IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 March 2023, accepted 16 April 2023, date of publication 20 April 2023, date of current version 18 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3268991

SURVEY

Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey

HOUDA AMARI[1,3,4], ZAKARIA ABOU EL HOUDA[2], (Member, IEEE), LYES KHOUKHI[3], (Senior Member, IEEE), AND LAMIA HADRICH BELGUITH[4]

[1]University of Caen Normandie, 14000 Caen, France
[2]University of Montreal, Montreal, QC H3C 3J7, Canada
[3]GREYC Laboratory, ENSICAEN, University of Caen Normandie, 14000 Caen, France
[4]Faculty of Economics and Management of Sfax (FSEGS), MIRACL, University of Sfax, Sfax 3018, Tunisia

Corresponding author: Houda Amari (houda.amari@ensicaen.fr)

ABSTRACT Over the past few decades, Intelligent Transportation System (ITS) has become a vital and extensive element of daily human life and activity. Vehicular Ad hoc Networks (VANETs) have become the most promising components of ITS, which promises to enhance transport efficiency, passenger safety, and comfort by exchanging traffic and infotainment information to intelligent vehicles. Moreover, VANETs have emerged with new paradigms (e.g., Cloud, SDN (Software-Defined Networking), Fog computing, Blockchain, and AI (Artificial Intelligence) techniques) to provide strategic and secure communications to increase their reliability. Therefore, efficient and robust mechanisms, such as trust management, are essential requirements in VANETs. This survey provides an extensive overview of the VANET and trust management's main concepts. After that, we briefly review existing surveys, followed by the significant challenges of security and trust in VANETs. Then, we identify, review, classify, summarize, and compare related approaches. Finally, we give some future research directions.

INDEX TERMS VANET, SDN, security, privacy, trust management, blockchain.

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is a particular category in mobile ad hoc networks (MANETs) with highly dynamic topology and intermittent connections [1]. Since the information transmitted is distributed in an open-access environment, security and privacy are among the most critical issues related to VANETs. Hence, any VANET must satisfy the security services and privacy requirements [2], as illustrated in Table 1 and Table 2, for an efficient and reliable system. It must guarantee that the exchanged messages are not inserted or modified by any attackers (e.g., insider/outsider, malicious/rational, local/extended, active/passive attackers). Any affected application can cause severe threats to drivers and passengers. According to the World Health Organization [3], every year, over 1.35 million road users are killed on the roads. Therefore, authentication and trust [4] in the extensive data exchange are crucial requirements in VANETs. Privacy is crucial on VANETs. Hence, only Trusted Authorities (TA) [5] have access to sensitive and private information about vehicles to preserve drivers' privacy from any third party and ensure accountability. Therefore, TA can trace malicious nodes and reveal their real identities in the case of reporting false information about vehicle position or the traffic condition by malicious nodes within the network. Exchanged messages contain private information of the driver and should be sent anonymously to ensure the effectiveness of communications. Nevertheless, more is needed to guarantee that these messages are authentic. In this case, internal nodes can disseminate false messages in the network, which leads to severe accidents. Once TA and RSUs notice the false messages, they must identify and reveal the real identity of the malicious node which disseminated this. The primary role of the TA is registering participant vehicles and RSUs and generating their private keys and security parameters [6]. Moreover, TA provides pseudo-identities for

The associate editor coordinating the review of this manuscript and approving it for publication was Qingchun Chen.

TABLE 1. Security services in VANETs.

Service	Description
Availability	It is considered the most important security service because most of the attacks work on creating a problem against the availability of resources.
Authentication	Knowing whether the coming data is from a legitimate node or not.
Data integrity	The intactness of the messages sent by the legitimate user should be strong so that an attacker can not easily change messages information.
Confidentiality	This security service controls the revelation of message contents to unauthorized entities to preserve the user's privacy by remaining the exchange of encrypted data between communicating nodes.
Non-repudiation	prevents the sender/receiver from denying transmitted messages.

TABLE 2. Privacy requirements in VANETs.

Requirement	Description
Availability	Since, most of the attacks have been against the availability of resources, this requirement is considered the most important in VANETs.
Authentication of data	Transferred data between VANET entities must be verified.
Integrity of data	Transmitted messages are forwarded to the correct locations or not.
Privacy of vehicle	Personal and confidential users' data should not be revealed to viewers, neither the future activities of nodes and transmitted messages should be highly secured.
Authorization	Only VANET entities can avail the services provided by the network.
Tracking of vehicle ID	Network must be able to track the identity of the vehicle.
Scalability	VANET should add new nodes without affecting its performance.
Efficiency	Improved by minimizing the overhead, computation, delays, and collisions.
Freshness	New messages should be verified regularly to avoid the use of old one.

registered vehicles and keeps its hands on the real identities to trace any vehicle's malicious activities. RSUs must first analyze the received messages from vehicles to prevent false information attacks. Hence, RSUs need to have the potential to detect false information reports sent by vehicles. Therefore, Public Key Infrastructure (PKI) is a crucial requirement in VANETs. Several security solutions depend on traditional PKI that quickly detect only outsider attackers. Traditional PKI can not detect insider attackers because they are participating within the network and already have verified credentials [7]. Therefore, researchers introduced the concept of trust [8] as a security parameter that can detect insider attackers by analyzing mutual messages. Additionally, trust-based approaches are still relatively in their early stage to ensure the effectiveness of VANET deployment. Based on trust models, a node will assign a trust degree to another node within the network during communication. Trust management recently attracted researchers' attention [9] due to its potential to broadcast reliable information across the network, eliminate false messages, track selfish and malicious nodes, and mitigate its activities. So, trust models need to be installed in RSUs and vehicles to determine the reliability, accuracy, and authenticity of received messages.

A. CONTRIBUTIONS OF THIS WORK

This paper provides a detailed survey on trust management in VANETs. Although recent researchers pay great attention to the trust deployment in such networks, related surveys that straightforwardly address this topic are limited. Therefore, we review, analyze, and compare in this survey the proposed schemes published in the last six years (from 2017 to 2022), which have been proposed for managing trust in VANETs. Also, we classify them based on emerging technologies and Artificial Intelligence tools. The organization of our survey is presented in Figure 1.

B. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows: In Section II, we provide a comprehensive overview of the trust management mechanism in VANETs. In Section III, we discuss some of the existing survey papers on this topic. Then, we outline the security and trust management challenges, also the most common attacks in VANETs in Section IV. In Section V, we provide a new classification of these approaches based on the technology used. In Section VI, we give a summary of the surveyed trust management approaches in VANETs and we provide a comparison based on a set of criteria. Some open issues and future directions are discussed in Section VII. Finally, we make some concluding remarks in Section VIII.

C. METHODOLOGY OF RESEARCH

This paper is meant to review, classify, compare, and summarize work done in the field of trust management in VANETs over the recent years (from 2017 to 2022). We established this survey based on a selective methodology of research (mainly the year of publication and adopted tools as the search's set of criteria). Selected works mentioned in this paper must respond to the following questions:

- What are the main pillars of trust management in VANETs?
- What are the standard metrics used to assess trust in such networks?
- How can we classify the recent trust management schemes?
- What is the set of criteria to summarize these approaches?

TABLE 3. Existing surveys on VANETs.

Ref.	Year	Major contributions	Topic
[11]	2017	Overview on VANETs architecture, security issues, prevention measures of those issues, and comparative analysis.	Security
[12]	2020	Comprehensive survey on various attacks, proposed solutions and analysis and comparison	Security
[13]	2019	Overview of VANET architecture, security attacks and challenges discussion	Security
[14]	2021	Comprehensive survey on VANETs, attack models, analysis of the security and privacy requirements for identity-based security and privacy schemes	Security, privacy
[15]	2021	Overview of VANETs, different possible attacks, detailed review of privacy and authentication schemes, attacks countermeasures and performance measures, some open issues	Security, privacy
[16]	2021	Existing authentication and privacy schemes, detailed comparison based on a set of criteria, qualitative comparison with the existing surveys	Privacy
[17]	2021	This survey review, interpret, and compare some of the recently proposed trust's building and management schemes and discuss the disadvantages of current works and future challenges.	Trust
[18]	2019	Detailed overview of VANET, authentication schemes review, location privacy protection mechanisms, trust management models analysis, future directions	Security, trust and privacy
[19]	2018	Identification and review of recent issues surrounding efficient routing protocols, detailed qualitative comparison	Routing
[20]	2018	Comprehensive survey and classification of pseudonym changing strategies, comparison based on relevant criteria, open issues, future directions	Privacy
[21]	2020	Critical analysis of existing machine learning-based trust approaches	Trust
[22]	2018	Identification of Trust management approaches, detailed analysis: concepts, methodology, algorithm, QoS and performance capabilities, qualitative comparison, open issues	Trust
[23]	2018	This survey addressed the quality of service in VANETs and presented a quantitative comparison between different routing protocols.s	QoS
[24]	2019	Detailed review of security attacks and protection schemes	Security
[25]	2019	Survey on recent trust management solutions in VANET	Trust
[26]	2017	Overview of security challenges, authentication and trust models	Security, trust
[27]	2022	Extensive survey: communications, applications, challenges, open issues	Security

To identify our selected surveys, we used relevant keywords such as ''VANET'', ''Trust'' and ''used tools''. We obtained a large number of papers related to the topic. During the search process, we notice that ''privacy'' and ''reputation'' are toughly related to ''Trust''. To extract more specific and new papers, we refined our used keywords to combine the ''Trust management'' and ''VANET'' keywords with ''Cloud Computing'', ''SDN'', ''Edge/Fog Computing'', ''Blockchain'', or ''Artificial Intelligence techniques''.

