Blockchain-based distributed management system for trust in VANET

Youssef Inedjaren, Mohamed Maachaoui, Besma Zeddini, Jean-Pierre Barbot

Version of Record: https://www.sciencedirect.com/science/article/pii/S221420962100019X
Manuscript_3fdb6557eba6c682455070f50657e931

Blockchain-based Distributed Management System for Trust in VANET

Youssef INEDJAREN[a], Mohamed MAACHAOUI[a], Besma ZEDDINI[b] and Jean Pierre BARBOT[c,**]

[a]*Quartz Laboratory, CY tech*
[b]*SATIE, UMR CNRS 8029, ENS Paris Saclay*
[c]*LS2N UMR CNRS 6004, ENSEA*

ARTICLE INFO

Keywords:
Blockchain
Trust management
Vehicular Adhoc network (VANET)
Fuzzy logic
Optimized link state routing protocol (OLSR)

ABSTRACT

Blockchain technology is gaining a lot of ground as a research topic lately. Wireless ad hoc network researchers are studying and applying blockchain to solve security and reliability issues. Blockchain is a distributed database maintained by multiple nodes in the network, and it is used as a solution to trust and security issues. Within a vehicular ad hoc network (VANET), vehicles provide mutual road safety by generating and broadcasting messages. However, due to the lack of trust in these networks, the reliability of the messages exchanged is questionable. To alleviate this problem, reputation systems have been proposed. Howbeit, these systems require trust and rewards management. Due to the characteristics of VANET, most safety systems require repetitive processes that have a direct impact on performance (resources). The proposed system provides all vehicles in the network with a distributed, highly secure and tamper-proof common framework for routing in VANETs using the Blockchain. In order to incorporate the Blockchain into the VANETs, we use the Optimized Link State Routing (OLSR) as a characteristic protocol. The OLSR is a routing protocol that presents several security concerns because its routing mechanism is based on the availability of a small group of nodes called Multi-point Relay (MPR), and the security mechanisms are executed at each node individually with repetitive processes to be performed. In our contribution, we use blockchain, as a reliable and highly secure technology, to solve OLSR security issues, motivating (rewarding) vehicles to collaborate and avoiding repetitive detection processes. The simulation shows that our system is very efficient to be used in environments with limited resources like VANET. Detection time and detection overhead are reduced, as isolation of malicious nodes increases the efficiency of the detection process.

1. Introduction

With the growing number of vehicles equipped with wireless communication technologies and on-board sensors, VANET is becoming a promising area of research. Due to the rapid changes in topology and the high mobility of vehicular nodes, VANET is a sub-case of Mobile Ad Hoc Networks (MANET).

Vehicles in VANET are self-organizing devices that do not rely on centralized management or infrastructure. Cooperation between vehicles can be seen as the solution to ensure decentralization towards the autonomy of the decision-making process of the vehicle, relying on communication information to complete its partial perception of the environment. In order to achieve communication between all these actors, it is necessary that these different systems interoperate with each other in the absence of a standardization of the communication protocol, both between vehicles (Vehicle-to-Vehicle) but also with infrastructure units (Vehicle-to-Infrastructure / Infrastructure-to-Vehicle). Therefore, each vehicle must maintain a local routing table, which defines the next hop to all destinations, this table is managed by a routing protocol.

Besides the benefits that can be gained from adopting VANET, there are also many security challenges that VANET faces. In a VANET infrastructure, important messages are transmitted and exchanged between vehicles. Since this information can save lives, it must be received on time and with a high rate of dissemination to the entities concerned. These requirements must be taken into account to secure communications in vehicular environments. In addition, securing network communication protocols should be the priority, as a vulnerability in the communication protocol will jeopardize the security of the information exchanged in the VANET. Moreover, to secure the communication

ORCID(s):

Table 1
Example of Attacks in VANETs

Violated Security Requirement	Attack	Solution
Authentication	Sybil Attack	Verification of the position of neighboring nodes [1], VANET PKI [2]
	Eavesdropping	Strong encryption of messages for user communication
	Impersonation attack	Use variable MAC and IP addresses for V-to-V and V-to-I communications [3], Authenticate via digital certificates [3]
	Spoofing attack	Multi-antenna system with known motions [4], Secure verification in the region [5]
Availability	Jamming attacks	Assign IP addresses to the vehicles and delete duplicate IP addresses when forwarding the message[6], DJAVAN[7]
	MITM (man in the middle) attacks	Strong cryptographic techniques [8]
	Black hole attack	Watchdog mechanism [9], Trust model based on weights [10]

between the VANET entities, multiple security requirements must be guaranteed, in order to avoid cyber attacks(see table 1):

Availability: VANET entities and applications require a high level of availability for data and services, and require that at all time, authorized entities should never be denied access to requisite services.

Authentication: Authentication guarantees to the recipient vehicle that the message is sent by a correctly identified sender. Asymmetric key cryptography is used to correlate the identity of the sender with the message sent.

However, each of the existing solutions (see table 1) has some vulnerabilities. In order to address this issue and achieve our system goals of authentication and availability, it is essential to provide a new, robust trust scheme in VANET.

In the literature, the most proposed systems are more compatible with MANETs than with VANETs, with high mobility. In addition, although existing works has presented approaches based on distributed processing, centralizing the management of trust and resource consumption in VANETs remain a serious problem to be solved. For example, when Road Side Units (RSUs) maintain a trusted blockchain updated collaboratively, the management of the blockchain is performed relatively centrally, by RSUs, who always remain the target of attackers. In some proposals, even if the use of the distributed blockchain has helped to ensure security, the computation and communication costs are however relatively high, given the nature of VANETs which are resource constrained environments.

We introduced the FT-OLSR (Fuzzy Logic Trusted - Optimized Link State Routing) [11] protocol to detect malicious vehicles in a VANET environment, but the problem is that repetitive attacks. When an attacker attacks a vehicle and is detected for the first time, he can target another vehicle and that second victim has to do the whole detection process from scratch with all the complexity of the calculation, knowing that we are in an environment of constrained resources, this is a real problem.

A trust management system in a VANET network allows vehicles to differentiate between trusted and malicious messages, and on that basis it provides a vehicle reward or sanction system [12]. Usually, the trust value of a vehicle can be calculated indirectly, based on exchanges with its neighbors. There are two families of trust management systems, centralized and decentralized. In centralized trust management systems [13] [14], all evaluation processing and storage is done in a central server, which is not practical in the case of VANETs, of which almost all applications are in real time, and Information must be received on time and with a high delivery rate in the entities concerned. In decentralized systems [15] [16], the evaluation of neighbors is done mutually, and the processing of evaluations is done locally at the vehicle level. This reduces the overhead due to exchanges with the infrastructure. However, due to the high mobility in VANET, the connection time between vehicles is limited, therefore, the information exchanged is limited. In addition, in an environment with limited resources such as VANET, it is not always easy to credibly assess all the vehicles encountered. Therefore, how to manage trust in VANETs is an issue that needs to be dealt with very rigorously.

