T-AODV: a Trust-Based Routing against Black-hole Attacks in VANETs

Farnam Honarmand
Shiraz University
Alireza Keshavarz-Haddad (keshavarz@shirazu.ac.ir)
Shiraz University

Research Article

Keywords: Trust-based Routing, Fuzzy logic, VANET

Posted Date: October 23rd, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3354407/v1

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Peer-to-Peer Networking and Applications on February 17th, 2024. See the published version at https://doi.org/10.1007/s12083-024-01632-y.

Abstract

Vehicular Ad Hoc Network (VANET) is a key component in the Intelligent Transportation System (ITS) with a number of applications for safety, traffic management, emergency services, entertainment, and so on. These applications are implemented by exchanging data among the nodes in an open, dynamic, and distributed fashion, and hence VANETs are vulnerable to different network attacks. For examples, DoS and black-hole attacks can be easily executed in VANETs, and strongly affect the routing protocol and its functionality. Through the nature of VANETs, trust management is considered one of the practical means to secure these networks. In this paper, we propose an up-to-date dynamic entity-centric trust model for VANETs, called T-AODV. We use social science techniques to apply weight and fuzzy logic theory and identify the malicious nodes. Our NS2 simulation results indicate that T-AODV can be more resists in contact with black-hole attacks by boosting the security of AODV routing protocol. T-AODV slightly increases the routing overhead of AODV and provides better performance than the existing I-AODV scheme.

1 Introduction

Recently the proliferation of demand for security and efficiency of road transportation procedure have persuaded the originators to integrate wireless communications and networking in vehicles. In VANETs, vehicles collaborate to disseminate miscellaneous data messages using multi-hop paths, without the need for centralized supervision [1, 2]. Additionally, VANET is gaining more popularity, since this communication network can improve transferring users' data, internet access, detection of transportation traffic congestion, and so on [3–5].

Being structure-less, decentralized, and highly mobile are the intricate characters of VANETs that create several security issues. For instance, vehicles can play a role in VANET as sender or receiver and convey and acquire messages about the circumstances that witnessed and also fake information in this unstable perimeter as an autonomous device. Therefore, during the data exchange between distributed nodes, VANETs become vulnerable to many types of attacks. Finding an efficient solution to address the trustworthiness of messages and vehicles is a challenging task in VANET [6, 7].

Cryptography is the best-known technique to guarantee authenticity, privacy protection and confidentiality. Nonetheless, the cryptographic materials cannot cope with some issues such as authenticated selfish vehicles, excessive dynamicity of the VANET topology, and etc. Thus, as a denouement and unanimity between researchers, they have emerged as inquisitive about the trust management in VANETs, to support the cooperation between entities, detect selfish and misbehaving ones, and make certain dependable information conveyance and enhance the decision-making process [8–10]. Trust-based approaches can be categorized into three classes based on the principle assessment object, entity-centric, data-centric, and a combination of these trust models. In addition, interaction of entity trustworthiness and data trustworthiness in this network is completely palpable [11].

In this paper, an AODV routing protocol applied in vehicular networks; further, an entity-centric trust model endeavors to identify malicious nodes that take part in a black-hole attack to diminish the performance of the vehicular networks. Our nominated node-based trust model, called T-AODV, is designed to notch up network security by enhancing the AODV routing protocol. Here we presented a summary to illustrate our research contributions:

• To highlight the importance of data and the position of nodes in the network, like [6, 11], node and information weight is considered in our model,

• Trust as a prominent element to improve security in computer science, has a vague meaning. Thus, with the aid of using the fuzzy-based trust evaluation, the trustworthiness of nodes is guaranteed,

• Trust concept in computer science has been borrowed from the social sciences. Thus, we use social sciences as a general format to judge the behavior of nodes based on ability, expectation and functionality to distinguish among different positions belonging to each group of nodes,

• Our NS2 simulation and the detailed analysis display the legitimacy of our suggested paradigm that improves the trustworthiness in the network.

The following divisions are elucidated the rest of our article: Related works on trust management in Ad Hoc and vehicular networks are examined in section 2. Section 3 describes the system models and associated assumptions. The trust modus is presented and detailed in section 4. The simulation results for comparing our method with other existing schemes in terms of performance measurement parameters are presented in section 5. Finally, by way of a conclusion, section 6 is presented.

2 Related work

When it comes to coaction among objects in VANETs, the most conspicuous necessity that guarantees the legitimacy and plausibility of its responses and respondents is trust. Here, sundry trust approaches are made known, which makes it possible to establish trust among entities and what they pass on, i.e., the reliability of messages and malicious entity blocking. However, introducing a way that coats all the stipulations of a faultless trust strategy is infeasible. As a consensus among researchers, they are sorted into three bunches: entity-based methods and data-based methods, and hybrid that is a combination of these methods [11, 13–15].

Concentration on assessing the trustworthiness of vehicles is the predominant strategy in entity-centric trust patterns, which can be done with the help of sentiments that are presented via other neighbors [15–17]. To lessen the effects of control overhead and at last have a quicker method, while intervening vehicles carry out their functions as an observer, just who has a passable scale of trust, further transmission range and a smaller load of evaluation can be selected for this cooperation [16]. In [18], the authors propose a ground-breaking trust algorithm which counts the control packets and has the ability to detect some attacks in the Ad Hoc networks like black-hole attacks. By adding a trust table for trust

level calculation on the original routing protocol, which here is AODV, the proposed scheme is able to diagnose the attacks by determining Trust Local (TL) and Trust Global (TG) specifications. As this method just concentrates on control packets, without any attention to data packets, some smart attacks would deprive the network.

In [11], to heighten the security, an entity-centric trust module and weight concept are applied by the authors on the GPSR routing protocol. Data packets play a prominent role in this recipe as opposed to the control packets, which was stated earlier. In [19], an infrastructure-based plan with the help of trust and fame, namely TRIP, is suggested. At any time that a node receives any information from another node, at first by combining direct previous experiences, neighbors' recommendations, and infrastructures' recommendation through RSUs (if it is available), the node computes the reputation score of senders and with the help of decision-making based on fuzzy logic and determines that each vehicle places in which trust levels. Another assumption in this model is the severity level for each message which helps us to forward or ignore them.

Researchers have speculated that it is more rational to construct the trust algorithm based on data instead of the reporting nodes. Accordingly, in event-centric trust models, the principal content is the transmitted data among nodes. Although, latency and data sparsity is the major demerits of this policy [11, 15, 16]. Energy-related information in electric vehicular networks and a central processing entity is proposed in [20]. It discriminates between credible and erroneous values and addresses malevolent vehicles to disseminate this false information based on a fuzzy trust model. Moreover, using this momentous action, authors try to figure out the quickest route from A to B based on the least time and energy consumption. In [6], authors who use genetic programming, concentrate their evaluation on data trustworthiness in VANETs and try to find genuine received data and benevolent sender.

Trust models falling under the combined set are created with the aim of insuring a safe communication between vehicles in a space that simultaneously considers the effects of malicious messages and malign vehicles. In most of the presented models, it is common to use the clustering technique to break the communication costs [8, 14]. In [21], to make a vehicular network safer as well as possible, acquaintance, credibility and a fuzzy trust model are exerted. Moreover, two auxiliary concepts, namely fog nodes and LOS/NLOS, are introduced as supplementary tools which calculate the events' location preciseness and senders' location faultlessness. Authors proposed the latter because they think immovable obstacles are extensive interferences in desirable communications among vehicles. In other words, these barriers can threaten the security components of the network. A proposed hybrid trust management scheme in [22], by dint of sporadic voting, identifies the cluster and proxy cluster head. Resource availability, as a composite metric, should be computed to demonstrate that a node has satisfactory resources and suffices the least possible requirement to accomplish its duty as a cluster head after selecting. In [23], suggested the structure according to the first-hand knowledge among neighbors, apply tier-based data circulating on the way to come across faux activities and vehicles as a doer. How much it can be practical must be reviewed on the basis of the amount of data that transfer in the network and the limitations about time for vehicular networks.