II. TRUST MANAGEMENT MECHANISM: OVERVIEW

In general, trust is the relationship between two elements within the network. In this paper, we denote them as trustors and trustees. The trustor is the participant who will evaluate the trustee, and the trustee is the participant being evaluated by the trustor. For example, when we say X trusts Y, X is the trustor, and Y is the trustee. In this section, we describe and define the trust mechanism to understand the surveyed approaches in this paper. Securing vehicular network communications results in the necessity of the deployment of robust and efficient trust management models. The trust mechanism aims to identify whether information from a sender node may be accepted or discarded by the receiver node (vehicle or RSU) based on a specific degree of certainty called trust value. The trust value is the probability of performing a specific action by an entity/node within the network. It varies from 0 to 1 : 0 thoroughly distrusted and 1 wholly trusted. We summarize the main concepts of the trust management mechanism in Figure 2.

A. PROPERTIES

The trust mechanism has many properties, and we can define them as follow:

- Direct: The trust value calculation is based on the direct relationship between the trustor and the trustee.
- Indirect: The trust value calculation is based on the recommendations broadcast by neighbors of the trustor.
- Local: The trust value is restricted only for both participants and it can not be broadcast in the network.
- Global: All entities of the network have a specific and unique trust value shared with each other.

FIGURE 1. Our survey organization.

- Subjective: The trust calculation only depends on the opinion formed by the trustor.
- Objective: The trust calculation depends on specific parameters of the trustee node.
- Asymmetric: One-way trust or unidirectional trust relationship. For example, when A trusts B that does not mean that B automatically trusts A. Asymmetric trust means when A trusts B, B does not trust A.
- History dependent: The trust calculation is based on the past behaviors of the trustee.
- Context-dependent: The trust calculation depends on environmental events or circumstances.
- Composite: The trust value is calculated based on some parameters such as honesty, security, etc.
- Dynamic: The trust value is dynamic with time and can be updated due to any change of initial parameters.

B. METRICS

Based on the surveyed approaches, we outline in this section the different metrics generally applied in the trust measurement and evaluation in VANETs.

- Reputation-based: The node calculates the trust value based on given recommendations/opinions from neighboring nodes in the network about a specific node.
- Knowledge-based: The trust calculation of the node is based on past or direct experience with a specific node within the network.
- Expectation-based: The trust value here is calculated based on the expectation or prediction of the node's behavior. In the expected way, the node will calculate the trust based on its history with another node or it will predict it when there is no previous communication with it.
- Node properties: The trust calculation uses the main parameters of the node like direction, speed/velocity, etc.
- Proximity-based: The trusted formula of the network includes also the proximity parameters of the node like the time, distance, location, etc..
- Environment-based: The network area, density, or topology (especially the presence of the main component of the clustering mechanism: the cluster head) are considered as factors or parameters which can be included in the trust formula of the system.

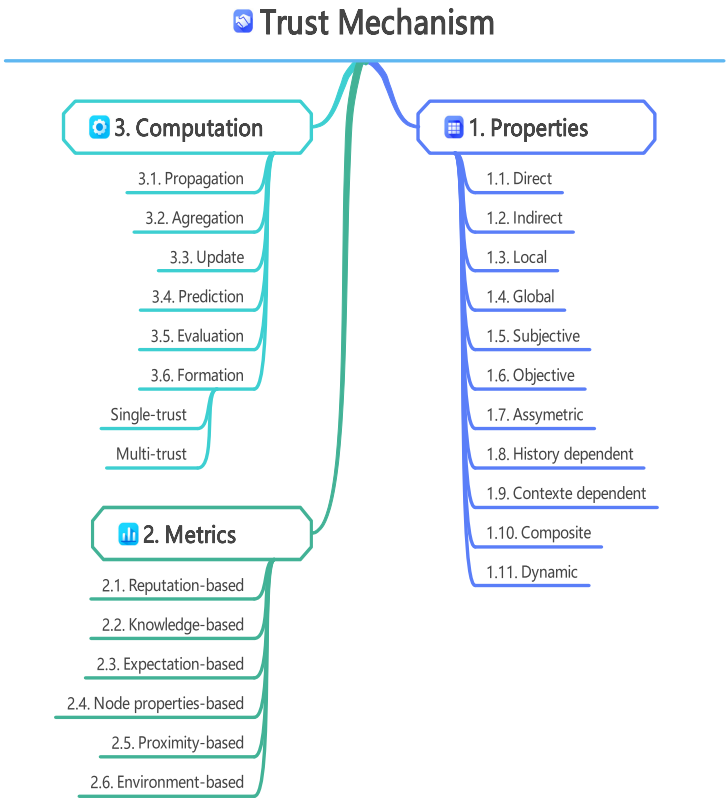

FIGURE 2. Trust management main pillars.

C. COMPUTATION MODULES

Trust management is a crucial aspect of securing communication in Vehicular Ad Hoc Networks (VANETs). The main modules of the trust management mechanism in VANETs include:

- **Trust Propagation Module:** Distributed, semi-distributed or centralized approaches are applied in the propagation module. In the distributed approach, every single node deploys the trust management and contributes to collecting information, trust computation, trust updating, storage, and dissemination without requiring a central agent. However, in the centralized approach, all these tasks are achieved by a central entity. Hence, the semi-distributed approach depends on a chosen set of entities and manages trust based on received information from other entities within the network.
- **Trust Aggregation Module:** Based on specific models, this module deals with the different propagated versions of the trust value of a node through different network paths from the previous phase. Machine Learning, Game Theory, Hybrid, Statistical, Probabilistic, and Fuzzy Logic models are the most used. The choice of the model depends on input attributes. For example, with a huge number of attributes we apply a Machine Learning model. However, the Bayesian model is applied to binary data.
- **Trust Update Module:** This module updates the trust values of nodes in real-time based on their current behavior and feedback from other nodes. The update module may use a variety of algorithms, such as Bayesian networks, decision trees, or neural networks, to update the trust values. This module consists of managing computed trust scores with time. Basically, we have two main approaches to updating trust: Event-driven and Time-drive. In the first approach, all activities (e.g. raising service/access request, delivery service, etc.) are assumed to be events. The trust value of the node is dynamically updated with each occurred event in the system. However, in the Time-event type, trust value is periodically updated using counter-based strategies without waiting for the occurred event.
- **Trust Prediction Module:** Trust between nodes is predicted based on specific metrics. This module deals with guessing whether a node will be trusted by a trustor or not.
- **Trust Evaluation Module:** Generally, the evaluation module depends on experience (direct/local knowledge), global knowledge parts (direct/indirect trust), and suggestion which is computed after requesting the node's neighbors and upgrading the table of trust. Hence, it will be computed as a recommendation and joins the global knowledge, and may asses the trustworthiness of an entity.

- **Trust Formation Module:** This module deals with the definition of the trust formula and how the trust value can be calculated. Trust formula depends on chosen metrics and properties which means it can be simple or composed. Two typical categories are defined in the formation module: Single-trust and Multi-trust.
  Trust Inference Module This module infers the trustworthiness of nodes based on their trust values and other contextual information. For example, if a node with a high trust value suddenly starts behaving suspiciously, the inference module may lower its trust value and mark it as untrustworthy.
  Trust Revocation Module This module revokes the trust of nodes that have been identified as untrustworthy or malicious. Once a node's trust is revoked, it is no longer allowed to participate in the network and its communication is blocked.

III. EXISTING SURVEYS

In this section, we introduce the most recent comprehensive surveys addressing trust management in VANETs. We summarize the contributions of these papers in Table 3. We remark that a restricted number of articles have underlined VANET trust management works. The mentioned surveys exploring the works on VANETs in terms of security and privacy could bring more understanding to our survey since we will discuss the critical VANETs' security challenges in the next section.

