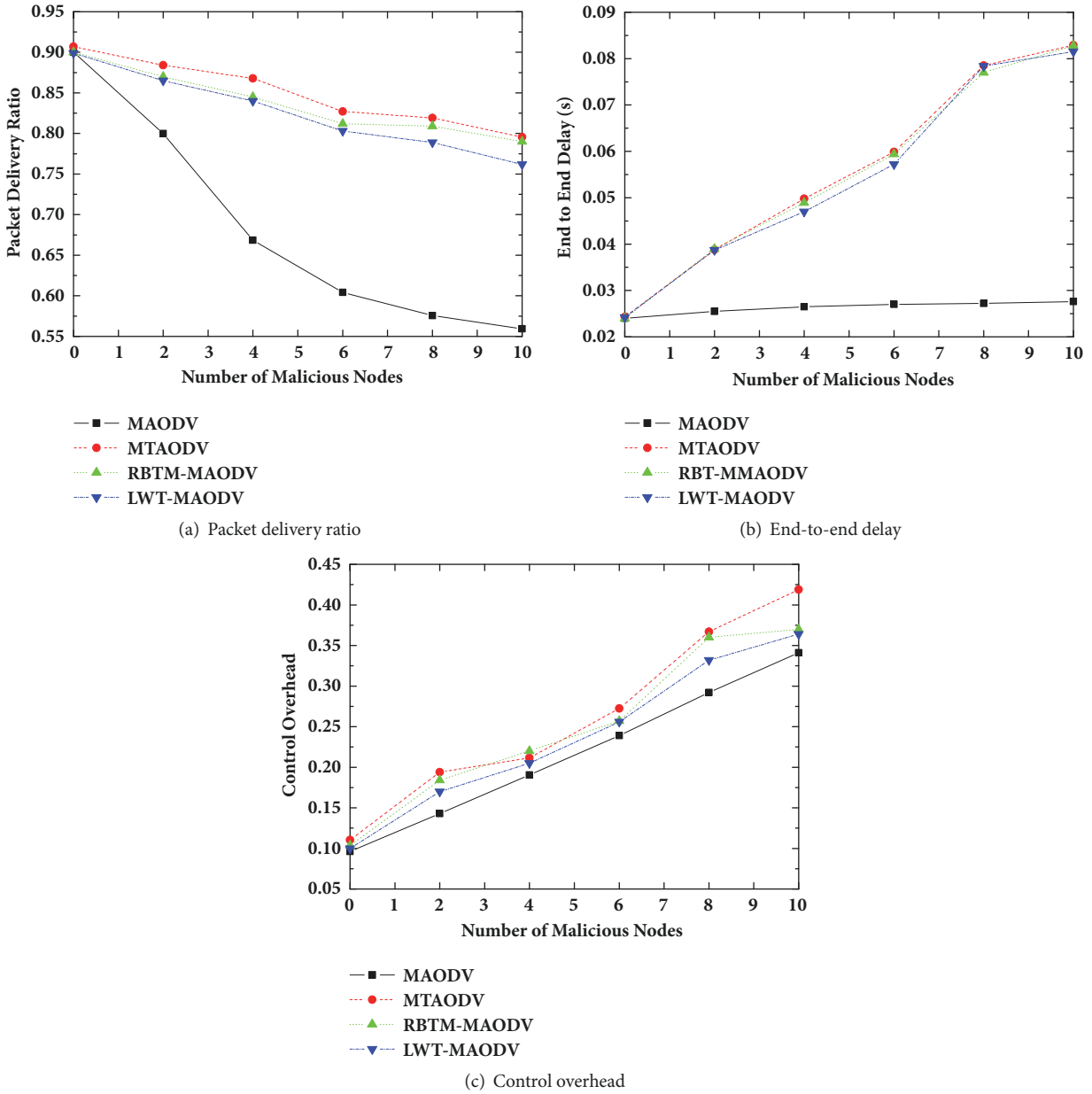
Figure 5: Performance with varying node maximum speeds.

three reduced slowly. The MTAODV performs the best. The fundamental reason is that the routing path which is built based on trusted routing algorithms is trustworthy. The source node can transmit the data packet to destinations without passing a malicious node.