As we know, entities have a fundamental role in a routing protocol in VANETs, thus our proposed trust model will be validated in routing protocols. Also, AODV is part and parcel of mobile networks, as the most leading routing protocol. Nevertheless, exerting AODV as a routing protocol in VANET is susceptible to security threats like black-hole attacks [11, 28, 34].

In this work, we introduce an entity-centric trust strategy that tends to be implemented over the AODV routing protocol. By inspiring social sciences and knowing that the application data is a key parameter for trust management, we consider the type of event as a key metric in our model. Obviously, different vehicles have different intentions and roles in VANETs, hence, it is rational to consider the type of vehicle as another metric. Since, data gathering in vehicular networks can be affected by imprecise and indistinct information on the basis of the nature of intermittent connection and sequential communication, the precision of embedded detectors, egotistical behavior, and so, etc., we apply the possibility theory for combining vague opinions of different nodes to obtain more accurate trust values.

3 Preliminaries and Assumptions

In order to describe our proposed method, in this section we briefly explain the network model, the application model, security model, fuzzy logic model, social sciences, and trust model.

3.1 Network model

In spite of the resemblance between VANET and MANET such as nodes that move fleetly and a network topology that alter ceaselessly is noticeable, in VANET, roads have been predefined for nodes and also nodes' rapidity has been confined by an authentic system. By and large, the VANET nodes are armed with special gadgets to form this kind of network like calculating and wireless communication modules, smart detectors, GPS, and other devices. The nodes have different types and would transfer different types of data. Routing is one of the most important aspects that should occur perfectly since establishing suitable routes for data access between vehicles is essential [11, 25, 26].

3.2 Application model

Predominantly, the supreme duty in the VANETs is to distribute observations that vehicles come across. Vehicles convey this information between themselves as safety or non-safety object. These messages can be categorized into two types: beacon and event messages. The latter one is disseminated by entities just according to what they perceive on the network. As a united acceptance, these observations are labeled by safety, efficiency, and infotainment. The first group is the most pivotal data, due to its role in increasing security in perilous circumstances. The second group aims to set up an efficient network to escalate productivity associated with situations such as rush-hour traffic gridlocks. The third group which has the least level of importance includes information about convenience and amusement like parking/petrol stations and public places [4, 6, 11, 27].

3.3 Security model

Security as a combination of processes and procedures endeavors the system to perform its assignments precisely. Due to VANET's security weaknesses, security and privacy are at risk [28]. Notwithstanding, not all of these threats can be predicted, some of these scenarios can be known to a certain extent, and therefore it is possible to be resistant to and robust against them. These attacks can challenge the physical part as well as data transmission. Thus, creating a trust-based process that has the aptitude to unmask and protect these potential risks and attacks is instrumental.

A brief review of what has been said up till now about trust methods unfolds that a comprehensive trust model should follow some requirements and desired properties such as a decentralized trust establishment, coping with sparsity, sensitivity to privacy concerns, and so forth. Notably, it is an indispensable act to consider the trust metrics for a meticulous calculation and to fulfil this goal. A part of these criteria is distance, time, recommendation by vehicles or RSUs, the quantity of senders and the quality of information they can provide according to their position, and direction, also sort of event and sort of vehicle that are pivotal in this paper. Nevertheless, as we know, active attacks like DoS and black-hole attacks can easily occur in VANETs, thus, in spite of the fact that all items in a network have their status, a secure path is the foundation of a secure connection. By considering security concerns associated with each layer in the protocol stack, precise routing execution is disturbed as a result of attacks like black-hole in the network layer [7, 29, 30].

3.4 Fuzzy Logic & Social Sciences & Trust

In classical theories, each member tends not to accept a proportion of the membership. That is, we need a mean like fuzzy set theory which is capable to display imprecise and insufficient amounts of data and a kind of uncertainty using a certain degree of membership. Therefore, some of the characteristics and structures of fuzzy logic are given below to clarify the reason for choosing this approach.

• When it comes to speaking about an environment in which uncertainty is part and parcel of that, and besides, the object of the game is to obtain a crisp output, trust tends to be an effectual tool,

• Trust as a precious concept in VANET can be illustrated by social science which is apposite to human dynamic traits,

• As for trust and its vague temperament, fuzzy techniques can lay a solid foundation for the trust decision making,

• Regarding inputs and their ambiguity, as a general rule, a natural skeleton can be contrived by fuzzy logic,

• The qualitative analysis of the fuzzy logic that presents intervals rather than exact values is the main facet to launch and come under scrutiny with natural language tags,

• Acquirement information in VANETs suffers from uncertainty owing to the fact that embedded sensors are inexact and behaviors can be in the interest of personal or group benefits, and so forth.

As a social sciences-based model, in a society, when we consider different positions for people, we cannot judge them and their functionality with an equal assessor. We need to look at our expectations and the social status of individuals as two issues together, not separately. Therefore, using a fuzzy logic model with equal fuzzy memberships cannot help us to achieve the goal. Thus, we must consider different fuzzy sets for each of the defined vehicle groups. With this work, we consider the nodes' ability in the system, and despite controlling all behaviors, we also pay attention to their positions in the network [8, 17, 31–33].

4 Proposed Methodology

We put forward this approach for the sake of an improvement in the performance of routing protocol and to enhance its security. As an undebatable topic, relay nodes have the most role in this action. Thus, it is logical to consider an entity-centric trust model for hinted goals. On the other hand, researchers believe that data has a pivotal role in VANETs since it makes sense to focus on data-centric trust models. According to what was discussed before, we intend to adapt our model to what exists in the social sciences and seek help from it. In a rational society, we expect the right behavior from people with higher social and moral status. Although, it can be claimed that inherently many humans show the right behavior as long as their own interests are not at stake. Hence, to make way for trust determination based on the social sciences, the importance of exchanged data must be taken into account. That is, to ensure the acceptability of the received message, we say: “Who said and what he said”. Because, that person may not be in a position to be aware of such an important message, which from the point of view of computer sciences also indicates which kind of node and what kind of data are in the network. For this reason, node and data in the network are considered weighted, which implicitly states that in vehicular networks, the basis of reliable data transmission, is reliable nodes, and these two are necessary and bound to each other.

4.1 Network model based on weight

Like the majority of methods that focus on trust computing based on existing entities, we calculate this amount of trust in accordance with the first-handed exchanges between two nodes and the suggestion and opinions of other nodes, such as neighboring nodes. Here, we do focus on the weight of data and nodes. Events have distinct effects on transportation and avenue protection, and also dissimilar trustworthiness levels are requisite. We divide them into three groups as follows:

• Data that has safety applications and is effective in enhancing public safety and saving lives. Such as announcing car accidents, announcing blind spots on the roads, thick fog, etc. This type of data has the highest degree of sensitivity and we assign weight of 1 to them

• Data that can be used to improve efficiency. Such as traffic control, parking information, closed streets, gas station, etc. which are less important than the first part, although they are very valuable and we assign a weight of 0.8 to them

• Data use for infotainment. Such as data related to advertising or exchanging entertaining information such as music, restaurants, etc. We assign a weight of 0.5 to them, because of the least importance

Also, nodes in vehicular networks contain a huge range of vehicles that have different roles, so according to their authenticity in the network and experimental results, we divide them into three groups as follows:

• Nodes that have the highest level of authenticity (High Level). Such as police cars and roadside units controlled by centers. we assign a weight equal to 1 to them

• Nodes that have the second level of authenticity (Medium Level). Such as vehicles that perform public transportation or road maintenance vehicles, etc. which can be controlled by certain centers. We assign a weight equal to 0.7 to them

• Nodes that have the lowest level (Low Level). Such as personal cars and freight cars. We assign a weight equal to 0.5 to them

4.2 Trust computing algorithm

The amount of direct trust, recommendation trust from third parties, and also their combined values are used as three meaningful parameters to determine the trust level of each node. Afterwards, we can identify the malicious node based on a threshold value, and remove those nodes from the network. Most articles consider first-hand experience as the most important data. We should also mention that such information is not always available, so it is necessary to rely on second-hand information through testimonies from witness nodes.