A. CONTRIBUTIONS OF EXISTING SURVEYS

There is a significant number of surveys have been proposed regarding VANETs, as shown in Table 3. Most of them inspected security and routing protocol issues and provided a detailed overview of VANETs from an architectural view [11], [12]. Other surveys provided detailed reviews on possible security issues following related solutions [24]. Authors in [14] introduced a comprehensive survey on VANETs and outlines some attack models and provided a qualitative analysis of the security and privacy requirements for identity-based security and privacy schemes. In [16], authors provide a comprehensive survey of the existing authentication and privacy schemes and compare them based on all security and privacy requirements, computational overheads, and the level of resistance to different types of attacks. This paper also provides a qualitative comparison with the existing surveys. Reference [20] introduced detailed surveys regarding privacy in VANETs.

B. COMPARISON WITH OUR SURVEY

Although there are a considerable number of publications concerning trust management in VANETs, there are so far rare exhaustive surveys that cover all the various characteristics of trust. In Table 4, we compare our paper with the above-mentioned scheme regarding trust management in VANETs based on: trust modules, trust metrics, trust challenges, trust attacks, open directions, taxonomy, evaluation criteria, and simulator. This comparison shows that our paper focuses extensively on identifying, reviewing, classifying, and comparing the different trust-based schemes while covering the various aspects of trust.

IV. CHALLENGES

In this section, we identify and discuss significant security and trust challenges of VANETs. Then, we briefly explain the most common security attacks and outline some related solutions.

A. SECURITY CHALLENGES

In VANETs, data is transmitted through a wireless network vulnerable to malicious nodes intercepting it. Hence, security issues are the most critical challenges in VANET. Hence, any affected application can cause severe threats to drivers and passengers. Also, in VANETs, the high mobility of vehicles, dynamic topology, scalability, short-duration communication links, heterogeneity of technologies deployed in the network make it challenging to detect malicious attacks. Therefore, maintaining security for VANET's entities (drivers, passengers, vehicles, roadside units, traffic management authorities, etc..) is very crucial. Therefore, VANETs must guarantee that the exchanged messages are not inserted or modified by attackers. In the case of an impersonation attack, the attacker uses the identity of another node (e.g., malicious nodes generally masquerade as emergency entities) and communicate with victim nodes to make them change their behavior. Security and privacy in VANETs are directly related to trust issues. Several research works have been done in the scope of this topic, such as privacy preservation approaches, cryptography-based, pseudonym-based, certificate/certificate-less-based authentication, and id-based signature approaches. These schemes are growing significantly and ensure the reliability of VANETs, especially by combining emerging technologies and Artificial Intelligence-enabled techniques.

B. TRUST MANAGEMENT CHALLENGES

In recent years, vehicle privacy and authentication concerns are growing significantly, and trust models are seen as security tools in VANETs. However, they are still relatively in their early stages and facing many challenges, same as security issues. Therefore, VANETs must ensure trustworthiness for users when communicating with each other. Trust models aim to track and eliminate malicious and selfish nodes and ensure that only reliable information is broadcast in the network. They must be highly resistant to malicious attacks (e.g., bad-mouthing, on-off, movement tracking, message sniffing, etc..) For instance, the on-off attack is a typical node-behavior attack that aims to avoid a bad reputation by launching a malignant service and behaving well alternatively. Moreover, selfish nodes' attacks aim to seek and deny communications, just like in greedy nodes, to interrupt event logging and stop tracking the actions of nodes. Also, we cite the Bad mouthing attack, another severe reputation-based attack. It aims to

TABLE 4. Comparison of our paper with different trust surveys.

Comparison aspects	Ref. [17]	Ref. [18]	Ref. [21]	Ref. [22]	Ref. [25]	Ref. [26]	Our survey
Trust's modules						✓	✓
Trust's metrics	✓	✓	✓		✓	✓	✓
Trust's challenges					✓	✓	✓
Trust's attacks	✓	✓		✓	✓		✓
Open directions				✓	✓	✓	✓
Classification	✓	✓	✓		✓	✓	✓
Evaluation criteria	✓			✓			✓
Simulator	✓	✓	✓		✓		✓

collapse/reduce the trust reputation of other nodes in the network by providing bad recommendations about them. Then, VANETs still claim privacy and trust requirements concurrently since private and sensitive users' information can be revealed (e.g., geographic location, real identity, etc..), which leads to ruin or infects the trust relationship and communications between nodes.

C. SECURITY ATTACKS IN VANET

Security means the state of being free from danger or threat. It means safety, as well as the measures taken to be safe or protected. VANET is a complex, heterogeneous system with several vulnerabilities. Therefore, several attacks can occur. Moreover, VANET's unique characteristics (e.g. dynamicity, scalability, etc..) make the prevention/detection of these security issues more challenging. Many researchers have explored the security attacks in VANETs [28] and tried to provide taxonomies and related solutions. In this subsection, we outline security issues in VANETs and we provide a summary of these attacks in Table 5.

- **Non-repudiation:** This attack aims to deny the transmission or reception of messages by the sender or receiver. It impacts VANET's resources. In fact, it overuses the bandwidth of the network by requiring several retransmissions and resulting in delays problems.
- **Spamming:** In this attack, spam messages are sent by nodes present inside the network. It aims to increase the rate of transferring of messages, latency, and utilization of bandwidth and leads to several collisions in the network.
- **Denial of Service (DoS):** DoS is one of the common attacks in VANETs, which is caused by internal or external vehicles in order to make the resources and the services inaccessible to the users in the network and is done by either making the channel or the node busy.
- **Distributed Denial of Service (DDoS):** DDoS attacks are a common problem in VANETs due to the decentralized and dynamic nature of the network [29], [30], [31], [32]. In a VANET, vehicles communicate with each other directly or through roadside units, forming a self-organizing and self-configuring network. This makes VANETs vulnerable to DDoS attacks, where a large number of malicious nodes flood the network with illegitimate traffic, overwhelming legitimate communication and making it difficult or impossible for vehicles to communicate with each other. DDoS attacks can take different forms in VANETs.
- **GPS Spoofing:** In VANET, the integrity of GPS signals of nodes has a vital role. So, the position and the location of nodes must be authentic. This attack aims to overpower the GPS signal and manipulate it to change the location table in the GPS satellite and reveal fake location information to the vehicles which infect its authentication.
- **Replay:** In this attack, the malicious node stores the received message by another node and replays it continuously which make it difficult to identify the vehicles in case of emergency. This may lead to several disasters such as potential collisions.
- **Masquerading:** The attacker masquerades using the identity of another legitimate node as his mask to allow him to produce false messages looking authentic. This attack aims to create a black hole in the network.
- **Man-in-the-middle:** This attack takes place in the middle of V2V communication to change and check the messages closely. The entire V2V communication can be accessed and controlled by the attacker.
- **Wormhole:** In VANET, this attack aims to extend the tunneling of packets between two malicious nodes. So, two malicious nodes at least can be controlled by the attacker. During this attack, malicious nodes include themselves as a part of the reply Wormhole. In VANET, this attack aims to extend the tunneling of packets between two malicious nodes. So, two malicious nodes at least can be controlled by the attacker. During this attack, malicious nodes include themselves as a part of the reply.
- **Greyhole:** This attack consists in removing only the data packets of certain applications that are vulnerable to

packet loss. Greyhole is considered as a Blackhole attack variant and it targets the availability in the network layer.