As a summarized introduction to blockchain technology, several transactions are performed between network users, these transactions are grouped into blocks. Each block is validated by network nodes called "miners", using techniques that depend on the type of blockchain. In the Bitcoin blockchain, this technique is called “proof of work”. The blocks are linked by cryptographic mechanisms making modification of transaction history by an attacker highly unlikely. Once the block has been validated by the miners, chained in the chain, it is no longer possible to modify its content, because the addition of new blocks will depend on the validity of all the hash functions of the existing blocks. The hash values are generated based on the hash of the previous block.

In this article, we have proposed a blockchain and fuzzy logic based trusted routing scheme that improves node security in VANET. Our approach is based on the use of the Blockchain, as a distributed, coherent and tamper-proof system, to isolate malicious vehicles. Our contribution is based on the use of Blockchain to build an effective trust management system. Blockchain has also been used in other related fields such as wireless networks [17], crowdsourcing [18] and cloud computing [19], etc. In order to benefit from the distributed nature of blockchain, managing trust in VANETs is an issue that must be addressed given the limited resources of the environment. For example, the Proof of Work (POW) consensus algorithm that validates transactions at the node level with high computational complexity and long commit time, is not suitable for a VANET environment with limited resources. Thus, we introduce the Proof-of-Trust (PoT) consensus algorithm for distributed, highly dynamic and constrained resource environments.

Additionally, we focus on the network layer of a VANET, assessing the trust of a node based on its routing performance. To implement the Blockchain, we have chosen the OLSR [20] as a proactive protocol that maintains information from the neighbor. Our proposal is a decentralized blockchain-based trust management system. This system is based on the FT-OLSR protocol [11], which uses the routing messages exchanged (HELLO, Traffic Control (TC)) in VANET, to calculate the trust values, then detect the black hole vehicles. In our system, after identifying a malicious vehicle, it is isolated from communication by sharing this information securely over the network using blockchain. Due to the limited resources of VANETs, the Proof-of-Stake (PoS) model is inserted into the FT-OLSR, instead of using proof of work. In the proposed diagram, the stake of the PoS corresponds to the trust value of each vehicle. The POS consensus algorithm is used to elect validators. Once an attacker is detected, the transaction is validated, counting the vehicles voting for a transaction, then the validator can generate and broadcast an encrypted block containing the attacker’s information. Therefore, all vehicles in the network will add the block to their local blockchains. Additionally, due to the collaboration between nodes to perform the discovery process that this paper presents, reducing bandwidth and power consumption is a priority. The majority of the security work offered in OLSR, including FT-OLSR, pushes nodes to perform complicated operations given the frequent topology changes that are periodically exchanged, resulting in unnecessary bandwidth and power consumption.

The rest of the article is organized as follows: In Section 2, we cover basic information and related work. In the third section, we present the proposed scheme, where we discuss the implementation of the Blockchain, from generation to reception of the block and the local chaining at the vehicle level. We have also described the block validation step, where the PoT consensus algorithm is built into OLSR and used as a suitable mechanism for VANETs. In Section 4, we illustrate the simulation environment and discuss the results, and assess how our contributions can help vehicles work together to reduce detection times and energy consumption. In section 5, we conclude the article.

2. Background and Related Work

2.1. OLSR Protocol

OLSR is a proactive routing protocol for VANETs. The routing process in OLSR is based on a group of nodes called Multi-Point Relay (MPR), which are the nodes that cover the maximum number of two-hop neighbors, to reduce control message overhead. With these central nodes, a node can reach all its neighbors, whether it is to exchange control or data messages, with the minimum possible of transmitted messages, and without duplication.

In a network with OLSR nodes, topology information is exchanged periodically using two types of control messages, namely HELLO (see figure 1) and TC (see figure 2). Each node includes information from neighboring nodes in a HELLO message and broadcasts it to 1 hop neighbors. By collecting the information exchanged in the HELLO messages, each node acquires the topology of the network up to the two-hop neighborhood. TC messages are broadcast by the MPRs, in order to announce the nodes which have elected the MPR nodes. By using the HELLO and TC messages, each node gains a larger view of the network topology.

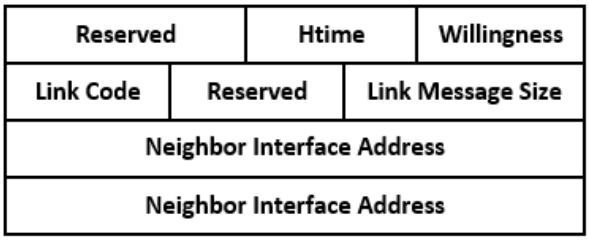


Figure 1: HELLO message (RFC 3626-OLSR)

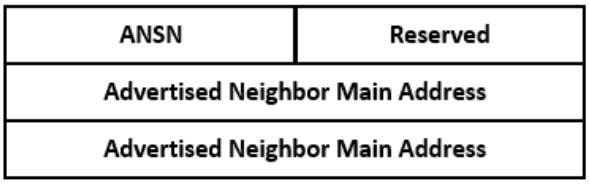


Figure 2: TC message (RFC 3626-OLSR)

2.2. FT-OLSR: Fuzzy Logic based Trusted OLSR

FT-OLSR is a secured routing protocol that we proposed in a previous work [11]. The detection of blackhole nodes in FT-OLSR is done by checking the different communication links and detects the nodes that drop the HELLO and TC messages. Once the black hole node is detected, messages received from that node are ignored and not processed, and subsequently these nodes can no longer be elected as MPRs.

FT-OLSR is based on the fuzzy logic technique [21]. As we are dealing with the cyber-security aspect, this means that we need more precision in calculating trust. Therefore, we choose to use a fuzzy logic approach for the calculation of the trust level. In fact, thanks to fuzzy logic, we can have the following properties:

- Fuzzy logic describes a system as a combination of two approaches: a numerical approach and a symbolic approach.
- Fuzzy algorithms are robust, insofar as they are not sensitive to changing environments and erroneous or forgotten rules.
- The reasoning process is simple, compared to other systems, then computing power is saved, which is important especially in real time systems.
- Fuzzy methods have a shorter development time than conventional methods.

The FT-OLSR consists of three modules which are: fuzzy-based parameter extraction, fuzzy inference module and fuzzy decision module.

Throughout the first module, the FT-OLSR obtains the necessary parameters for analysis from the network traffic, then inserts them into the fuzzy inference module. In the fuzzy inference module, these parameters are used to calculate the trust value of the vehicles, applying fuzzy rules and membership functions, then the calculated trust value is used to check the reliability of the vehicle in the fuzzy decision module. If the trust value is greater than the threshold trust value, the vehicle is reliable, otherwise the behavior of the vehicle is suspicious.