We can see from Figure 6(b), the impact of the number of malicious nodes on end-to-end delay. The end-to-end delay is slowly growing in MTAODV, LWT-MAODV and RBTM-MAODV as the number of malicious nodes increases, while the packet delivery time in MAODV is not affected by the number of malicious nodes. The reasons for that are as follows: (1) the greater the number of malicious nodes in the network, the more times the number of available paths can be disconnected; (2) each node in the three trust-based protocols periodically broadcasts control packets for sharing the trust information; (3) the available channels are congested by the packets, delay occurs.

Figure 6(c) shows the changing trend of the control overhead with the increasing number of malicious nodes. The greater the number of malicious nodes in the network, the more control packets need to be broadcast, increasing the control overhead. The calculation method of malicious nodes in MTAODV is more complicated than the other two protocols, and more control packets need to be sent in the network, which leads to the maximum overhead.

According to Test 1 and 2, we can conclude that our new protocol can effectively improve the transmission rate of data



(a) Packet delivery ratio

(b) End-to-end delay

(c) Control overhead

FIGURE 6: Performance with varying the number of malicious nodes.

packets at the expense of a slight increase in end-to-end delay and control overhead.

6. Conclusions and Future Work

Vehicle ad hoc networks are vulnerable to various attacks due to their inherent features. It is relatively easy for multiple malicious entities to bring down the whole network in several network services. In recent years, the problem of routing security has become a significant concern for researchers. The trust-based countermeasure is considered to be more acceptable as a promising approach. The trust computing plays an important role to initialize a trusted network system. In this paper, we carry out a detailed study of the various trust-based countermeasures. More specifically, we first abstract a novel trust model. In the proposed trust model, direct trust is calculated based on Bayesian theory and indirect trust is computed according to evaluation credibility and activity. We subsequently proposed an efficient trust-based multicast routing protocol (MTAODV) on the basis of standard MAODV protocol, which is used to defend against multiple attacks and improve the routing efficiency.

In future work, we plan to conduct an in-depth study of trusted routing strategies, taking into account the requirements for deployment area issues, network applications, and security levels [35]. Moreover, trust computations and management can be an attractive target for attackers, since major decisions can be taken based on these trust computations.

Hence, defence mechanisms are also needed to be designed at the same time [36].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The received funding does not lead to any conflicts of interest regarding the publication of this manuscript.

Acknowledgments

This work is sponsored by the Natural Science Foundation of China (NSFC) under Grant no. 61872205, the Project of Shandong Province Higher Educational Science and Technology Program no. J16LN06, Source Innovation Programme of Qingdao no. 18-2-2-56-jch, and the State Foundation of China for Studying Abroad to Visit the United States as a 'Visiting Scholar'.

References

[1] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2015.

[2] Y. Zhou, Z. Mo, Q. Xiao, S. Chen, and Y. Yin, "Privacy-Preserving Transportation Traffic Measurement in Intelligent Cyber-physical Road Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3749–3759, 2016.

[3] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.

[4] S. Bitam, A. Mellouk, and S. Zeadally, "Bio-inspired routing algorithms survey for vehicular ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 843–867, 2015.

[5] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1362–1375, 2016.

[6] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling Cloud Storage Auditing With Key-Exposure Resistance," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1167–1179, 2015.

[7] J. Yao, S. Feng, and X. Zhou, "Secure Routing in Multi-hop Wireless Ad-Hoc Networks With Decode-and-Forward Relaying," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 753–764, 2016.

[8] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[9] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42–47, 2015.

[10] M. Slavik and I. Mahgoub, "Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET," *IEEE Transactions on Mobile Computing*, vol. 12, no. 4, pp. 722–734, 2013.

[11] G. Li, L. Boukhatem, and S. Martin, "An intersection-based QoS routing in vehicular ad hoc networks," *Mobile Networks and Applications*, vol. 20, no. 2, pp. 268–284, 2015.

[12] M. A. Togou, A. Hafid, and L. Khoukhi, "SCRP: Stable CDS-Based Routing Protocol for Urban Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1298–1307, 2016.