- **Jellyfish:** This attack targets mainly the availability of the network layer. There are two types of jellyfish attacks. The first aims to make the malicious node reorders the packets before forwarding them; acknowledgments are not received in the sequence which means messages need to be sent again. The second type is the periodic dropping attack where packets are randomly discarded during the communication processes, and incorrect route congestion information is reported. This information makes the JF node take a decision of discarding a fraction of packets, for a few milliseconds, which increases the timeout of retransmission.
- **Black hole:** A black hole means redirected traffic where the malicious node announces that it has the shortest path and receives the data from the registered user and declines to contribute to the system. In fact, all received packets may be dropped by the receiver too which results a disruption in the routing table. This attack targets the availability of VANET.
- **Sybil:** This attack aims to inject wrong information through the system in order to control the network by the malicious node which affect directly the generated reports by different nodes. Therefore, affected vehicular nodes may take wrong decisions different to the real scenario which targets the efficiency of the system.
- **Message tampering:** This attack is used when the route is congested and the attacker wants to clear the road. Therefore, it modifies or alters a recent message by a malicious node and then sent to the destination as an authentic one which targets the integrity of messages and troubles the network since everyone in the surrounding can listen to it.
- **Tunneling:** It aims to compromise the system. In fact, the attacker initiates a private conversation and connects two parts of the network using an external communication channel named a tunnel, therefore, the nodes which are far can communicate as neighbors which completely troubles the network.
- **Greedy behavior:** The attacker misuses the message authentication code (MAC) protocol to increase a large amount of bandwidth and use network resources only for himself and make other nodes go through alternate routes and get a clear path to the destination which results in a traffic overloading, collision on the transmission channel and delay in the legitimate services of the registered user.
- **Illusion:** This attack received data from antennas and collected malicious data from sensors and generate traffic warning messages by using the existing road which may create an illusion for the vehicles. Since drivers 'behaviors depend on the traffic warning messages they have received, this attack will cause vehicle accidents and traffic congestion and also minimize the performance of the system.
- **Traffic analysis:** The attacker works on extracting the maximum useful information by listening to the message transmission and analyzing its frequency. This is one of the dangerous attacks which threaten confidentiality and privacy in VANETs.
- **Jamming:** This attack aims to disturb the communication channel in VANETs by using a heavily powered signal with an equivalent frequency and it lowers the Signal to Noise ratio for the receiver. Since this attack did not follow the valid safety alert, then it is considered the most dangerous attack for safety applications.
- **Impersonation:** In order to attract other vehicles to communicate with and change their behavior, some vehicles masquerade as emergency entities using this attack. It depends on Building up a Secure Connection along with Key Factors (BUCK) Filter which detects impersonation attacks by broadcasting beacons and detecting the accurate position of the messaged vehicle. Once the faulty node is detected, it is isolated from the communication environment.
- **Free riding:** It occurs by false authentication efforts while associated with the cooperative message authentication. So, the attacker takes advantage of other users' authentication contributions without having its own. This attack is considered a serious threat to cooperative message authentication.
- **Replication:** In this attack, the malicious node has the job to add nodes to the network. It uses the identity of another node present legally in the network to transmit false messages to the network. The attacker needs proof of authentication to create uncertainty in the system so, he uses duplicate keys and/or certificates of other users which makes the situation worst for traffic authorities to identify the vehicle and creates confusion for the Trusted Authority (TA).
- **Eavesdropping:** It is against confidentiality and it is very common in VANETs. It aims to disclose and get confidential information from the vehicles' protected data. So, non-registered users can get secret details such as user identity and data location that can be used for tracking vehicles and performing various attacks easily.

V. CLASSIFICATION

There are basically three types of trust management approaches currently in use: Entity-based schemes, Data-based schemes and Hybrid schemes. in this subsection, we overview these categories and we discuss the proposed taxonomy based on used technology: emerging technologies and Artificial Intelligence.

A. ENTITY-BASED SCHEMES

Entity-based schemes focus on associating the trust concept with the participating nodes in the network. Each entity has its trust value that evolves. These approaches evaluate the nodes' trust levels based on reputation-based trust metrics.

TABLE 5. Threats and attacks regarding security in VANETS.

Layer	Attack name	Attacks on	C. service	Solution
Physical	Jamming	Sensors input in vehicle	Authentication	[35]
	Impersonation	Infrastructure	Authentication	[36]
	Free riding	Infrastructure	Authentication	[37]
	Replication	Infrastructure	Availability	[38]
	Eavesdropping	Wireless interface	Confidentiality	[39]
	Man in the middle	Infrastructure	Confidentiality	[40]
Data Link	Traffics analysis	Infrastructure	Availability	[41]
	Illusion	Sensors input in vehicle	Confidentiality	[42]
	Greedy behaviour	Wireless interface, hardware and software	Authentication	[43]
Networking	Tunneling	Wireless interface	Authentication	[44]
	Sybil	Wireless interface	Authentication	[45]
	Message Tampering	Infrastructure	Authentication	[46]
	Black hole	Wireless interface, hardware and software	Availability	[47]
	Jellyfish	Infrastructure	Availability	[48]
	Grey hole	Wireless interface, hardware and software	Availability	[49]
	Wormhole	Hardware and software	Availability	[50]
Transport	Masquerading	Infrastructure	Confidentiality	[51]
	Replay	Hardware and software	Data integrity	[52]
	GPS Spoofing	Sensors input in vehicle	Data integrity	[53]
	DoS	Wireless interface	Authentication	[54]
	DDoS	Wireless interface	Availability	[55]
	Spamming	Wireless interface	Availability	[56]
Application	Non-repudiation	Infrastructure	Repudiation	[57]

Trust and reputation have been widely used in the literature to assess the trustworthiness of an entity. Hence, the trust formula depends on past knowledge-related metrics, such as the node experience of perceived behavior and activities over time and the exchanged recommendations among the different entities. For instance, a vehicle in a specific cluster thinks all vehicles in the same cluster are more trustworthy than vehicles in another cluster.

In [57], authors proposed a trust inference scheme invulnerable to attack in VANET. This approach is resistant to black/grey-hole attacks. The model is based on subjective trust, derived from historical interactions, and recommendation trust obtained from neighboring opinions. Hereafter, the authors illustrated a trust-aware multicast routing protocol.

Authors in [58] proposed a similarity-based scheme to mitigate the injection of false information and, in fact, the trustworthiness of safety-event reports in the network. In this work, the trust model generates the similarity rating based on periodic beacons containing the location and speed information and uses the echo protocol to confirm the produced reports.

Authors in [59] proposed a trust model based on a trusted authority node responsible for managing reputation scores. This entity decides whether a specific participant node can access the network or eliminate it. A low reputation score means an untrusted node that needs to be revoked. However, a high/acceptable reputation score means the credibility to access and communicate with the infrastructure.

In [60], authors integrate the highway platooning concept. Hence, platoon head vehicles are ranked based on reputation metrics. The trust model in this work introduces a particular server to assess vehicle head trust. The reputation calculation here depends on gathering feedback from vehicles user. The authors involved an iterative filter in banning the feedback of malicious nodes. Therefore, a reliable platoon head vehicle is recommended by the server node.

B. DATA-BASED SCHEMES

Data-based schemes aim to assess the data produced by an entity instead of the entity itself. Hence, trust is related to the content of produced messages. Therefore, the data authenticity requirement is crucial. The data-based trust model evaluates the trustworthiness of data content based on its utility. Utility means the worth of a specific event over another in the same context. Time, proximity, produced event, and node role are the influential factors that assess the data utility. Data trust evaluation is more convenient than the entity's trust due to the absence of social connections between fast-moving entities in VANETs.

A data-based scheme was presented in [61], authors in this work provided a scheme that detects malicious nodes in VANETs based on the similarity of messages. This model aims to check the similarity of nearby vehicles' received and self-reported messages. Based on speed and density parameters, each node can figure out its flow value using the Green-shields traffic model. Hence, the vehicle will compare the estimated flow value with the received message. Then, it will accept the received content if it matches its own estimation. Else, the sender node will be signaled and reported.

Another data-based scheme was presented in [62], the trust model is built based on location, proximity, location verification, and time closeness. Hence, the receiver entity calculates its confidence in each reported event by a specific sender. In this work, each message has its distinctive trust value concerning a reported event. Therefore, the suggested technique sorts the calculated trust weights to make the judgment in favor of the respective message.

In [63], authors presented an intrusion-aware strategy to guarantee the trust requirements in VANETs. In this model, the trust assessment counts on each content's confidence and trust values gathered about an exact event. Therefore, the trust formula relies on location closeness, data freshness, location correctness, and time verification parameters. Then, according to the sender node number and their confidence values, the authors proceed to calculate the trust value. Finally, the receiver will decide whether to accept or block the message by comparing the trust value to the threshold.

In [64], the authors introduced a trust model based on the Tanimoto coefficient. This solution depends on the cooperation between RSU and vehicles within the network. In fact, trust values are disseminated, built, and used by RSUs and vehicles after checking the reported events and beacons.

C. HYBRID SCHEMES

In Hybrid approaches, trust calculation is based on entity and exchanged data trustworthiness. The primary objective of hybrid schemes is to provide a more efficient trust evaluation that considers both the message and the entity's trustworthiness. In fact, in networks such as VANETs, data content evaluated by many trusted entities is exposed as trustworthy to other nodes within the network.

In [65], authors introduced a hybrid scheme that aims to enhance the efficiency of trust management in VANETs by paying more attention to the decision step. In fact, a decision must be taken within a specific time slot or when receiving several messages exceeding defined thresholds.

In [66], researchers introduced a scheme based on vehicles' and data trustworthiness. This approach is based on the behavior assessment process and similarity rating. The trust evaluation is conducted according to the DST-based data analysis. Then, the trustworthiness of data is estimated via reported traffic information similarity. Node trustworthiness is expressed utilizing a functional trust, which tells how probable the vehicle can perform appropriate behavior (the scheme assigns for each node a function of misbehavior's observed by neighboring nodes), and combined filtering-based recommendation trust. Cosine similarity is involved in helping the evaluation of recommendations' credibility, especially in trust rate formation and trusted neighbor selection. Hence, predicted trust rate computations are carried out to assist in defining the recommendation trust.