2.3. Trust management in VANETs

As the VANET provides critical road safety applications, and important messages that may contain vital information are transmitted and exchanged between different vehicles and nearby RSUs, security of VANETs is an emerging issue. These systems are based on vehicular communications which inherit the traditional security problems associated with wireless networks. There are several types of attacks targeting VANETs, according to [22], these attacks

primarily target security requirements: availability, authentication, confidentiality and integrity. To face these threats by securing the physical entities and the communications between them, and to guarantee the security requirements mentioned above, the establishment of trust between these entities is very important. A model is proposed in [23] with a trust-based communication model that is based on individual experience rather than a third party advocating trust levels. The model introduces the notion of trust and provides a dynamic measure of reliability and trustworthiness. Another proposition in [24], where the authors establish a distributed trust level, as a measure of trust in the warning message system, then define the trust and present the reasons that require the trust. Attackers may target exchanged messages (data or control) in a VANET, to interrupt the routing process.

Furthermore, our system is based on the OLSR protocol, which is frequently the subject of discussion and research, due to its security vulnerabilities in terms of exchange of control messages. The authors of [25] proposed a secure version of OLSR, based on the exchange of acknowledgments between 2-hop neighbors, when control traffic is successfully received. Additionally, in [26], the authors presented a new approach to TOLSR trust management, to deal with node isolation attack. In this approach, each node observes the behaviors of its 1-hop neighbors as a function of energy, bandwidth, and location.

In addition, our proposed scheme uses fuzzy logic to calculate the trust value. In the literature, several recent researches on VANET security use fuzzy logic. The authors of [27] integrate the trust and certification authority, using a fuzzy-based analyzer, to deal with malicious nodes. Several researchers have combined fuzzy logic and the OLSR protocol, to guarantee better security. In [28], the authors presented an MPR selection algorithm based on fuzzy logic (FLMPR), in order to improve network performance. This proposal focuses on the optimization of the MPR selection process, based on QoS (Quality of Service) metric such as node energy, node mobility and node coverage. However, these proposed systems are more compatible with MANETs than with VANETs, with high mobility. Additionally, although this work has presented approaches based on distributed processing, centralizing the management of trust and resource consumption in VANETs remain serious problems to be solved.

2.4. Blockchain-Based trust management

Blockchain is a distributed system for performing digital transactions whose authenticity cannot be questioned. These transactions can be carried out without recourse to a trusted third party. The first blockchain appeared in 2008 with the digital currency Bitcoin [29]. Due to its high security and decentralized control, it has been used with different cryptocurrencies.

The use of blockchain in various technological fields other than digital currency is arousing the interest of researchers (companies, governments, etc.). Blockchain-related researches on trust management to improve the security of VANETs have recently been published.

In [30], a blockchain-based and trust-based learning scheme has been proposed. In this work, routing information was stored in the blockchain to protect it from tampering and traceability. Reinforcement learning is integrated to improve routing. Validators are defined, which validate the blockchain using Proof of Authority (POA), instead of Proof of Work (POW) to optimize resource consumption, which make routing information traceable. However, since all central tasks are performed at the validator node level, this runs counter our goal of eliminating centralized management, so this system seems inappropriate for decentralized VANETs.

In [31], the authors propose an authentication scheme based on the blockchain and preserving confidentiality in the VANETs. They used a private and public blockchain for authentication and handling of event messages, respectively. The Trusted Authority (TA) is responsible for performing the transactions which are the identity information needed to authenticate a vehicle once it joins the VANET, in the private blockchain. The public blockchain is responsible for ensuring the security of the distribution of messages, it takes the place of an RSU in a vehicular network. In this article, even if the use of the distributed blockchain has helped to ensure security, however, the computation and communication costs are relatively high, given the nature of VANETs which are environments of resource constraints.

In [32], a blockchain-based trust management model, combined with a confidentiality-preserving conditional announcement system (BTCPS) for VANETs is proposed. The authors proposed a protocol to ensure vehicle confidentiality when exchanging messages. Then, in order to ensure the reliability and synchronization of messages, a blockchain-based trust management model is proposed. Message reliability is determined by RSUs based on reputation values stored in the blockchain. In this work, the POW consensus algorithm is used, combined with the practical Byzantine fault tolerance algorithm. although the management system is distributed, the management of the blockchain is done centrally, by certain predefined trusted nodes.

In [33], the authors proposed a secure trust-based blockchain architecture to increase security and privacy to mit-

igate the aforementioned MAC layer attacks. The block chain technology of the proposed solution uses time stamps and hashing techniques to maintain the freshness of delivered messages. These techniques minimize message fabrication or modification attacks because time stamps record the time a message is delivered, while hashing secures the message from tampering by malicious nodes. In addition, the proposed solution also uses a message assessment and credibility approach which ensures the management of trust between vehicles when exchanging information in VANET. Any vehicle that communicates false messages to other vehicles in the network will be assigned low values, which will decrease its credibility. Vehicles with a confidence value below the threshold value will be rejected from the network and their vehicle certificates will be revoked. The solution proposed in this work is efficient and it uses the same philosophy as our proposed system, but in our proposal we use a more precise trust management system based on fuzzy logic and we target routing in the network layer.

In [34], a decentralized trust management system in vehicular networks based on blockchain techniques was introduced. In this system, the blockchain is maintained at the RSU level, and validation is done by combining the two consensus mechanisms POW and proof of stake (POS). Based on the evaluations performed by the vehicles on each other, the RSUs calculate the trust value offsets of the affected vehicles and aggregate this data into a "block". Then each RSU will try to add their "blocks" to the blockchain. Since all RSUs maintain a collaboratively updated trust blockchain, management of the blockchain is done relatively centrally, by RSUs, who always remain the target of attackers.

3. Proposed Solution

3.1. Design Objectives

The design of a reliable blockchain-based system for detecting and isolating misbehaving vehicles in vehicle networks is expected to achieve the following goals:

Distributed management: The assessment of vehicle trust must be done in a distributed and decentralized manner, i.e. the calculation and evaluation of the trust values must be done at the vehicle level and in a mutual manner.

Reliability and Availability Requirements: The applications used in VANETs are real-time, so no reception delays are allowed and the delivery rate must be high. Therefore, each vehicle must have a trust table for evaluating neighboring vehicles, in order to be able to select the optimal vehicles for data transfer.

Security and Privacy: The more information are exchanged on the network, the more vulnerable users information are, and the possibility of its exploitation by attackers is higher. In addition, when there is no cooperation between VANET components, the attacker can repeatedly target different vehicles. As a result, trust exigencies should be taken into account in protocols for VANET.