In Table 1 some notations are listed to illustrate the proposed scheme (node A is sender and node B is receiver).

Table 1
Notations.

Notations	Meaning
N_A^B	All messages that the sender pled the receiver to forward
M_A^B	All messages that the receiver has forwarded for the sender
W_D^x	The weight of data (x), (in detail, part 4.1)
W_N^A	The weight of the sender, (in detail, part 4.1)
$U_W^{A.B}$	Total weight of data that the sender pled the receiver to forward
$S_W^{A.B}$	Total weight of data that the receiver has successfully forwarded for the sender
$E_{TW}^{A.B}$	The average weight of all data that the sender pled the receiver to forward
$E_{SW}^{A.B}$	The average weight of all data that the receiver has successfully forwarded for the sender
F_W^B	The malicious tendency of the receiver, (part 4.2 & Eq. (1))
DT_A^B	The direct trust value of sender-receiver
RT_A^B	The recommended trust value of sender to receiver
T_A^B	The comprehensive trust value of sender to receiver

Direct Trust. This concept expresses the expectation that one node has of another node's future behavior. Since, due to the dynamic behavior of vehicular networks, these nodes may not have communicated with each other in the past, initial direct trust values are usually considered 0.5 in most articles.

Here the value of direct trust is considered equal to the node's weight to imply the importance of the vehicle's position, also, received information from the center, is more reliable than normal vehicles, because of more control centers that monitor their actions. For this part, as an assumption, node A tries to compute node B's direct trust. Thus, first and foremost, a malicious tendency is calculated by Eq. (1) which defines the nature of B as a member of society. Based on experimental results that elucidate the portion of miscellaneous data type in traffic models. Thus, 0.72 is considered as a threshold, in other words, having a malicious tendency more than this value clarifies the malevolent essence of the receiver node and vice versa.

$$F_W^B = (U_W^{A.B} - S_W^{A.B})(N_A^B - M_A^B)$$

1

Therefore, assuming that node A has requested to send message x from node B, taking into account the reaction of this receiver, direct trust can be calculated as Eq. (2) as below:

$$DT_A^B = \begin{cases} \frac{W_D^x.(\frac{(flag+1)}{2} - DT_A^B)}{1+\frac{E_{TW}^{A.B}}{E_{SW}^{A.B}}} + DT_A^B; F_W^B < 0.72 \\ \frac{W_D^x.(\frac{(flag+1)}{2} - DT_A^B)}{4} + DT_A^B; F_W^B \geq 0.72 \& (flag = 1) \\ W_D^x.\left(\frac{(flag+1)}{2} - DT_A^B\right) + DT_A^B; F_W^B \geq 0.72 \& (flag = -1) \end{cases}$$

2

If the receiver sends the message successfully, the flag in Eq. (2) is equal to 1, otherwise, is equal to -1.

Recommendation Trust. The recommendation trust is taken from other nodes or even central units along the road so that the agent can express their opinion about the subject with others' suggestions. Usually, this happens when in direct contact, the obtained value is not quite close to the upper or lower limit, and it is not possible to comment clearly on a node (subject). Therefore, here in Eq. (3), node A as the sender of message x to node B takes help from neighboring nodes to give its final vote.

$$RT_A^B = \frac{\sum_{i=1}^{n} DT_A^{N_i}.T_{N_i}^B.W_N^{N_i}}{\sum_{i=1}^{n} DT_A^{N_i}}; N_i \neq B; N_i \mathrm{is the} i' \mathrm{th neighbor of sender.}$$

3

Comprehensive trust & Fuzzy based trust assessment approach. The total amount of trust, in other words, how to combine the values of direct and recommendation trust in the previous sections is vital. How and in what pattern should combined these two values to achieve the best result? Most articles, such as [11] usually use one coefficient, or even several coefficients such as [19], which is a number in the range of zero to one, and try to create the best creation mode in the form of dynamic coefficients. For example, when one node directly has sufficient knowledge of another node, it tries to reduce the effect of the proposed trust value to a slight or even close to zero, and vice versa. But such a performance in the few articles discussed did not lead us to the desired results. So, it enforced us to move on to another model. We will make use of fuzzy logic to combine hinted values.

Here the proposed fuzzy-based paradigm is described. Indeed, the use of fuzzy logic, whose philosophy is to combine vague inputs to achieve crisp output [19–21]. By using three different fuzzy models for different groups of vehicles, we judge all these vehicles' behavior, regardless of their weight, with the same threshold value for the desired results. Thus, each group uses the fuzzy logic model according to next stages: (1) a fuzzy set is created by a fuzzifier as a transmutational action; (2) layout fuzzy IF-THEN rules; (3) the credibility level is notched up for each node by an amalgamation of the fuzzy inference engine and IF-THEN rules; (4) the fuzzy trustworthiness output is transformed to a real value of trust by a defuzzifier [20, 24]. Therefore, for each group of vehicles, using fuzzy logic, according to Direct Trust Level (DTL) and Recommendation Trust Level (RTL), and considering Table 1, in VANETs, we can identify malicious nodes, in black-hole attack (in Table 1; L is Low, M is Medium, H is High, and TTL is Total Trust Level).

Table 2
Obtain total trust through the fuzzy inference engine.

Rule no.	DTL	RTL	TTL
1	L	L	L
2	L	M	L
3	L	H	L
4	M	L	L
5	M	M	M
6	M	H	H
7	H	L	H
8	H	M	H
9	H	H	H

We use a Min-Max inference and also a defined fuzzy set to obtain the correlation among these columns. Finally, a fuzzy domain is converted to precise domain using a centroid method for the defuzzification aim. Thus, in three sections we will express it in a completely separate and understandable way:

Case 1

Input fuzzy set membership functions for the vehicles that receive the message and have the highest weight values equal to 1 (Fig. 1 and Fig. 2). Also, excerpts from the node trust evaluation process, taken from MATLAB software to better understand the differences between positions (Fig. 3)

Case 2

Input fuzzy set membership functions for the vehicles that receive the message and have the weight values equal to 0.7 (Fig. 4 and Fig. 5). Also, excerpts from the node trust evaluation process, taken from MATLAB software to better understand the differences between positions (Fig. 6)

Case 3

Input fuzzy set membership functions for the vehicles that receive the message and have the weight values equal to 0.5 (Fig. 7 and Fig. 8). Also, excerpts from the node trust evaluation process, taken from MATLAB software to better understand the differences between positions (Fig. 9)

In this algorithm, DTL and RTL, are two inputs in Table 1, and each of them includes three fuzzy sets, that are defined in the table. Therefore, according to these inputs, the table of rules is formed with 9 so-called IF-THEN rules, so that we can express the Total Trust level (TTL). It should be noted that in Table 1, the importance of direct communications between two nodes is quite clear. Because, when a node has a definite opinion about the behavior of the other node, there is no need to consult other nodes, and waste the time.

5 Performance Evaluation

Here, the performance of our trust-based AODV (T-AODV) strategy with the original AODV and another trust-based AODV (I-AODV) [11] are measured and compared via simulation.