In [67], authors combined behavior and similarity factors to illustrate a robust and hybrid trust management scheme in VANETs. This work aims to detect the malicious data that are injected by the Sybil attack. The trust values are given via the verification of the similarity between the envisioned and the actual behavior (i.e., driver response face to traffic signals) of a vehicle and the similarity of neighbor vehicles generated message.

In [68], researchers introduced a model that aims to ensure location privacy in VANETs. It calculates the entity trust value by treating and verifying the probability of event and beacon messages. The trust assessment of the sender's entity beacon messages is based on the Cosine similarity technique. The trust calculations rely on position, velocity, and drive direction values. It takes into account too recorded trust information of neighboring vehicles' beacons. Hence, data trust is evaluated in two dimensions direct trust (e.g., based on event and beacons directly received and by verifying vehicle position and movement information; by using the Tanimoto coefficient additionally to the cosine similarity.) and recommendation trust (e.g., estimated based on vehicles recommendations). Then, based on the Dempster-Shafer Theory (DST), direct and indirect trust values are merged to obtain the final trust score and proceed to the decision phase according to a trust threshold value.

D. TECHNOLOGY-BASED CLASSIFICATION

Artificial Intelligence and emerging technologies, such as Cloud Computing, SDN, Fog/Edge Computing and Blockchain, are seen as useful tools for developing robust trust models. In this subsection, we review recent approaches of each technology.

TABLE 6. Basic trust managements schemes in VANETs.

Ref.	Class	Used metrics	Tools	Simulator	E. parameters
[58]	Entity	Reputation, knowledge	Markov process	SUMO, NS-2:	Detection rate
[59]		Node proprieties	Association rule mining and echo protocol	SUMO	Success rate
[60]		Reputation	Elliptic curve method	Not specified	Computation and communication cost
[61]		Reputation	Iterative filtering method	MATLAB	QoS of vehicles, accuracy level and resistance to bad-mouthing and ballot stuffing attack
[62]	Data	Node properties, proximity, environment-factors.	Defined formulas and signature-based	OMNET++, SUMO, VACaMobi	Average density and success rate.
[63]		Proximity	Defined formulas and signature-based	SWAN++	false location detection accuracy, false positive rate
[64]		Location	Defined formulas	Not provided	Time complexity and false node impact on trust.
[65]		Beacon	Tanimoto coefficient	NS-2, SUMO	Precision, recall, Detection delay
[66]	Hybrid	Reputation, event	Decision making process	NS-2	Detection accuracy, decision delay
[67]		Reputation, knowledge, environment	DST-based, osine similarity rule	GloMoSim	Precision, recall, communication overhead
[68]		knowledge+node proprieties	Defined formulas, stochastic cellular	Automata Model	detection rate,average delay
[69]		Beacon+event+reputation	Cosine similarity rule,signature-based	NS-2	attacks detection rate, misbehaving vehicle rate, detection delay

1) CLOUD-BASED SCHEMES

In [69], the authors exploited cloud technology to develop a trust approach that depends on the inter-connectivity between autonomous, connected vehicles. This approach contains three main layers: the cloud layer, the communication layer, and the physical layer. Authors suggested the fliplt game to capture the interactions between the services of the Cloud layer to support its security, which attackers endanger. Moreover, the different communication between the Cloud servers and connected machines is illustrated in the communication layer. Authors introduced in this layer a reputation and knowledge-based trust model using the signaling game to determine the trustworthiness of the Cloud services. The physical layer controls the performance of the participating devices, the attacker, and the defender in the signaling game. The performance of the Cloud layer and the physical layers' performance primarily define the necessary decision.

In [70], authors introduced a trust management work in VANET, which handles the computation process. The solution is formed of three steps. The pre-processing data task is performed in the first phase by the DST-based technique. In the next stage, the authors used a Fuzzy analyzer to determine the trust values of participating nodes in the network. The calculation of the trust values depends on direct and indirect trust values. Then, they exploited in the thirst phase rewarding and punishment algorithms to reward the honest vehicles and punish the malicious, respectively. In this approach, any vehicle can request the trust value of a neighboring node through the Cloud servers.

Another Cloud-based trust management approach was introduced in [71]. This work also is formed by three layers and two trust managers: a central Cloud layer, a roadside Cloud layer, a vehicle Cloud layer, a global and domain trust managers. The first layer contains all the vehicles' history communications and trust list, which the global trust manager manages. The performance of the domain trust manager and the roadside Cloud layer handles the different trust values' requests (neighboring, friends, history trust requests). The roadside Cloud layer is responsible for creating vehicular virtual machines. Therefore, the general trust degree is obtained

at the vehicle Cloud layer, where the vehicle can request the message's sender's trust from a vehicular virtual machine. This latter calculates the trust values of neighboring and friends nodes and obtains the history trust value from a central server. After that, the general value of the requested node's trust will be gathered to the requester vehicle. Needed updates are performed after each request.

Authors in [72] exploited the Cloud technology to introduce an agent-based intelligent scheme to manage the trust process. This approach contains two principal agents: mobile and static agents. The authors used both agents to evaluate the trust value of the Cloud service provider and the user. They exploited the direct (the past transactions of the accounts) and indirect (calculated by the mobile agent) trust values to estimate the cumulative trust value.

2) SDN-BASED SCHEMES

Authors in [73] exploited the SDN technology and deep reinforcement learning techniques to simultaneously develop a trust establishment and path learning solution in VANETs. Integrating the SDN leads the way to separate the data and control planes. In this work, a centralized controller contains the deep reinforcement algorithm so all legitimate vehicles can locate the best path trust value. Hence, they can establish performing data transfer. The authors used a Q-learning-based convolution neural network algorithm and the ratios of forwarding packets to assess the trust values.

In [74], the authors used the

Another work in [75] exploited the SDN technology to enhance the network performance by integrating the on-demand distance vector routing method. The presented work contains three main layers: data, control, and application. The data layer is responsible for forwarding data, and the control layer aims to discover the data route and manage the network topology. Tasks such as routing protocols' controlling are managed by the application layer. The calculation of the trust value in this work is based on the ratios of both the data and control packet forwarding.

Another SDN-based scheme was introduced in [76]. The authors in this work combined a geographic routing protocol with the capabilities of SDN to develop a routing process based on a trust management mode and encryption function. The authors integrate the clustering paradigm, where nodes are grouped into different clusters. Each cluster has an elected cluster head and cluster nodes. The cluster head node represents a semi-centralized controller that manages its communications' errors log. The cluster head election in this work is conducted using a map factor. Hence, the vehicle that keeps its public key and its neighbors' weights will be selected as the cluster head node. Moreover, these weights values are calculated based on the capacity of load identified by the trust level and the received beacons. The saved past interactions in the error log are the main parameter to determine trustworthiness.

3) FOG/EDGE-BASED SCHEMES

Authors in [77] exploited the Edge/Fog technology to enhance trust management in VANET. This approach aims to execute reputation management using local servers. Hence, Edge servers are scheduled by trusted local authorities to improve the trust process. Therefore, a set of reputation segments will be uploaded to the nearest local authority by each node. Then, it will be aggregated and updated and stored in a global reputation dataset simultaneously. Hence, each vehicle will be able to discover the fresh reputation value of another passing node before cooperating with it.

In [78], the authors exploited the bidding price-based method to enhance the trust in Fog services. In this work, the authors integrate the requirement of certificates by each vehicle for guaranteeing the registration of legitimate nodes to the infrastructure to conduct For services transactions. After registration with their digital currency, accepted vehicles can perform activities within the uncovered zone. Hence, the need to use the infrastructure-based Fog node resources to boost the exploitation of the Fog services. The trust calculation in the rural zone used metrics such as the transaction record, the type of node, bidding number. It also considers the global transactions (e.g., infrastructure-based Fog node). Malicious activities within the network may conduct to reveal the bidding of actors, which results in a trust loss and victim's compensation.

In [79], the authors exploited the Fog computing technology to manage the trust in VANETs. This scheme is composed of two layers. A layer is responsible for the communication system, consisting of a Cloud server and trusted authority, and the other layer is formed by vehicles and Edge nodes. The trust value of the sender and the message is calculated using defined Fuzzy rules that consider the location verification-based, vehicle type, and experience as parameters. Hence, each registered vehicle has an authentication level assigned by the Edge nodes. Moreover, this level is extracted by a query from the relevant Edge node so the receiver vehicle can make the right decision. The authors exploited the Cuckoo filter to enhance the system's performance against the generated data volume. They also used the k-nearest neighbors algorithm to mitigate the none line sight circumstances.