Scalability: difficulties in management and the problems related to the limited bandwidth. Nevertheless, for VANETs as a resource constrained environment, it is better to use a simple method with a certain level of security, than a more secure method but requires complicated mechanisms and consume more resources.

3.2. Blockchain-Based FT-OLSR

FT-OLSR is a routing protocol that improves the security of communications in the VANET. After performing a risk analysis, our target is the black hole attack which is one of the most dangerous attacks. The black hole detection process in FT-OLSR is performed mutually at the vehicle level, by verifying communication links and detecting vehicles that drop HELLO and TC messages. Once the black hole node is detected, messages received from that node are ignored and not processed, and subsequently these nodes can no longer be elected as MPRs.

With the aforementioned goals in mind, we used Blockchain technology to isolate malicious vehicles detected by FT-OLSR and eliminate complicated calculations by improving cooperation between VANET components in a dynamic environment with limited resources. Depending on the needs of VANET, the proposed system can be divided into components as shown in figure 3.

3.2.1. Trust value calculation

The FT-OLSR uses the exchanged HELLO and TC control messages to determine the level of reliability of neighboring vehicles. If the trust value of a vehicle is greater than or equal to the trust threshold, that vehicle can be (candidate MPR) selected for packet transmission. To take into account the new modules added, the list of neighbors will be modified to store in addition to neighbor identifiers, the number of messages received from each neighbor as well as its level of trust. These parameters will be updated each time HELLO or TC messages are received. As we

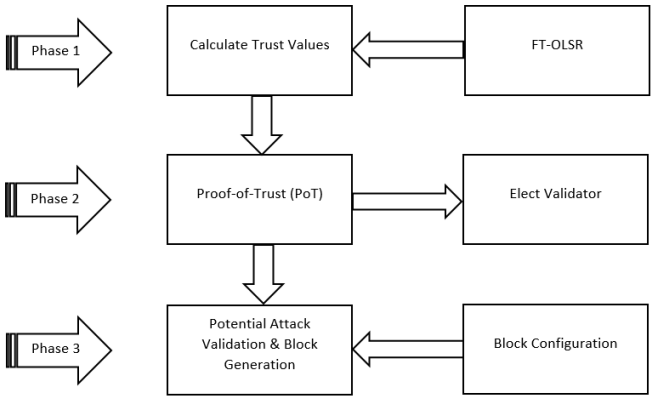
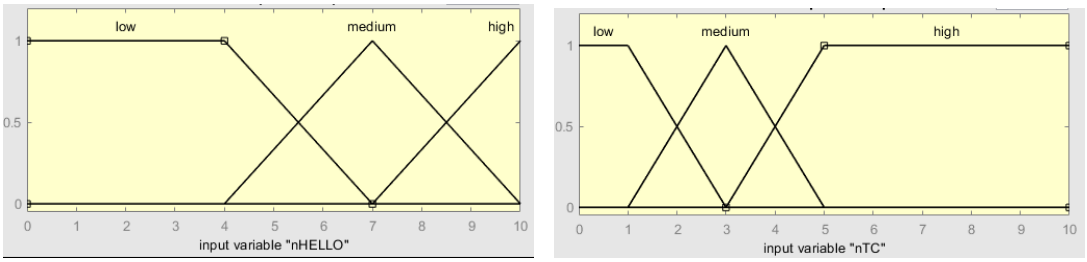


Figure 3: System Design



(a) nHELLO **(b)** nTC

Figure 4: nHELLO and nTC membership functions

mentioned in section two, our proposed detection system is based on fuzzy logic, which consists of three modules which are: fuzzy-based parameter extraction, fuzzy inference module, and fuzzy decision.

Extraction of fuzzy based Parameters

In OLSR, two main control messages are used, HELLO and TC messages. Since these messages make a significant contribution to routing operations, the trust level of each vehicle is derived from the number of HELLO and TC messages exchanged with this one. The malicious vehicles may also generate control packets, however, generation probability is quite low with regard to trustworthy vehicles. The number of control messages generated is linked with the value of trust, by the mathematical function: Trust = F [nHELLO, nTC], with nHELLO and nTC are the number of hello and tc messages generated respectively. In the proposed system, the nHELLO and nTC are the crisp inputs that are passed to the inference engine.

Fuzzy Inference System

Fuzzification process The inference engine uses a rule base to predict reliable vehicles. We propose an inference engine to calculate the trust value, using three levels of membership for each entry: low, medium and high. The numeric values of nHELLO and nTC are converted to fuzzy linguistic variables using the corresponding predefined variables and membership functions, as shown in the Figure 4.

- Input functions

  Illustrated in Table 2 and Figure 4.

- Output functions

  Illustrated in Table 3 and Figure 5.

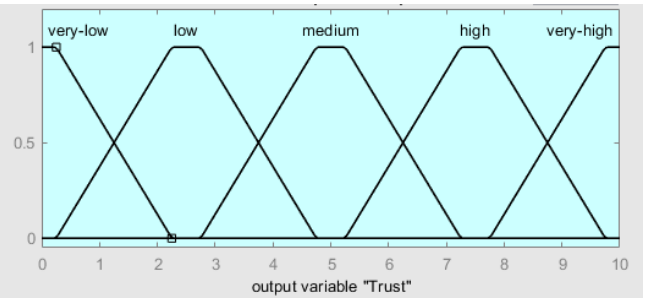


Figure 5: Trust membership function

Table 2
Input membership values

Input	Fuzzy Sets		
nHELLO	Low	Medium	High
nTC	Low	Medium	High

Table 3
Output membership values

Output	Fuzzy Sets				
Membership	(1)	(2)	(3)	(4)	(5)
Trust value	Very low	Low	Medium	High	Very high

Table 4
Fuzzy rules

nHELLO	**nTC**	**Trust**
low	low	very low
low	medium	low
low	high	medium
medium	low	very low
medium	medium	medium
medium	high	high
high	low	low
high	medium	high
high	high	very high

Fuzzy rule base In FT-OLSR, a rule base is created for the fuzzy inference engine. There are 12 rules that are used by the inference engine. The proposed rules are shown in the table 4.

Deffuzification process The FT-OLSR uses a defuzzification process to obtain the crisp values. We use the Weighted Average Method [35] to obtain the below formula to determine the trust value of a vehicle:

$$Trust(x) = \frac{1*VL(x)+3*L(x)+5*M(x)+7*H(x)+10*VH(x)}{VL(x)+L(x)+M(x)+H(x)+VH(x)}$$

With:

VL(x): Very Low membership level.

L(x): low membership level.

M(x): medium membership level.

H(x): high membership level.
VH(x): very high membership level.