5.1 Simulation Setup

Inclusively, we have listed all necessities for simulation in Table 2. The main aim is to diagnose which node is malevolent in the network. Thus, firstly, our routing protocols (AODV, I-AODV, and T-AODV) are experimented whilst the network has not under any attack. Secondly, by keeping other details constant, we subject the network to a black-hole attack to compare the performance.

Throughput, average end-to-end delay, average consumed energy, and packet delivery ratio, as four main metrics, are obtained to monitor the performance in different situations, especially the efficacy of the trust

strategy on AODV routing protocol in a vehicular network.

Table 3
Simulation details.

Parameters	Values
network simulator	NS2.35
network area	1000m*1000m
simulation time	500s
number of nodes	15,30,50,70,90,110,130,150
number of malicious nodes	3 (20%,10%,6%,4.3%,3.4%,2.7%,2.3%,2%)
signal propagation model	Tow Ray Ground
routing protocols	AODV, I-AODV, T-AODV
traffic model	CBR
radio distance	250m
mac layer protocol	MAC 802.11
moving speed	0m/s ~ 20m/s
the maximum size of a packet	512byte
trust threshold	0.6

5.2 Simulation Results

In order to obtain the smooth curve we consider the mean value of each metric over 10 iterations. We present the results for two scenarios separately as following.

Scenario 1. Without any attack; It is illustrated in Fig. 10 ((a), (b), (c), and (d)) that the performance of T-AODV and AODV are fundamentally in line with each other and they have a striking resemblance in the four desired parameters. However, I-AODV is distinctly different and leaves behind a weaker performance in comparison with the other two routing protocols.

In detail, as regards trust model for I-AODV routing scheme, even without any attacks in the VANET, some nodes are identified as malicious, while they are not inherently malevolent. It causes a considerable decline in the performance of this scheme. In other words, the results show that during a normal and expected network operation, the average packet delivery ratio and the throughput for I-AODV are around 84% and 70 respectively, in comparison with the other two methods that are roughly in line with each other and nearly 91% and 76 in turn.

Moreover, the average consumed energy and end-to-end delay for AODV and T-AODV are acceptable because of more activity in the direction of data transmission. Clearly, there is a trade-off between security and these metrics for trust models.

Scenario 2. With attack; A black-hole attack in this part is activated and thus, all the packets will be dropped by these malevolent nodes. The simulation results are depicted in Fig. 11 for all three AODV-based routing protocols.

The simulation results show in (e) and (f) of Fig. 11 that the T-AODV, the I-AODV, and the original AODV routing protocol have the best execution with respect to packet delivery ratio and throughput, respectively. On the contrary, (g) and (h) of Fig. 11 show that the original AODV routing protocol has a much lower average consumed energy and average end-to-end delay than those of T-AODV and I-AODV, which is because of less activity in the direction of data transmission.

In detail, comparing with the scenario without attack, regarding the original AODV routing protocol which does not have any trust mechanism to find malicious nodes, in (a) and (b) of Fig. 10 and in (e) and (f) of Fig. 11, the execution has plummeted. But, T-AODV and I-AODV routing protocols have a stiff resistance against black-hole attacks. So, it is worth noting that T-AODV executes more desirable with respect to the packet delivery ratio and the throughput than I-AODV, at least 16% and 17% in turn.

The mean value of end-to-end delay and consumed energy in (g) and (h) of Fig. 11 for T-AODV and I-AODV routing protocols are to some extent in line with each other, and more than the original AODV routing protocol, which is because of more activity in the direction of data transmission, and absolutely acceptable.

Overall, what stands out from these graphs is that there were considerable upward trends in the performance of routing protocols that use trust to enhance security issues, meanwhile, when the network is subjected to a black-hole attack, the work presentation of the original routing protocol plunged.

6 Conclusion

In this paper, as one of the most challenging issues in the VANET, the black-hole attack is addressed. A trust method based on entity simultaneously considering the importance of data with weighted values, also with inspiration from the social sciences as a model that simulates the role of nodes in the network, is considered as a countermeasure. Ultimately, to combine these fuzzy inputs to find and cross out malicious nodes in the vehicular grid, the possibility theory is proposed. We demonstrated that the performance of our revised AODV routing scheme (T-AODV) is higher than the existing scheme (I-AODV) and the original AODV routing scheme by simulation analysis in NS2. The packet delivery ratio and the throughput, as two critical touchstones, are considerably improved in T-AODV. As a tradeoff among different metrics, the increase in time and energy is important; fortunately, the values are acceptable in this work. Future research concerns designing a more general routing scheme based on trust to deal with other types of attacks on VANETs.

Declarations

Ethics Approval Not applicable.

Conflict of Interest The authors declare no conflict of interest/competing interests.

Data Availability All data generated or analyzed during this study are included in this published article.

Author Contribution The manuscript was written entirely by the authors. All authors made an equal contribution to the development of the paper.

Funding No funds, grants, or other support was received.

Consent to publish All authors unanimously agree to publish the paper.

References

1. S.-Y. Han and C.-Y. Zhang, "ASMAC: An Adaptive Slot Access MAC Protocol in Distributed VANET," Electronics, vol. 11, no. 7, p. 1145, 2022.
2. 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, 2015.
3. R. S. Al-Qassas, "Routing and the Impact of Group Mobility Model in VANETs," J. Comput. Sci., vol. 12, no. 4, pp. 223-231, 2016.
4. M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," EURASIP Journal on Wireless Communications and Networking, vol. 2018, no. 1, pp. 1-17, 2018.
5. K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," International Journal of System Assurance Engineering and Management, vol. 11, no. 2, pp. 426-440, 2020.
6. M. Aslan and S. Sen, "Evolving trust formula to evaluate data trustworthiness in VANETs using genetic programming," in International Conference on the Applications of Evolutionary Computation (Part of EvoStar), 2019: Springer, pp. 413-429.
7. A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. A. Kumar, B. K. Panigrahi, and K. C. Veluvolu, "Black-hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," Microprocessors and Microsystems, vol. 80, p. 103352, 2021.
8. S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee, and S. Mandala, "Trust management in vehicular Ad Hoc network: a systematic review," EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, pp. 1-22, 2015.
9. I. Souissi, N. B. Azzouna, and T. Berradia, "Towards a Self-adaptive Trust Management Model for VANETs," in SECRYPT, 2017, pp. 513-518.

10. K. N. Tripathi, A. M. Yadav, and S. Sharma, "Fuzzy and Deep Belief Network Based Malicious Vehicle Identification and Trust Recommendation Framework in VANETs," Wireless Personal Communications, pp. 1-30, 2022.
11. 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.
12. A. Paranjothi, M. S. Khan, S. Zeadally, A. Pawar, and D. Hicks, "GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model," Internet of Things, vol. 7, p. 100071, 2019.
13. W. Ahmed, D. Wu, and D. Mukathie, "Blockchain-Assisted Trust Management Scheme for Securing VANETs," KSII Transactions on Internet and Information Systems (TIIS), vol. 16, no. 2, pp. 609-631, 2022.
14. C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS," Computer Communications, vol. 93, pp. 68-83, 2016.
15. Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018: IEEE, pp. 98-103.
16. A. Chowdhury, G. Karmakar, and J. Kamruzzaman, "Trusted autonomous vehicle: Measuring trust using on-board unit data," in 2019 18th IEEE International conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), 2019: IEEE, pp. 787-792.
17. A. Tajeddine, A. Kayssi, A. Chehab, and H. Artail, "Fuzzy reputation-based trust model," Applied soft computing, vol. 11, no. 1, pp. 345-355, 2011.
18. H. Simaremare, A. Abouaissa, R. F. Sari, and P. Lorenz, "Secure AODV routing protocol based on trust mechanism," in Wireless Networks and Security: Springer, 2013, pp. 81-105.
19. F. G. Mármol and G. M. 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.
20. I. Souissi, N. B. Azzouna, T. Berradia, and L. B. Said, "Fuzzy Logic based Model for Energy Consumption Trust Estimation in Electric Vehicular Networks," in ICETsE (2), 2018, pp. 387-399.
21. 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.
22. A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A hybrid trust management heuristic for VANETs," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019: IEEE, pp. 748-752.
23. T. Gazdar, A. Belghith, and H. Abutair, "An enhanced distributed trust computing protocol for VANETs," IEEE Access, vol. 6, pp. 380-392, 2017.