In [80], authors exploited Fog Computing's capabilities and proximity from edge users to employ the most competent node, which reduces the workload demanded by vehicles, such as the sender's trust evaluation and propagation of the details of events. Hence, the trust evaluations performed by local vehicles are gathered by the fog node, which makes the vehicles more autonomous to perform specific tasks locally and reduces the communication of the Edge nodes with the cloud. The authors developed the trust scheme based on the vehicles' performance reputation with the Task-based Experience Reputation (TER) method. Applying the TER in this work decreases the overhead of message transmission and workload on the vehicles.

4) BLOCKCHAIN-BASED SCHEMES

The use of the Blockchain in VANET for trust management is gaining more attention. Authors in [81] integrated Blockchain technology to enhance privacy in VANET by establishing a reputation management system. This latter comprises the main entities: the certificate authority and the law enforcement authority. The certificate authority will deal with the certificates' generation and management in this work. Then, it will be added to the Blockchain. The law enforcement authority performs tasks such as vehicle registration and reputation assessment. Hence, real identities, public keys of registered nodes, generated or revoked certificates, and the exchanged messages of the Blockchain are stored in a dataset managed by the law authority. Therefore, reputation management adapts reward and punishment standards based on an anonymous authentication algorithm to improve trust establishment.

Moreover, in [82], the authors exploited a regional federated learning technique to improve security and preserve privacy in the network. In this work, there are different regions of vehicle training models locally. The reputation management of these vehicles is performed by a robust mechanism that ensures their trustworthiness.

In [83], the authors combined the Blockchain and deep learning technologies to enhance trust management in VANET. In this work [83], each node can proclaim malicious nodes to the RSU entity after assessing all the received messages from the nearby vehicles. The Blockchain is exploited to verify the authenticity of these credentials. Thus, the RSU will correctly revoke the malicious nodes within the network. In another work [84], the authors in [84] introduced a robust system based on these steps: ratings' generation and uploading, trust values offset computation, miner election, generating new block, and the consensus algorithm. In this work, the authors exploited the Bayesian inference to filter the credibility of received messages. Hence, a specific rate is accorded to each message and uploaded to the RSU. Then, the trust value offsets are calculated based on weighted aggregation to pack them into one block. The miner election step aims to determine which node should generate a new offset block. In this work, the RSU with more stakes is considered the miner because, according to the consensus mechanism, offsets absolute values are considered as stakes. Next, a new offset block will be added to the trust Blockchain. Applying the consensus algorithm shows good resistance against the simultaneous receiving of blocks.

5) ARTIFICIAL INTELLIGENCE-BASED SCHEMES

AI-based approaches integrate clustering and reinforcement learning, fuzzy logic, and game theory techniques in trust management in VANETs.

a: CLUSTERING AND REINFORCEMENT LEARNING-BASED SCHEMES

In [85], authors exploited the stability and clustering algorithms to manage the trust in VANETs using the metrics of communication and data trust. In this approach, the vehicle's stability depends on the similarity factor of its mobility. This trust model comprises three phases: neighborhood discovery, cluster head election, and stability maintenance. The neighborhood discovery phase considers only neighboring vehicles in the same direction. In the second phase, the authors used a backoff timer to calculate the trust score depending on reputation, direction similarity, and mobility. To maintain the cluster's stability, the authors also used two main steps. The Beta reputation system-based to supervises cooperated vehicles' behaviors with other nodes. The further step consists of an event reputation-based with severity metric-based system to evaluate the exchanged information reliability.

Another clustering-based approach was introduced in [86], where the authors presented a composite metric to contain the given vehicle's trustworthiness values and known related resources. In this scheme, neighboring vehicles can allocate a trust score to each node using behavior-based metrics. Hence, all the participating nodes have a precise trust score assigned by their neighboring nodes. The authors concern the computation resources by giving more attention to factors such as the nodes' link capacity and the remaining power to determine the later resource requirements of nodes. The cluster head election in this approach depends on the composite value. The node with the highest composite value will be elected as the cluster head.

In [87], the authors presented a collaborative intrusion detection system for VANETs. This scheme is based on ensemble learning and shared knowledge techniques. Therefore, the participating nodes aggregate rating scores using a voting scheme to elaborate a set of weighted random forest classifiers. Hence, these local classifiers will be trained by each vehicle and communicate its knowledge as a trust factor.

Another scheme was presented in [88]. It integrated crewless aerial vehicles to help route and identify dishonest vehicles (e.g., when roads are disconnected, crewless aerial vehicles can assist in relinking communications). This scheme contains two main routing modes. The routing data among vehicles with the help of crewless aerial vehicles is to decrease delay and overhead and the routing data among crewless aerial vehicles. The uncrewed aerial vehicles choose the cluster heads based on the speed, position, and trust parameters. The authors exploited the ant colony optimization algorithm to enhance the routing procedure, and the trust score is knowledge and recommendation-based.

b: FUZZY LOGIC-BASED SCHEMES

In [89], the authors presented a trust management approach based on fuzzy logic techniques to check the plausibility of exchanged data. In this scheme, each node encrypts its transferred data with a unique identifier, which the receiver node will verify. The authors introduced a range of behavior metrics for the trust evaluation process: cooperativeness, honesty, and responsibility. Each node with a high trust value is an excellent cooperative node. Honesty represents

the percentage of transmitted honest packets. The trustee node with a high percentage in detecting event reports is considered a responsible node. The fuzzy logic process in this solution depends on calculating the mentioned metrics to convert them to fuzzy values. Hence, these values will be applied to fuzzy rules. Hereafter, the final trust value is calculated after applying the defuzzification phase.

Another Fuzzy logic-based scheme was introduced in [90]. The authors in this scheme modeled the malicious behaviors of the node using three trust factors captured by the Fuzzy sets. In this work, the trust calculation is based on a fuzzy-logic algorithm. The authors also paid attention to the impact of content modification. Hence, this impact is defined by a specific parameter to identify its effect on the trust estimation. This approach showed a remarkable precision, recall, and accuracy rate.

Another work was presented in [91], where the authors proposed a robust authentication scheme to protect the users from malicious nodes using Fuzzy logic. They developed a fuzzy-based authentication algorithm to detect the malicious nodes in the system depending on the Mamdani Fuzzy Inference technique. The authors conducted good simulations using this technique with MATLAB. This approach allows only honest nodes to transmit data with participating nodes within the network.

In [92], the authors presented a trust protocol called Fuzzy Trust Optimized Link State Routing (FT-OLSR). It is an extension of the OLSR security protocol. In this approach, each node will calculate the trust score of its one-hop neighboring nodes by exchanging control messages using the FT-OLSR routing protocol. Conducted simulations in NS-2 showed that applying the Fuzzy logic to the OLSR routing protocol enhanced its performance.

c: GAME THEORY-BASED SCHEMES

In [93], the authors introduced a theory-based game method to secure communications in the Internet of Vehicles (IoV). The solution depends on the hedonic coalition's model. The coalition vehicle collaboration is formed depending on integrating the vehicles' trust to enhance building trust relationship and coalition joining intention in the system. Using some direct historical interactions, the authors used the Bayesian inference filter to evaluate the trust value. In this solution, the receiver vehicle compared the content of the transmitted message to the real event state. Therefore, it can update the sender vehicle's trustworthiness score depending on the incomplete beta function. The authors also presented a punishing model for the newly joining nodes with no historical interactions. This scheme aims to capture trust score changing variation and derive new coalitions by periodically conducting the coalitions' algorithm. This latter forms the final coalition depending on the vehicles' trustworthiness and preference relation. According to this scheme, the shifting rules allow vehicles to move between coalitions.

Another multi-layered intrusion detection scheme for VANET work was introduced in [94]. The authors used the game theory technique with a distributed Cluster Head (CH) selection algorithm. Therefore, the classification of malicious nodes is conducted by a lightweight neural network classifier. To enhance the performance of the vehicles in electing the relevant cluster head, the authors applied the Vickey-Clarke-Groves method. Hereafter, the RSUs hold the reputation values of nodes to evaluate the trustworthiness of the CH.

In [95], the authors presented a theory-based game scheme to manage the trust in the IoV system using an evolutionary game framework within a reputation-based trust model to simulate the dynamic protection system by giving the attacking strategies models of the malicious nodes. This trust mode allocates a trust score to the vehicles and traffic-related event messages. Moreover, the authors introduced a punishment algorithm for the vehicles sending false reports or deleting sent messages. Hence, their trust score will be decreased by one unit. Deception intensity is critical in deploying this scheme, representing the vehicle's ability to deceive other nodes and falsifying events' reports. These nodes aim to conduct the best negative system by changing the distribution of the decision to converge the optimal choice. The joining or rejoining process and the dishonest nodes' eviction are enhanced with the evolution of such a scheme.