[13] K. Alodadi, A. H. Al-Bayatti, and N. Alalwan, "Cooperative volunteer protocol to detect non-line of sight nodes in vehicular ad hoc networks," *Vehicular Communications*, vol. 9, pp. 72–82, 2017.

[14] A. Mohamad Mezher and M. Aguilar Igartua, "Multimedia multimetric map-Aware routing protocol to send video-Reporting messages over VANETs in smart cities," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10611–10625, 2017.

[15] H. Fatemidokht and M. Kuchaki Rafsanjani, "F-Ant: an effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks," *Neural Computing and Applications*, vol. 29, no. 11, pp. 1127–1137, 2018.

[16] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[17] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017.

[18] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security ofwireless vehicular Ad-hoc networking," *Ad-Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[19] D. Sun, H. Zhao, and S. Cheng, "A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS," *Security and Communication Networks*, vol. 9, no. 18, pp. 5710–5723, 2016.

[20] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A Weighted Trust-Aware Relay Selection Scheme for VANET," in *Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017*, 6, 1 pages, May 2017.

[21] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET," *Wireless Networks*, 2018.

[22] T. Bouali, E.-H. Aglzim, and S.-M. Senouci, "A Secure Intersection-Based Routing Protocol for Data Collection in Urban Vehicular Networks," in *Proceedings of the 2014 IEEE Global Communications Conference, GLOBECOM 2014*, pp. 82–87, December 2014.

[23] Q. Wu, Q. Liu, L. Zhang, and Z. Zhang, "A trusted routing protocol based on GeoDTN+Nav in VANET," *China Communications*, vol. 11, no. 2, pp. 166–174, 2014.

[24] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TROUVE: A trusted routing protocol for urban vehicular environments," in *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, pp. 260–267, 2015.

[25] T. Gazdar, A. Belghith, and H. Abutair, "An Enhanced Distributed Trust Computing Protocol for VANETs," *IEEE Access*, vol. 6, pp. 380–392, 2017.

[26] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[27] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang, and R. Bie, "A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds," *IEEE Transactions on Big Data*, 2018.

[28] K. Xing, C. Hu, J. Yu, X. Cheng, and F. Zhang, "Mutual privacy preserving *k*-means clustering in social participatory sensing," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 2066–2076, 2017.

[29] S.-J. Lee, W. Su, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks," *Mobile Networks and Applications*, vol. 7, no. 6, pp. 441–453, 2002.

[30] Z. Cai, Z.-Z. Chen, and G. Lin, "A 3.4713-approximation algorithm for the capacitated multicast tree routing problem," *Theoretical Computer Science*, vol. 410, no. 52, pp. 5415–5424, 2009.

[31] Z. Cai, R. Goebel, and G. Lin, "Size-constrained tree partitioning: approximating the multicast *k*-tree routing problem," *Theoretical Computer Science*, vol. 412, no. 3, pp. 240–245, 2011.

[32] Z. Cai, Z.-Z. Chen, G. Lin, and L. Wang, "An improved approximation algorithm for the capacitated multicast tree routing problem," in *Combinatorial Optimization and Applications: Second International Conference, COCOA 2008, St. John's, NL, Canada, August 21–24, 2008. Proceedings*, vol. 5165 of *Lecture Notes in Computer Science*, pp. 286–295, Springer, Berlin, Germany, 2008.

[33] "A discrete event simulator ns-2," 2017, https://www.isi.edu/nsnam/ns/.

[34] F. Xiao, W. Liu, Z. Li, L. Chen, and R. Wang, "Noise-tolerant wireless sensor networks localization via multi-norms regularized matrix completion," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2409–2419, 2018.

[35] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. C. Choi, and H. Sekiya, "A Novel Light-weight Subjective Trust Inference Framework in MANETs," *IEEE Transactions on Sustainable Computing*, 2018.

[36] H. Xia, F. Xiao, S. Zhang, X. Cheng, and Z. Pan, "A Reputation-Based Model for Trust Evaluation in Social Cyber-Physical Systems," in *IEEE Transactions on Network Science and Engineering*, 2018.