24. H. Xia, S.-s. Zhang, B.-x. Li, L. Li, and X.-g. Cheng, "Towards a novel trust-based multicast routing for VANETs," Security and Communication Networks, vol. 2018.
25. M. Sindhwani, R. Singh, A. Sachdeva, and C. Singh, "Improvisation of optimization technique and AODV routing protocol in VANET," Materials Today: Proceedings, vol. 49, pp. 3457-3461, 2022.
26. S. Xi and X.-M. Li, "Study of the Feasibility of VANET and its Routing Protocols," in 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008: IEEE, pp. 1-4.
27. Y. Toor, P. Muhlethaler, A. Laouiti, and A. De La Fortelle, "Vehicle Ad Hoc networks: Applications and related technical issues," IEEE communications surveys & tutorials, vol. 10, no. 3, pp. 74-88, 2008.
28. M. Akhlaq, M. N. Jafri, M. A. Khan, and B. Aslam, "Addressing security concerns of data exchange in AODV protocol," International Journal of Information and Communication Engineering, vol. 2, no. 4, pp. 677-681, 2008.
29. L. Jun, L. Zhe, L. Dan, and L. Ye, "A security enhanced AODV routing protocol based on the credence mechanism," in Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005, vol. 2: IEEE, pp. 719-722.
30. F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," Ad Hoc Networks, vol. 61, pp. 33-50, 2017.
31. C. Castelfranchi, R. Falcone, and G. Pezzulo, "Trust in information sources as a source for trust: a fuzzy approach," in Proceedings of the second international joint conference on Autonomous agents and multiagent systems, 2003, pp. 89-96.
32. N. Jyothi and R. Patil, "A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET," Journal of Information and Telecommunication, pp. 1-19, 2022.
33. H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proceedings of the IEEE, vol. 98, no. 10, pp. 1755-1772, 2010.
34. H. Yang, "A study on improving secure routing performance using trust model in MANET," Mobile Information Systems, vol. 2020, 2020.

Figures

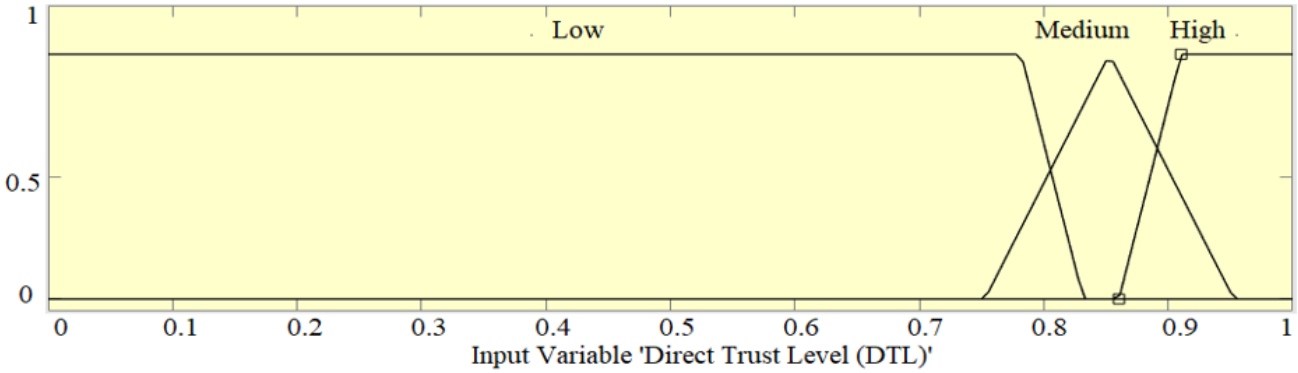


Figure 1

Input fuzzy set membership functions for direct trust level.

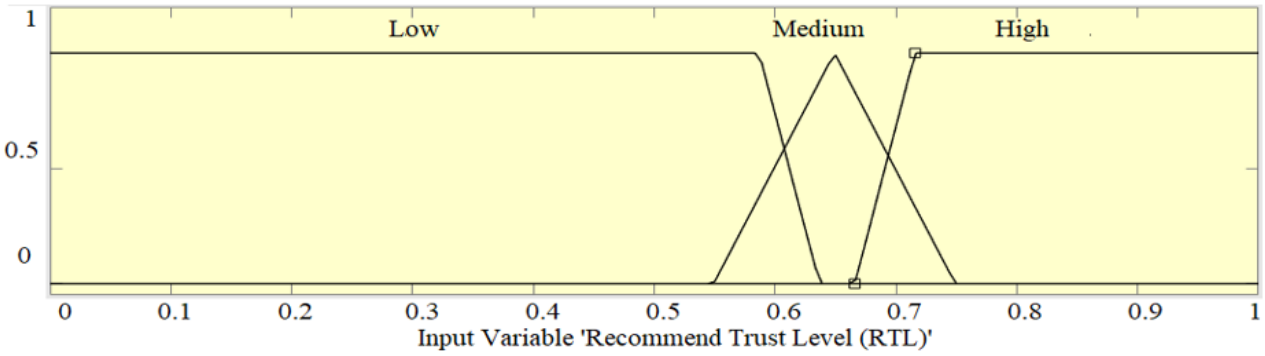


Figure 2

Input fuzzy set membership functions for recommend trust.