In [96], the authors introduced a trust management scheme to enhance the performance of vehicles to estimate other nodes' trust values (using the reputation-based method) and to assess legitimate messages. Certainty is the critical factor in evaluating the trust of the vehicles. In this approach, the direct reputation information is extracted from the direct interactions and stored in historical communication tables. However, the indirect reputation is conducted by the neighbors' ratings and the recommendations of the RSUs. The authors used the Fuzzy C-means clustering technique to distinguish the trustworthy reported messages in the indirect-reputation establishment. Both computed scores are combined using the uncertain deductive theory. The authors used the K-means algorithm in this scheme to evaluate the received contents' legitimacy. Only received messages with a good reputation level (bigger than a defined threshold) will be forwarded, else they will be discarded. The authors developed the scheme to achieve nodes' cooperativeness. They presented an evolutionary game theory-based incentive scheme. This model combined three main modules: nodes cluster, adopted methods, and payoff calculation.

VI. DISCUSSION

Based on the extensive survey above proposed, trust management is crucial to ensure the reliability of the network. We summarize, compare and discuss the surveyed schemes in Table 6, Table 7, Table 8, Table 9 and Table 10. Integrating multiple technologies to the network, brings out new security and privacy challenges

TABLE 7. Emerging technology-based trust management schemes in VANETs.

Ref.	Class	Used metrics	Tools	Simulator	E. parameters
[70]	Cloud	Reputation, knowledge	Flipit game,signaling game	MATLAB	Cloud's controlling service probability
[71]		Reputation,knowledge,event	DST-based,fuzzy rules	Java-based	Response time,trust value change
[72]		Reputation,knowledge	Defined formulas	Performance Evaluation,Process Algebra	Throughput,response time
[73]		Node proprieties	DST-based	Not available	Not available
[74]	SDN	Knowledge,node properties	Q-learning	TensorFlow, OPNET	Throughput
[75]		Knowledge+ node properties	Deep Q-learning, Markov decision process	TensorFlow	Convergence performance, delay
[76]		Node proprieties	Defined formulas	OPNET	Throughput, total messages sent
[77]		Knowledge	Clustering scheme, signature based	NS-2.34, VanetMobiSim	Packet delivery ratio, average end to end delay
[78]	Fog/Edge	Node proprieties	Signature-based bidding price	Not available	Transactions, attacks number
[79]		Reputation	Multi-weighted subjective logic	Not available	Average reputation value, Detection rate
[80]		Knowledge, node proprieties, event	Fuzzy logic, K-nearest neighbour algorithm	NS-2,SUMO, MOVE	Precision,recall,communication overhead
[81]		Node properties, reputation	Task-based Experience Reputation (TER)	NS-2	Overhead and workload of messages.
[82]	Blockchain	Reputation, knowledge	Proof-of-work signature-based SHA-256	Not available	Storage and transmission overhead
[83]		Reputation	Regional FL algorithm signature-based	Not available	Model accuracy rate
[84]		Node proprieties	Deep Learning (FeedForward Neural Network	NS-2, SUMO	Precision, Recall of malicious nodes detection
[85]		Node proprieties	Proof of Work, Proof of stake,SHA-256,Bayesian inference	Matlab-based	unfair ratings vs false reports rates

A. SUMMARY

We summarize the surveyed schemes based on a set of criteria: approach's category (basic or emerging/AI based approach),class of the approach (entity-based, data-based, or hybrid), used trust metrics, used tools, simulator, and evaluation parameters (E. parameters), in Table 6, Table 7 and Table 8 This summary serves to display a qualitative comparison between these approaches in the next subsection.

B. COMPARISON

This subsection serves to display a qualitative comparison between summarized approaches in terms of scalability, dynamicity, privacy, complexity, computation overhead, and robustness as indicated in Table 9 and Table 10.

In this subsection, we will discuss the surveyed trust managements approaches based on a set of criteria: Privacy, scalability, dynamicity, complexity, overhead communication and efficiency.

1) PRIVACY

Privacy is still one of the most critical concerns of future connected vehicle networks. Hence privacy preservation is highly required by trust management schemes. Using Table9 and Table 10, most of the surveyed approaches (30% of

TABLE 8. AI-based trust management schemes in VANETs.

Ref.	Class	Used metrics	Tools	Simulator	E. parameters
[86]	Clustering	Reputation, node proprieties	Defined formulas	Omnet++	CH's election time and duration, rate of malicious nodes elected as CH, delivery rate.
[87]		Knowledge, node proprieties	Defined formulas	Matlab-based	Trust metric value with dishonest vehicles.
[88]		knowledge	Learning ensemble	SUMO	Dishonest nodes detection rate, False Negatives, False positives, dishonest vehicles detection accuracy.
[89]		Reputation, Knowledge	Optimization colony	NS-2, MobiSim	Communication overhead, dishonest nodes detection rate, hops' number average, packet delivery rate, end to end delay.
[90]	Fuzzy Logic	Knowledge, Reputation	Defined formulas	NS-2, SUMO, MOVE	Behaviour of correlation, detection accuracy with and without collusion.
[91]		Knowledge, node proprieties	Fuzzy logic-based algorithm	NS-2, SUMO	Dishonest nodes detection rate, precision, Recall, accuracy.
[92]		Reputation, node proprieties	Mamdani Fuzzy Inference	MATLAB	Malicious nodes detection rate, accuracy
[93]		Reputation	Fuzzy logic,FT-OLSR	NS-2	Delay, packet delivery rate
[94]	Game theory	Knowledge	Bayesian inference filter	Matlab	Computation's time, compromised decision's rate
[95]		Reputation	Vickrey–Clarke–Groves, Neural Network	NS-3, SUMO	True positives, true negatives, false alarm rate,malicious nodes' detection rate.
[96]		Reputation	Defined formulas	Evolutionary game-theory model	Overall utility's growth rate, nodes' strategy change.
[97]		Reputation	K-means algorithm, fuzzy C-means clustering, defined factors	MobiSim, NS-2	Decision making's accuracy rate, throughput, false alarm's rate, forwarding rate, packet delivery delay.

mentioned papers) lack privacy protection. However, in [59], [62], [63], [64], [68], [77], [79], [80], [81], [90], [92], [93], and [94] authors paid significant attention to preserving the privacy of users' credentials.

2) DYNAMICITY

We notice that most of the referred schemes have fulfilled dynamicity criteria (i.e., lower infrastructure support, dynamic trust metrics, fast trust values update, etc.). Basically, major data-based models are more dynamic than entity-based models, where there is no requirement for extended exchanges between nodes to extract global trust. However, reputation-based models may conduct connection loss during the trust assessment of highly moving nodes.

3) SCALABILITY

Scalability is the ability of a VANET to accept an increasing number of communicating vehicles without any disruption or loss in data transferring or traffic loading. Also, it means the stability of the network with numerous malicious nodes. Some of the surveyed papers satisfied this requirement, as shown in Table 9 and Table 10.

4) COMPLEXITY

Estimating the time complexity in VANETs is crucial for dependable evaluation. The time of trust computation and its dissemination is essential in the surveyed approaches. In the IoV context, authors work on deriving the trust value immediately. A notable delay is presented in the calculation of direct trust. Also, with the presence of attackers in the

TABLE 9. Comparison of different surveyed trust management schemes in VANETs.

Ref.	Year	Category	Privacy	Dynamicity	Scalability	Complexity	Overhead	Efficiency
[58]	2019	Entity-based		✓		✓	✓	✓
[59]	2015			✓	✓			
[60]	2019		✓	✓		✓	✓	✓
[61]	2016			✓				✓
[62]	2014	Data-based		✓	✓			
[63]	2014		✓	✓		✓		✓
[64]	2012		✓	✓	✓	✓	✓	
[65]	2013		✓	✓		✓		✓
[66]	2014	Hybrid		✓		✓		✓
[67]	2015			✓	✓	✓	✓	✓
[68]	2016			✓	✓			✓
[69]	2013		✓	✓	✓			
[70]	2019	Cloud		✓				
[71]	2019			✓	✓	✓		✓
[72]	2017			✓		✓		✓
[73]	2017			✓				
[74]	2018	SDN		✓			✓	✓
[75]	2022			✓		✓	✓	✓
[76]	2016			✓		✓		
[77]	2020			✓		✓	✓	✓
[78]	2017	Fog/Edge	✓	✓		✓	✓	✓
[79]	2019			✓	✓		✓	✓
[80]	2020		✓	✓	✓	✓	✓	✓
[81]	2021		✓	✓	✓		✓	✓
[82]	2018	Blockchain	✓	✓			✓	✓
[83]	2021			✓				✓
[84]	2020			✓	✓			✓
[85]	2018			✓	✓	✓	✓	✓
[86]	2018	Clustering		✓	✓			✓
[87]	2019			✓	✓	✓	✓	✓
[88]	2020			✓			✓	✓
[89]	2021			✓		✓	✓	✓

TABLE 10. Continued Table.9.