Fuzzy Decision Module

In this module, we set the threshold value of trust to 5, to analyze the behavior of a vehicle in our VANET. After several simulations we found that the maximum number of HELLO and TC messages sent by a node is around 10 messages and at the output of our fuzzy system, the maximum value of the trust using the above formula is 10, which is equivalent to the maximum number of HELLO and TC messages sent at the input, this is why we choosed the value 5 as the trust treshold, which represents the value from which the node can be considered as active in the routing process. If the value of trust calculated is greater than the threshold, the vehicle is not a black hole otherwise it is. The Algorithm 1 explains the vehicle-level processing in the FT-OLSR.

The Algorithm 1 explains the vehicle-level processing in the FT-OLSR.

Algorithm 1 Vehicle-level processing FT-OLSR

```
procedure RECV-OLSR
    N Vehicle
    Trust (N) = 5
    for <Each Source Vehicle S> do
        if <S is suspicious> then                    ▷ /*S drops received messages*/
            decrement NHELLO(S) by 5
        end if
        if <HELLO-message> then
            increment NHELLO(S) by 1
        else if TC-message then
            increment NTC(S) by 1
        end if
        if Trust(NHELLO(s), NTC(s)) ≥ 5 then
            Process the message
        else if Trust(NHELLO(s), NTC(s)) ≤ 5 then
            Drop the message
        end if
    end for
end procedure
```

3.2.2. Trust Management method

Based on the fuzzy trust model, the FT-OLSR calls the trust management procedure to verify the trust of the vehicle (reliable or not) and thus make the routing decision. The structure of the FT-OLSR flowchart and the relationships between its components are shown in figure 6.

3.2.3. Consensus Algorithm (Proof-of-Trust)

The trust value is used to determine which vehicles to isolate and then include in the blocks, so that each vehicle in VANET can access information on its local blockchain. Due to the lack of centralized management within the VANET, the consensus process has to be done at the vehicle level in a decentralized manner. Several consensus algorithms exist in the literature, the most commonly used are proof of work (PoW) and proof of stake (PoS). The POW validates transactions by the nodes with the highest compute capacity, which is not suitable for a VANET environment with limited resources. The POS chooses the richest node as the validator, which is not equal even though the PoS algorithm fits well in an environment with limited resources. To avoid the challenges confronting the existing consensus algorithms

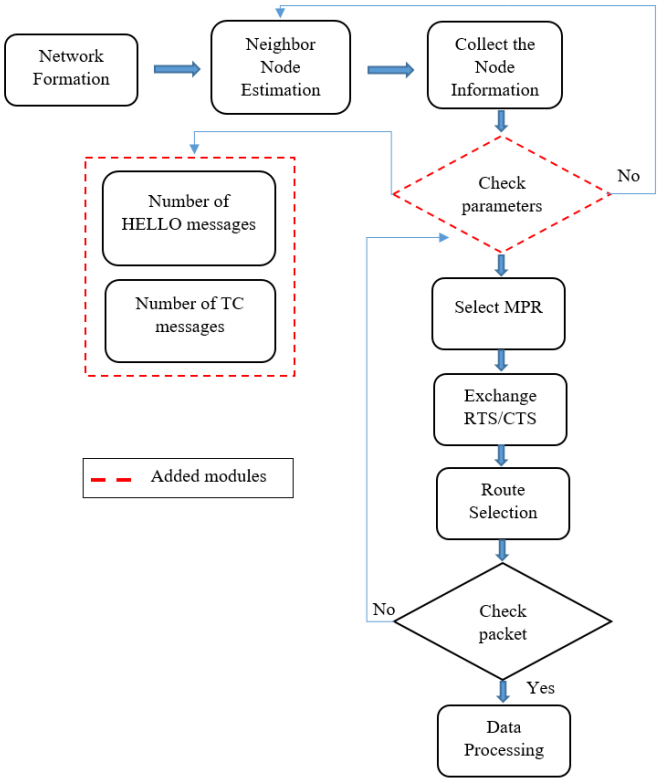


Figure 6: FT-OLSR flow chart

[36], we present the Proof of trust (PoT) consensus algorithm for distributed, highly dynamic and constrained resource environments. c

Validator

In our blockchain, only the node with the highest trust value and is elected by its neighbors as MPR can become the validator. There is a threshold value of 5 in the network that determines whether a specific node is trustworthy enough to become a validator. In our validator electoral strategy, a vehicle cannot pretend to be trustworthy, which means it needs neighbors. If an MPR vehicle has a trust value above the threshold, its neighbors send a complaint message with their private keys. Likewise, each node with its MPR with a trust value greater than the threshold can broadcast a claim message to the entire network by piggybacking it on a HELLO message. If the trust values disseminated by the neighbors of the MPR (who elected it as their MPR) are greater than the threshold and there are no malicious complaints on this vehicle or its neighbors, this vehicle becomes the validator.

Algorithm 2 shows the validator election process in detail.

Block Generation

The exchange of control messages increases the trust values of all vehicles in the VANET. The vehicles with the highest trust values will be elected as validators, and then they will be responsible for generating the blocks. To guarantee authentication, each vehicle will encrypt its transactions using its private key, before distribution via the MPRs.

If a malicious vehicle is detected by FT-OLSR, it will be isolated once and for all from the communication, putting its information in the shared blockchain. The detection process is performed using the potential attacker message, which vehicles send to the validator once they have suffered an attack. However, a vehicle could send a potential attacker message in error, containing information from a reliable vehicle. Therefore, an attack claim transaction must be confirmed by the neighbors before the validator generates a block as a result of this claim. This complaint contains information about the attacker that is reported in a potential attacker message. In addition, a potential attacker message

Algorithm 2 Validator election algorithm

procedure VALIDATOR-ELECTION
  for each vehicle i in the network **do**
    `Broadcast HELLO message to its neighbors`
    `let N1(i) is the set of 1-hop neighbors of i`
    `let N2(i) is the set of 2-hop neighbors of i`
    `Select that 1-hop k from N1(i) that is the only neighbor of some vehicle in N2(i)`
    $Trust(k) \geq 5$
    $MPR(i) = [k]$
    while `<there is a vehicle in N2(i) not covered by MPR(i)>` **do**
      for `<every vehicle in the MPR(i)>` **do**
        `<compute the number of vehicles that each vehicle covers among the uncovered vehicles of N2(i)>`
        `<Add to MPR(i) the vehicle with the maximum number>`
      end for
    end while
  end for
end procedure

Table 5
The new HELLO message

Reserved		Htime	Willingness
Link Code	Reserved	Link Message Size	
Potential Attacker Address			
Neighbor Interface Address			
Neighbor Interface Address			

Table 6
the new TC message

ANSN	Reserved
BLOCK	
Advertised Neighbor Main Address	
Advertised Neighbor Main Address	

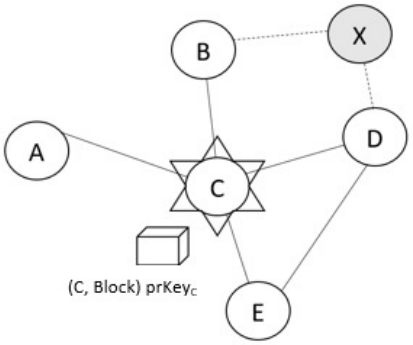
(A, B, PotentialAttackerMessage) $prKey_A$ is sent, where the information of sender A and attacker B are encrypted by the private key of the sender. This message is carried in a HELLO message. It is possible for an attacker to send a potential attacker message in order to isolate a trusted vehicle. To avoid this problem, if the majority of neighboring vehicles included the same vehicle information in their hello, the transaction is validated.