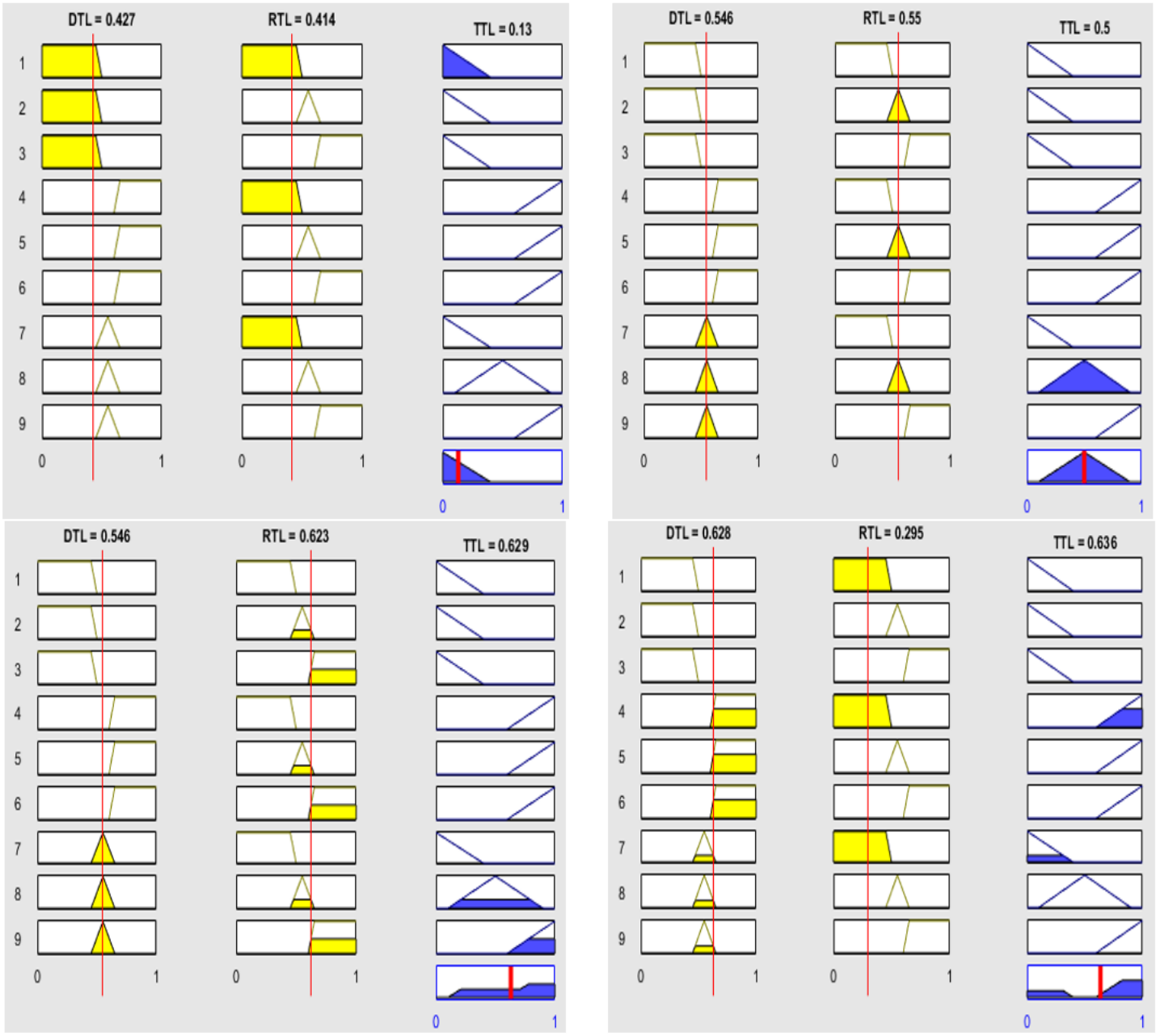


Figure 3

Node trust evaluation process.

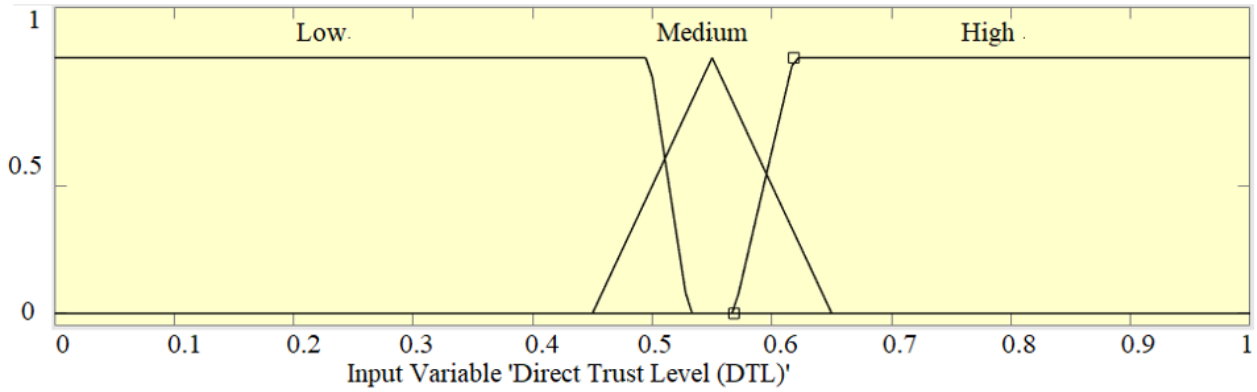


Figure 4

Input fuzzy set membership functions for direct trust level.

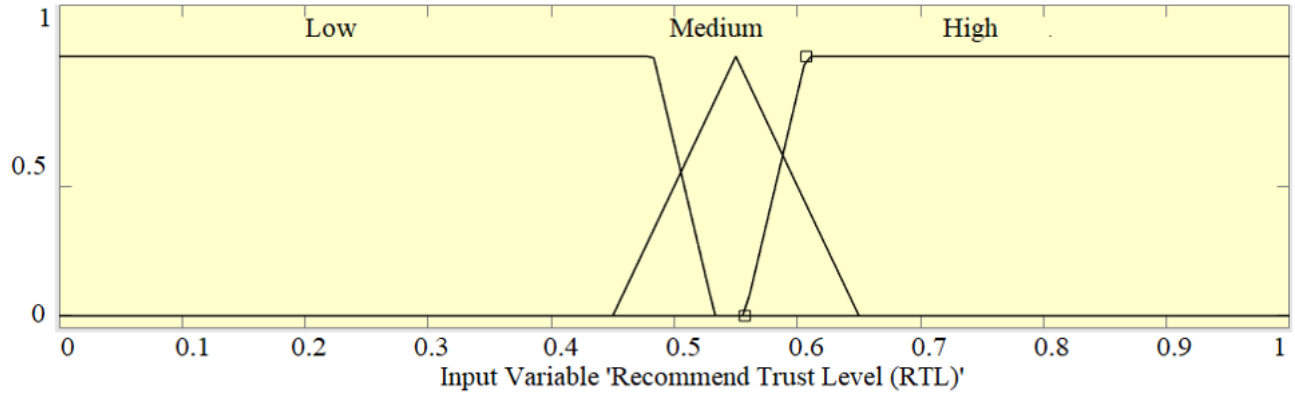


Figure 5

Input fuzzy set membership functions for recommend trust.