After the validation of a transaction, by counting the vehicles voting for a transaction, the validator will be able to generate and broadcast an encrypted block containing the attacker's information, then all the vehicles in the network will add the block to their local blockchains. The demonstration of this phase is shown in 7.

Table 5 and table 6 illustrate the new hello and tc messages, used to overlap the potential attacker's message and the blocks, respectively.

Block Configuration

In our VANET blockchain, blocks are made up of transaction data which is the attacker's information, the block index, the hash value of the current block and the previous hash. In order to hash a transaction, we will include the attacker's information to ensure non-repudiation so that even a small manipulation of the content of the block changes



Potential Attacker Message	
B	(B, X, hello from X)$prKey_B$
D	(D, X, hello from X)$prKey_D$

Figure 7 & Table 7: Demonstration of block generation phase

the hash value. The hash from the previous block will be built into the block and will be used for chaining, meaning that manipulation of data in any block can disrupt the entire blockchain. As shown in figure 8.

The Algorithm 3 clarifies the vehicle-level processing with the proposed scheme.

Algorithm 3 Vehicle-level processing Blockchain based FT-OLSR

```
procedure RECV-OLSR
    N Vehicle
    Trust (N) = 5
    for <Each Source Vehicle S> do
        <Lookup in the Blockchain to verify if S is an attacker>
        if S − Attacker = True then
            Drop the message
        else
            if <S is suspicious> then                    ▷ /*S drops received messages*/
                decrement NHELLO(S) by 5
            end if
            if <HELLO-message> then
                increment NHELLO(S) by 1
            else if TC-message then
                increment NTC(S) by 1
            end if
            if Trust(NHELLO(s), NTC(s)) ≥ 5 then
                Process the message
            else if Trust(NHELLO(s), NTC(s)) ≤ 5 then
                Include S in a HELLO message as a potential attacker
            end if
        end if
    end for
end procedure
```

4. Performance Evaluation

4.1. Simulation Environment

In this section, the proposed scheme is implemented in Network Simulator 3 (NS3). We used NS3 to evaluate the performance of our system, as VANET simulations require a network simulator that provides the conditions closest to

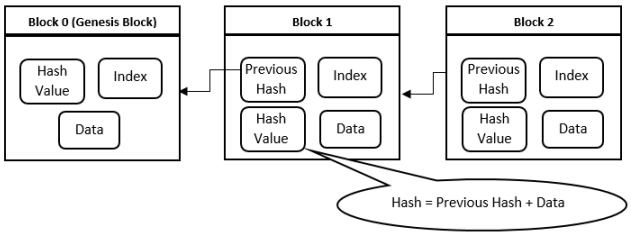


Figure 8: Block configuration

Table 8
Simulation Parameters

Parameters	Values
Simulator	NS-3
Number of nodes	25 mobile nodes
Mobility model	Random Waypoint Mobility Model
Simulation range	1 km * 1 km
Movement speed	3 m/s
Transmission range	250 m
Simulation time	100 s

the real world. The number of nodes involved for the simulation is 25 nodes. The table 8 summarizes the simulation parameters.

The performance evaluation of our system was carried out from both sides namely practical results and theoretical analysis. The theoretical analysis was performed by evaluating the computational complexity of a vehicle when it detects an attacker, to demonstrate the effectiveness of our scheme in reducing network overhead. We used another performance indicator in our theoretical analysis which is block generation latency, to compare the efficiency of our blockchain against other blockchain-based systems. On the other hand, the practical performance of our proposed scheme is evaluated using the detection time to observe the overall vulnerability times in the network by comparing our proposed scheme with FT-OLSR, and the detection rate to clarify the efficiency of our pattern every time we increase the percentage of blackchole nodes.

4.2. Theoretical Analysis

4.2.1. Resources consumption and Overhead

We evaluated the resource consumption by studying the computational complexity that a vehicle uses to detect an attacker (see table 9). According to the FT-OLSR, we assume that the detection process of a malicious vehicle, using Hello, TC messages, and trust computation, requires computational complexity of O(n). In our proposed scheme, the process of detecting a malicious vehicle B for the first time required the same computational complexity O(n). The difference occurs when the same attacker is detected for the second time, when a malicious vehicle B is detected by a victim vehicle for the first time, its information is shared through local blockchains in the network. Therefore, once attacker B targets another victim, the detection process is no longer necessary, so the computational complexity incurred is reduced to O(1). Knowing that the VANET is a resource-constrained environment, our proposed scheme reduced resource consumption by reducing the computational complexity required for rebroadcast attacks from the same attacker. In the table 9 we compared the computational complexity required to detect three malicious nodes (A, B, C) targeting two different victims, using FT-OLSR and the proposed system. As you see in the table, using FT-OLSR, malicious nodes attack two different victims but the complexity of detection remains O(n). Unlike our proposed scheme, where detection for the first time requires O(n), but once attacker A, B or C targets another victim, the complexity of detection is reduced to O(1).

For overhead, TC messages are used in our system to piggyback blocks that are generated after an attacker is detected, and knowing that TC messages are frequently exchanged and propagate more than one hop, this incurs

Table 9
resources consumption

-	A	B	B	C	A	C
FT-OLSR	O(n)	O(n)	O(n)	O(n)	O(n)	O(n)
Proposed scheme	O(n)	O(n)	O(1)	O(n)	O(1)	O(1)

overhead on the additional fields. Since the time taken to detect an attacker equals the time taken required to disseminate a hello message (2 s), and the generated block will be disseminated using a TC message which has an interval of 5 s, from the generation of the potential attacker's message to reception of the block by the vehicles, the process requires at most 7 s after an attack. In every second of the TC interval after an attacker is detected, the overhead will be slightly higher than the FT-OLSR scheme. However, by studying a larger scenario with four attacks for example. At the beginning, two attacks are launched and detected, then two blocks are generated and broadcast through the VANET. As for the computational complexity, the difference occurs when detecting the same attacker for the second time, when a malicious vehicle is detected, its information is shared across the network and no additional detection process is required. Thus, the overhead of our system is reduced for repeated attacks from the same malicious vehicles.