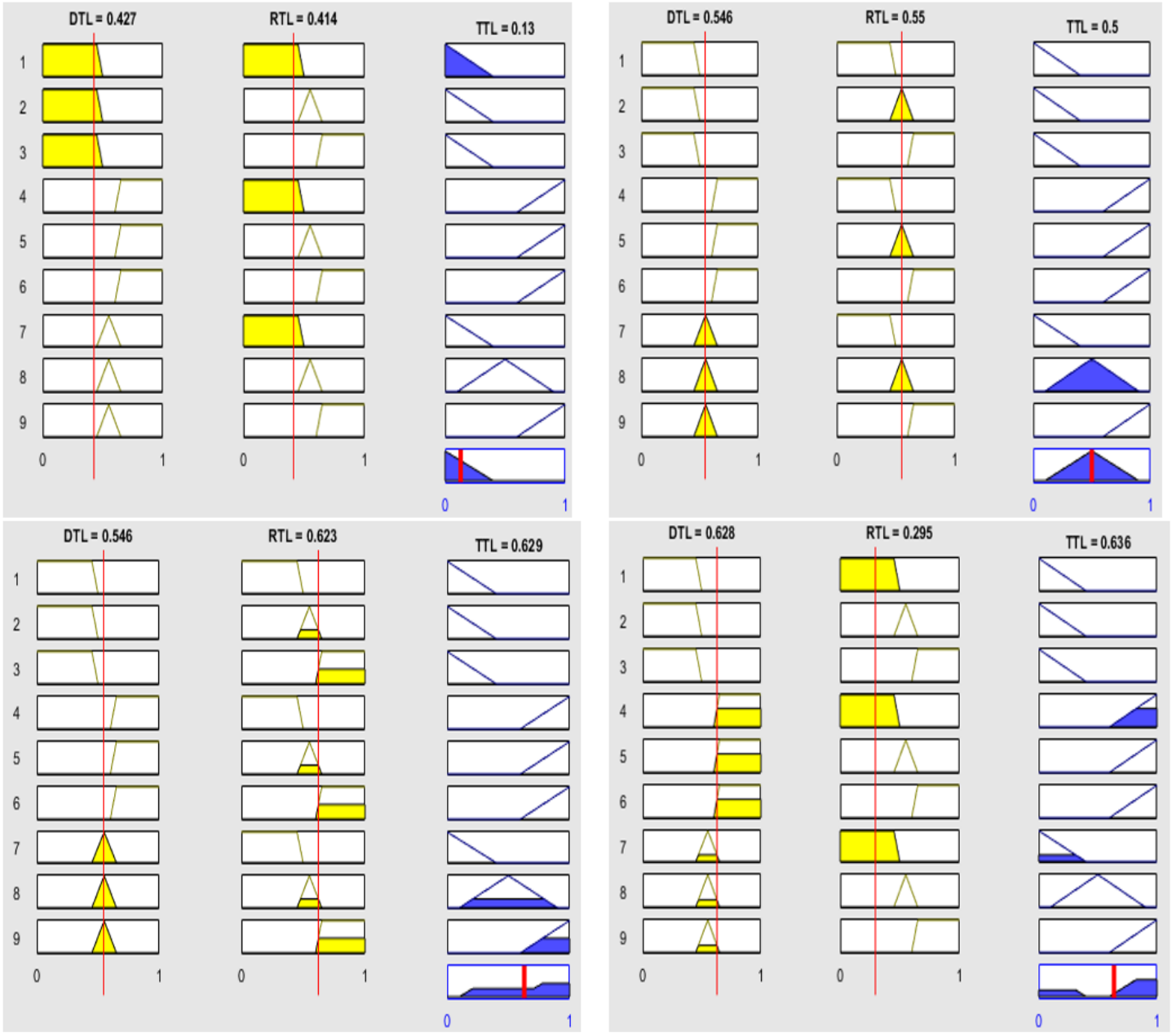


Figure 6

Node trust evaluation process.

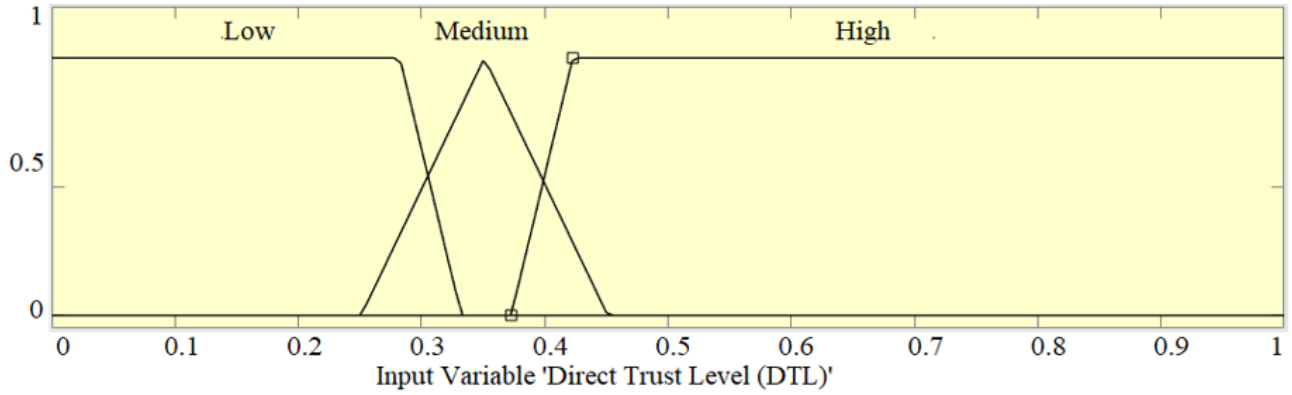


Figure 7

Input fuzzy set membership functions for direct trust level.

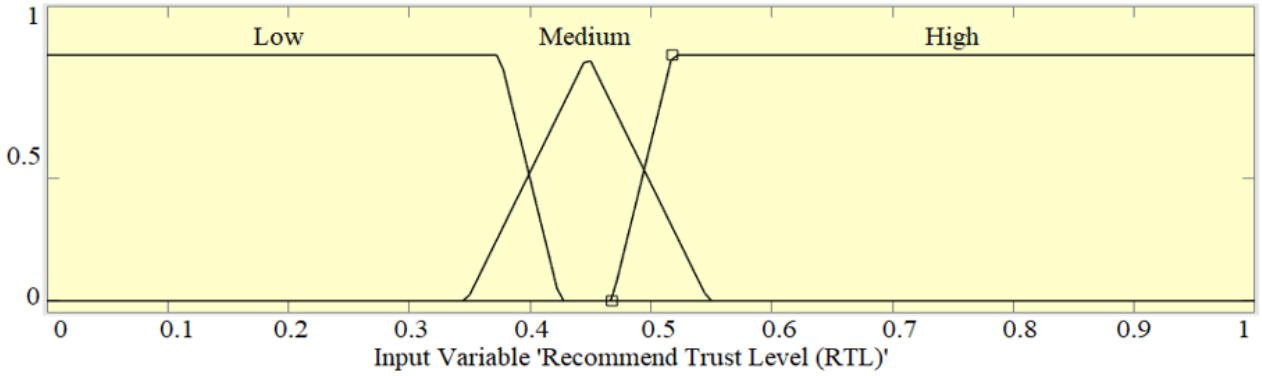


Figure 8

Input fuzzy set membership functions for recommend trust.

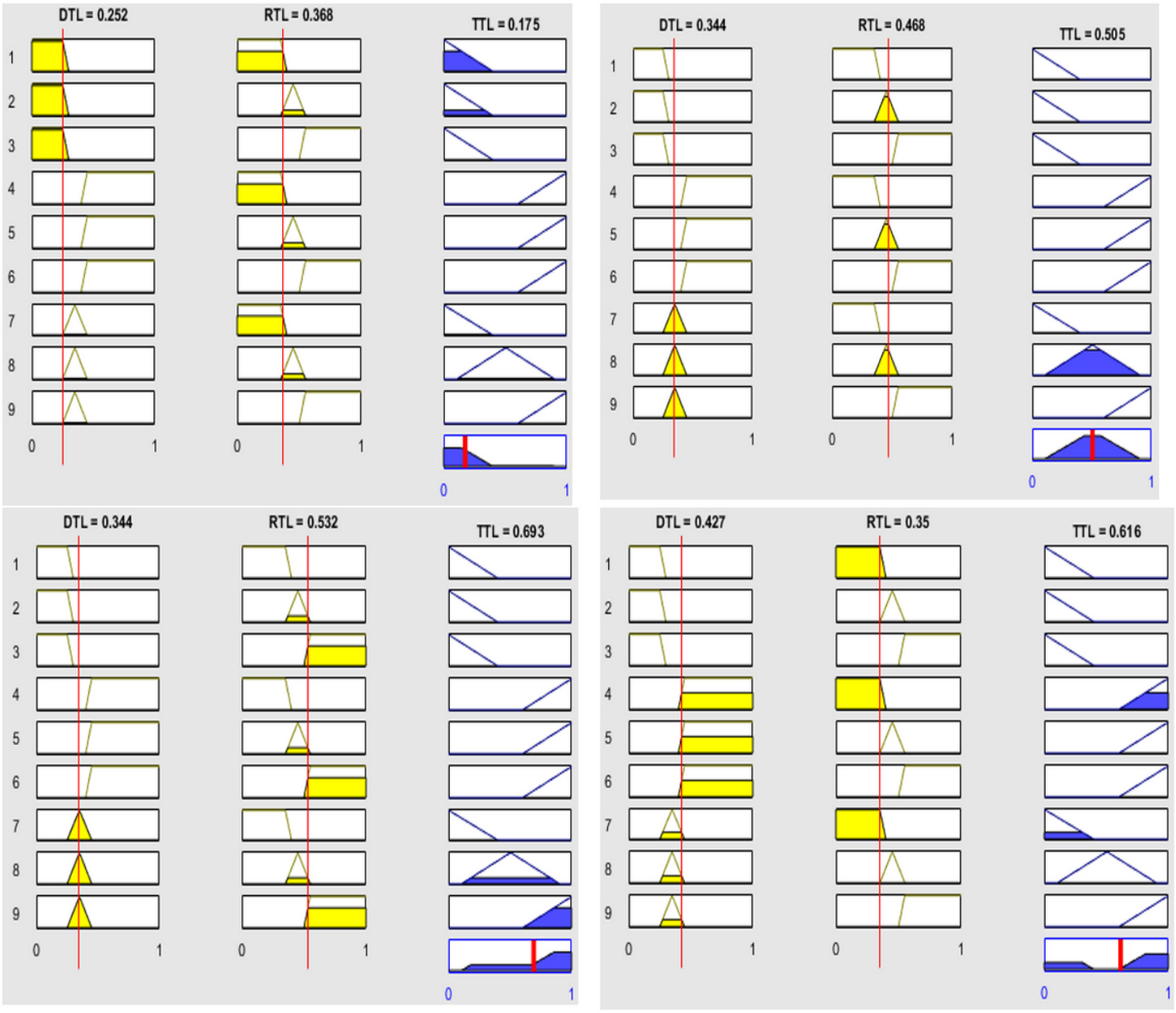
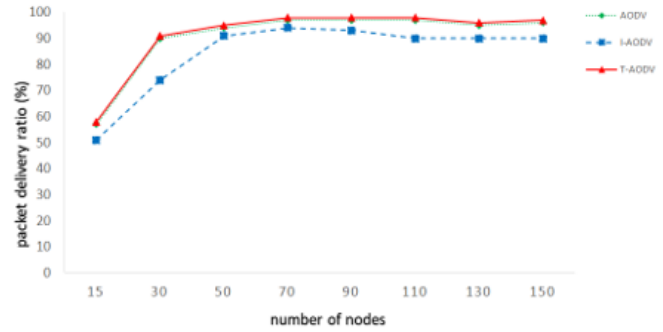
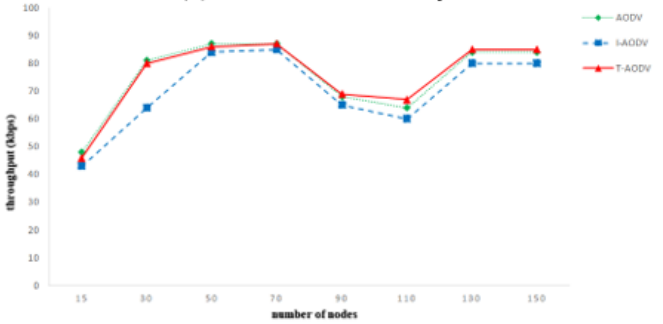


Figure 9

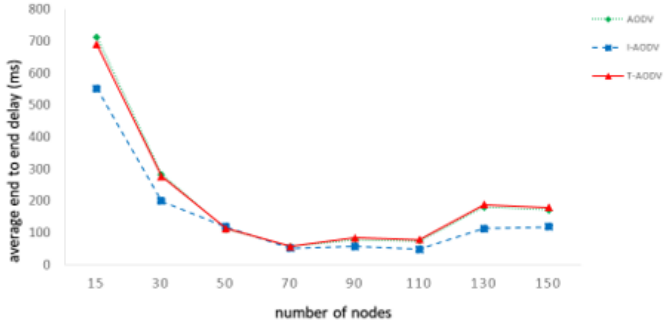
Node trust evaluation process.



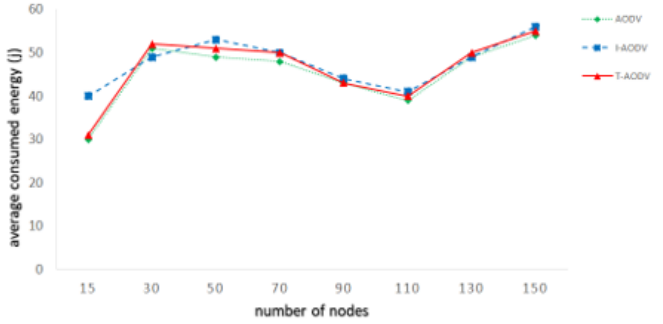
(a) The Packet Delivery Ratio



(b) The Throughput



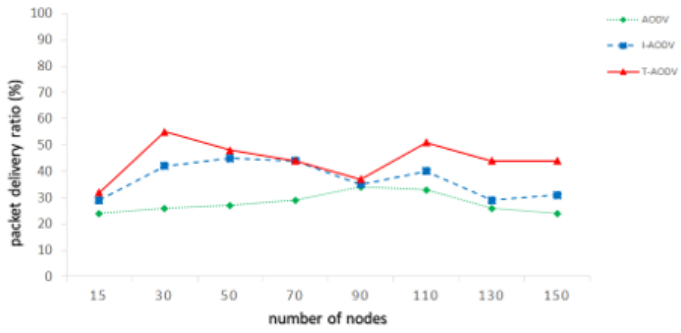
(c) The Average End to End Delay



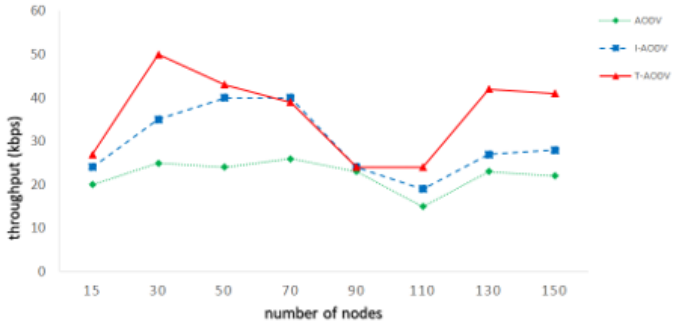
(d) The Average Consumed Energy

Figure 10

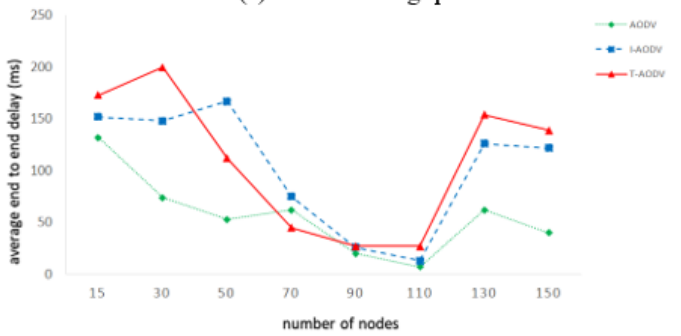
Simulation results in the non-attack situation.



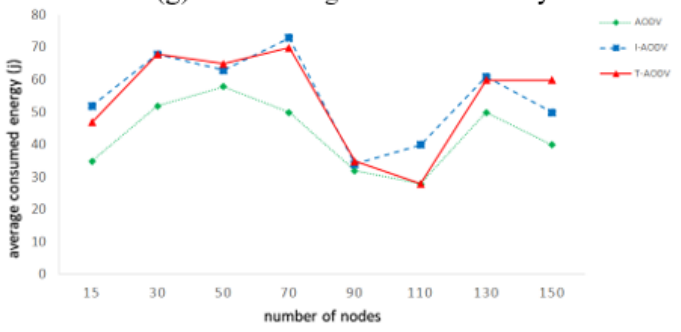
(e) The Packet Delivery Ratio



(f) The Throughput



(g) The Average End to End Delay



(h) The Average Consumed Energy

Figure 11

Simulation results in the black-hole attack situation.