4.2.2. Block Generation time

In order to evaluate the block generation latency, we compared the time it takes to create and dessimnate a block in our proposed scheme, with the Etheureum system where the block generation time is 20 s. In Figure 9, we demonstrate that our proposed system requires much lower time to generate a block. To speed up the isolation process, hello messages are used to piggyback potential attack messages, and TC messages are used as a carrier in order to disseminate the blocks through the network. For potential attacker messages, the detector vehicle includes the attacker's address piggybacked in the Hello so he can send it to its MPR. As illustrated in the figure 8, the field Reserved is normally used for future extensions, in our case we used it to point out if the hello message contains attacker information or not. When the detector vehicle includes a potential attacker message in the hello message, we assign to Reserved the value 1. Once the MPR receives a Hello with reserved set to 1, it validates this request, acknowledging that it contains potential attacker information, by updating the number of potential attacker messages received from neighbors containing this same attacker information. Thus, the time required to validate a potential attacker message is equivalent to the time needed to disseminate a hello message (2 s). Moreover, once the MPR vehicle collects the same attacker information from at least half of its neighbors, a block will be generated and disseminated via TC messages in the next TC interval, with ''Reserved = 1" to indicate that a Block is included in the TC. Therefore, from potential attacker message generation to the block reception by vehicles in the network, the process necessitate at most 7 s (2s hello, and 5s TC). Depending on the detection time, the time required could be lower in the case of the victim vehicle being the validator (MPR), or higher than 7 s.

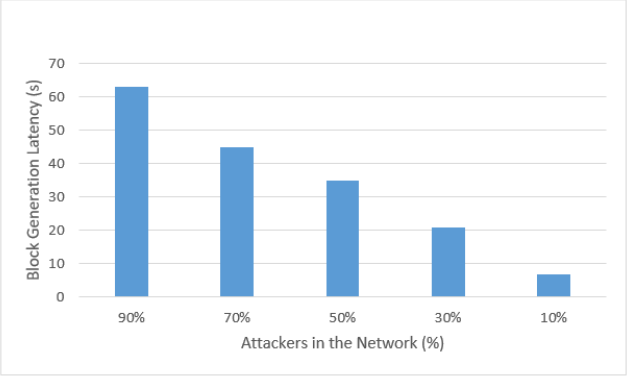


Figure 9: Block Generation Latency

4.3. Simulation Results

4.3.1. Detection time

In this experiment, we compared the detection time using the proposed system with that using FT-OLSR. Figure 10 shows the time taken to isolate attackers from communicating with other vehicles relative to the percentage of attackers in the VANET. According to [37], if there are 2 inputs, 3 fuzzy sets for each input, and 10 levels of discretization of the discourse universe, then the number of operations used for our fuzzy logic system is estimated to be around 9127. If it is assumed that our FT-OLSR is implemented in hardware with a CPU in clocks of 700 MHz and that the execution of an instruction takes an average of 10 clocks, then an inference takes about 0,13 ms.

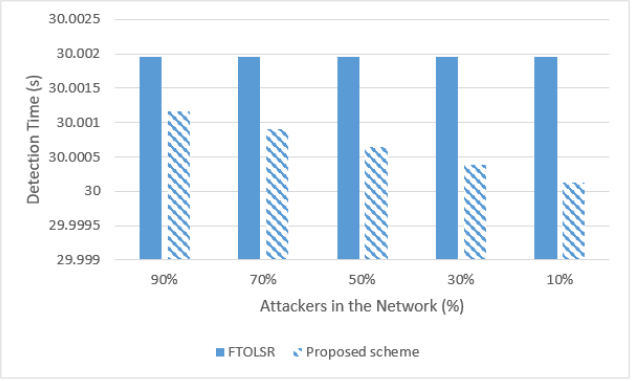


Figure 10: detection time

In our simulation, the network contains 25 nodes including 10 potential attackers. In our proposed system, when an attacker is detected by a victim vehicle, its information is shared via the local blockchains in the network, and a repeated detection process by the nodes is no more needed. Thus, once the attacker targets another victim, it already has the attacker information in its local blockchain, so the detection time is reduced. Contrairement of nodes using FT-OLSR where they are oblige to repeat the detection process every time, even if the attacker is already detected. Therefore, the overall detection time in a VANET with the proposed scheme is reduced, as the percentage of the malicious nodes decreases.

4.3.2. Detection rate

The objective of our proposal is to detect and isolate Blackhole nodes. In this simulation, we evaluate the detection rate of our scheme, with 0% and 50% of the nodes as attackers. In figure 11, we have presented the detection rate performed using the Blockchain-based FT-OLSR. We have illustrated the trust levels of the nodes projected onto a circle surrounded by numbers denoting the identity of the node and the numbers from 1 to 10 which are shown vertically as the trust values. The node with a trust value less than or equal to 5 will be considered malicious. On the other hand, nodes with trust values greater than 5 will be considered reliable. Furthermore, we take from the figure 11 that the detection rate of our diagram increases proportionally with the increase in the number of attackers. At the end of the simulation, the proposed scheme detects and isolates 90% of the black hole nodes. Thus, we have extended the simulation time, in order to observe the behavior changes of the nodes in a larger window. Consequently all the nodes increase their trust value, except the Blackhole nodes which are isolated from the communication once and for all, as you can see in figure 11.

5. Conclusion

In this article, we have proposed a blockchain and fuzzy logic based trusted routing scheme to improve detection of malicious nodes in VANET. Our approach is based on the use of Blockchain to isolate vehicles detected using FT-OLSR, communication. The results of the simulation showed that the distribution of processing at the node level is an effective way to better secure the network, since each node has a local chain containing the attackers. Even though the overhead is a little higher compared to other systems, due to the collaboration between nodes to generate and share the blockchain, but the overall detection time and complexity are reduced. In addition, by using the Blockchain to

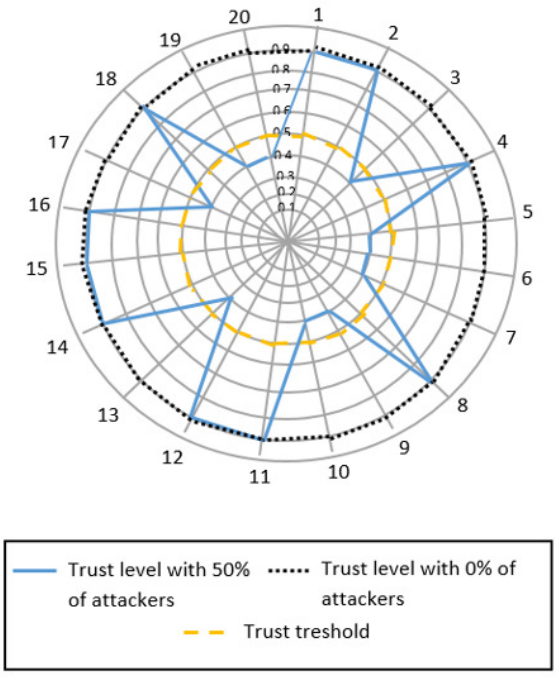


Figure 11: Detection rate

decentralize the computation, VANETs can guarantee all security requirements. As future work proceeds, we will focus on blockchain revocation, when an attacker changes their attitude from malicious to trustworthy or the opposite.

References

[1] T. Leinmüller, C. Maihöfer, E. Schoch, F. Kargl, Improved security in geographic ad hoc routing through autonomous position verification, in: Proceedings of the 3rd international workshop on Vehicular ad hoc networks, ACM, 2006, pp. 57–66.

[2] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, IEEE wireless communications 13 (2006) 8–15.

[3] M. S. Al-Kahtani, Survey on security attacks in vehicular ad hoc networks (vanets), in: 2012 6th International Conference on Signal Processing and Communication Systems, IEEE, 2012, pp. 1–9.

[4] P. Y. Montgomery, Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer, in: Radionavigation Laboratory Conference Proceedings, 2011.

[5] J.-H. Song, V. W. Wong, V. C. Leung, Secure location verification for vehicular ad-hoc networks, in: IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, IEEE, 2008, pp. 1–5.

[6] A. T. Nguyen, L. Mokdad, J. Ben Othman, Solution of detecting jamming attacks in vehicle ad hoc networks, in: Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems, ACM, 2013, pp. 405–410.

[7] L. Mokdad, J. Ben-Othman, A. T. Nguyen, Djavan: Detecting jamming attacks in vehicle ad hoc networks, Performance Evaluation 87 (2015) 47–59.

[8] A. Daeinabi, A. G. Rahbar, Detection of malicious vehicles (dmv) through monitoring in vehicular ad-hoc networks, Multimedia tools and applications 66 (2013) 325–338.

[9] X. Yao, X. Zhang, H. Ning, P. Li, Using trust model to ensure reliable data acquisition in vanets, Ad Hoc Networks 55 (2017) 107–118.

[10] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, A. Iyer, Flooding-resilient broadcast authentication for vanets, in: Proceedings of the 17th annual international conference on Mobile computing and networking, ACM, 2011, pp. 193–204.

[11] Y. Inedjaren, B. Zeddini, M. Maachaoui, J.-P. Barbot, Securing intelligent communications on the vehicular adhoc networks using fuzzy logic based trust olsr, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), IEEE, 2019, pp. 1–6.

[12] S. Li, X. Wang, Quickest attack detection in multi-agent reputation systems, IEEE Journal of Selected Topics in Signal Processing 8 (2014) 653–666.

[13] C. Lai, K. Zhang, N. Cheng, H. Li, X. Shen, Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets, IEEE Transactions on Intelligent Transportation Systems 18 (2016) 1559–1574.

[14] M. E. Mahmoud, X. Shen, An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks, IEEE Transactions on Vehicular Technology 60 (2011) 3947–3962.

[15] X. Huang, R. Yu, J. Kang, Y. Zhang, Distributed reputation management for secure and efficient vehicular edge computing and networks, IEEE Access 5 (2017) 25408–25420.
[16] S. Gurung, D. Lin, A. Squicciarini, E. Bertino, Information-oriented trustworthiness evaluation in vehicular ad-hoc networks, in: International Conference on Network and System Security, Springer, 2013, pp. 94–108.
[17] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5g beyond, IEEE Network 33 (2019) 10–17.
[18] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, R. H. Deng, Crowdbc: A blockchain-based decentralized framework for crowdsourcing, IEEE Transactions on Parallel and Distributed Systems 30 (2018) 1251–1266.
[19] P. K. Sharma, M.-Y. Chen, J. H. Park, A software defined fog node based distributed blockchain cloud architecture for iot, Ieee Access 6 (2017) 115–124.
[20] T. Clausen, P. Jacquet, Rfc3626: Optimized link state routing protocol (olsr), 2003.
[21] T. J. Ross, Fuzzy logic with engineering applications, John Wiley & Sons, 2005.
[22] M. N. Mejri, J. Ben-Othman, M. Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Vehicular Communications 1 (2014) 53–66.
[23] A. A. Pirzada, C. McDonald, Establishing trust in pure ad-hoc networks, in: Proceedings of the 27th Australasian conference on Computer science-Volume 26, Australian Computer Society, Inc., 2004, pp. 47–54.
[24] M. Mejia, R. Chaparro-Vargas, Distributed trust and reputation mechanisms for vehicular ad-hoc networks, in: Vehicular Technologies-Deployment and Applications, IntechOpen, 2013.
[25] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, Sa-olsr: Security aware optimized link state routing for mobile ad hoc networks, in: 2008 IEEE International Conference on Communications, IEEE, 2008, pp. 1464–1468.
[26] D. Bharathi, S. Behera, Extenuate the dos attacks in olsr protocol using novel trust management method, IJEDR (2017).
[27] V. Manoj, M. Aaqib, N. Raghavendiran, R. Vijayan, A novel security framework using trust and fuzzy logic in manet, International Journal of Distributed and Parallel Systems 3 (2012) 284.
[28] N. Dhanalakshmi, C. Sathya, G. K. Sri, K. Suresh, Multi-constraint fuzzy logic based optimal mpr selection in olsr, Advances in Natural and Applied Sciences 11 (2017) 317–322.
[29] S. Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system, Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf 4 (2008).
[30] J. Yang, S. He, Y. Xu, L. Chen, J. Ren, A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks, Sensors 19 (2019) 970.
[31] B. Guehguih, H. Lu, Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet, in: Proceedings of the 2019 5th International Conference on Systems, Control and Communications, 2019, pp. 16–21.
[32] X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets, IEEE Internet of Things Journal 7 (2019) 4101–4112.
[33] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, J. Abdullah, Secure trust-based blockchain architecture to prevent attacks in vanet, Sensors 19 (2019) 4954.
[34] Z. Yang, K. Yang, L. Lei, K. Zheng, V. C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet of Things Journal 6 (2018) 1495–1505.
[35] A. Morim, E. S. Fortes, P. Reis, C. Cosenza, F. Doria, A. Gonçalves, Think fuzzy system: developing new pricing strategy methods for consumer goods using fuzzy logic, Int. J. Fuzzy Logic Syst. IJFLS 7 (2017) 1–15.
[36] S. Velliangiri, P. K. Karunya, Blockchain technology: Challenges and security issues in consensus algorithm, in: 2020 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2020, pp. 1–8.
[37] Y. H. Kim, S. C. Ahn, W. H. Kwon, Computational complexity of general fuzzy logic control and its simplification for a loop controller, Fuzzy Sets and Systems 111 (2000) 215–224.