Ref.	Year	Category	Privacy	Dynamicity	Scalability	Complexity	Overhead	Efficiency
[90]	2017	Fuzzy-Logic		✓	✓			✓
[91]	2021		✓	✓	✓		✓	✓
[92]	2022			✓	✓	✓	✓	✓
[93]	2019		✓	✓	✓	✓	✓	✓
[94]	2019	Game theory	✓	✓	✓		✓	✓
[95]	2018		✓	✓	✓			✓
[96]	2019			✓				✓
[97]	2019			✓			✓	✓

system, some detailed simulations in approaches showed that the detection rate of malicious nodes decreases due to the high density of the network.

5) OVERHEAD

The communication overhead must be considered for a dedicated evaluation of such approaches, as it defines the amount of transmitted data. The efficiency of the network depends on the communication overhead. The more it is high, the less the network is efficient. Hence, high consumption of the allocated bandwidth, delay in response time, etc. Some schemes introduced a reasonable forwarding rate by increasing the number of malicious nodes. But, authors in some surveyed approaches need to pay more attention to it. They deployed multiple technologies in one work, leading to high communication overhead and complexity.

6) EFFICIENCY

Evaluating the efficiency criteria is essential when inspecting such schemes. The system's efficiency means the security level and the resistance against security attacks. In this survey, we reviewed schemes as efficient when resistant to multiple common security attack types. We can notice, using Table 9 and Table 10, that most of the approaches using emerging technologies are efficient.

VII. FUTURE WORK

This section discusses some of the major challenges and possible future research directions in trust management in VANETs. We outline: Federated Learning-based solutions, Clustering approaches, energy consumption and emerging technologies.

A. FEDERATED LEARNING-BASED SOLUTIONS

Integration of the potential of Artificial Intelligence-enabled techniques in the trust management of VANETs brings more efficiency to the network. Federated Learning (FL) is a decentralized Machine Learning approach [97] that solves centralized training concerns. All network participants may contribute to the global model development without sharing data. In VANETs, participant nodes may not have the same roles. Therefore, FL will lead to robust trust formulas and models depending on distributed intelligent approaches with diverse parameters and metrics.

B. CLUSTERING APPROACHES

Since the trust management is decentralized, applying the paradigm of clustering [98] scheme serves in enhancing the reliability of the system specially when integrating emerging and decentralized technologies like SDN or Blockchain. These technologies will enhance the performance and th coordination between different Cluster Heads (CH) in the vehicular network.

C. ENERGY CONSUMPTION

With each new mechanism or technology deployment in the VANETs, the communication overhead and the complexity time increase directly, making it a very challenging task to deal with real-time application requirements. Hence, future researchers must pay attention to energy efficiency [99] when building trust management models. Such light-weighted approaches are recommended to reduce the system's energy consumption.

D. EMERGING TECHNOLOGIES

Deploying emerging technologies such as Cloud Computing, SDN, Edge/Fog Computing or Blockchain in trust management in VANETs will serve to enhance the performance of the system. These technologies provide a credible, dynamic, scalable and secure trust management. For instance, Cloud Computing and SDN lead the way to have a scalable, programmable and flexible system but future research needs to deal with the complexity time and overhead communication. Also, a localized processing is provided by the Fog/Edge Computing but integrating such technology will enlarge the circle of security and privacy attacks due to the

close interaction with users identities and sensitive informations (such as location, identity, etc..). So, this issue need to be addressed. With the Blockchain, all exchanged data is signed, verified and stored with resiliency and traceability. However, trust management Blockchain-based schemes present some issues with power consumption during the trust building process due to the block and consensus generation delays.

VIII. CONCLUSION

This extensive work has discussed the principal concepts of trust management in VANETs. Via this study, an efficient trust management approach design aims to find a suitable harmony regarding privacy, security, and quality of service. Unlike the above-mentioned surveys focused on this context, our paper illustrates proposed trust models' classes in VANETs. First, we represent a significant overview of ITS and VANETs and indicate the significance of security in this area. We discuss the necessity of building trust models for VANET communications. We also have discussed the security and trust management challenges in such networks and illustrated security attacks with related solutions. Then, we surveyed the existing trust basic management schemes (entity-based, data-based, hybrid) and exposed our taxonomy based on combined Artificial Intelligence (Clustering and Reinforcement Learning, Fuzzy Logic, Game Theory) and emerging technologies (e.g., Cloud, SDN, Fog/Edge Computing, Blockchain). After that, we summarized the surveyed schemes based on a set of criteria followed by a qualitative comparison. We have discussed four new research directions related to Federating Learning-based trust approaches, clustering approaches, energy consumption, and the impact of deploying emerging technologies in the trust models regarding scalability, overhead computation, and time complexity.

REFERENCES

[1] M. Ren, J. Zhang, L. Khoukhi, H. Labiod, and V. Veque, "A unified framework of clustering approach in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1401–1414, May 2018.

[2] P. Tyagi and D. Dembla, "Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2014, pp. 2084–2090, doi: 10.1109/ICACCI.2014.6968313.

[3] (2018). *Death on the Roads, Based on the WHO Global Status Report on Road Safety*. World Health Organization, Geneva, Switzerland. [Online]. Available: https://extranet.who.int/roadsafety/death-on-the-roads/deaths

[4] S. Zarbi, S. A. Mortazavi, and P. Salehpour, "Security analysis of an efficient authentication scheme for vehicular ad hoc networks," in *Proc. 17th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, Sep. 2020, pp. 44–47, doi: 10.1109/ISCISC51277.2020.9261912.

[5] M. Asghar, R. R. M. Doss, and L. Pan, "A scalable and efficient PKI based authentication protocol for VANETs," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–3, doi: 10.1109/ATNAC.2018.8615224.

[6] J. Zhang and Q. Zhang, "On the security of a lightweight conditional privacy-preserving authentication in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1037–1038, 2021, doi: 10.1109/TIFS.2021.3066277.

[7] B. Pooja, M. M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," in *Proc. Asia–Pacific Conf. Comput. Aided Syst. Eng. (APCASE)*, Feb. 2014, pp. 152–157, doi: 10.1109/APCASE.2014.6924490.

[8] B. K. Chaurasia, S. Verma, and G. S. Tomar, "Trust computation in VANETs," in *Proc. Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2013, pp. 468–471, doi: 10.1109/CSNT.2013.103.

[9] H. Sateesh and P. Zavarsky, "State-of-the-art VANET trust models: Challenges and recommendations," in *Proc. 11th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2020, pp. 0757–0764, doi: 10.1109/IEMCON51383.2020.9284953.

[10] H. Amari, L. Khoukhi, and L. H. Belguith, "Prediction and detection model for hierarchical software-defined vehicular network," in *Proc. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Sep. 2022, pp. 463–470, doi: 10.1109/LCN53696.2022.9843483.

[11] A. Kumar and M. Bansal, "A review on VANET security attacks and their countermeasure," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 580–585, doi: 10.1109/ISPCC.2017.8269745.

[12] T. Pavithra and B. S. Nagabhushana, "A survey on security in VANETs," in *Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2020, pp. 881–889, doi: 10.1109/ICIRCA48905.2020.9182823.

[13] N. Phull and P. Singh, "A review on security issues in VANETs," in *Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2019, pp. 1084–1088.

[14] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522–121531, 2021, doi: 10.1109/ACCESS.2021.3109264.

[15] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS.2021.3125521.

[16] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.

[17] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021, doi: 10.1109/TITS.2020.2973715.

[18] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019, doi: 10.1109/TITS.2018.2818888.

[19] A. Ahamed and H. Vakilzadian, "Issues and challenges in VANET routing protocols," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 0723–0728, doi: 10.1109/EIT.2018.8500180.

[20] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2017, doi: 10.1109/COMST.2017.2771522.

[21] G. M. Jinarajadasa and S. R. Liyange, "A survey on applying machine learning to enhance trust in mobile adhoc networks," in *Proc. Int. Res. Conf. Smart Comput. Syst. Eng. (SCSE)*, Sep. 2020, pp. 195–201, doi: 10.1109/SCSE49731.2020.9313021.

[22] M. Gillani, A. Ullah, and H. A. Niaz, "Trust management schemes for secure routing in VANETs—A survey," in *Proc. 12th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Nov. 2018, pp. 1–6, doi: 10.1109/MACS.2018.8628440.

[23] Z. Shafiq, M. H. Zafar, and A. B. Qazi, "QoS in vehicular ad hoc networks—A survey," *J. Inf. Commun. Technol. Robotic Appl.*, vol. 9, pp. 48–58, Jun. 2018.

[24] Z. Wang, Y. Wang, Y. Zhang, Y. Liu, C. Ma, and H. Wang, "A brief survey on cyber security attack entrances and protection strategies of intelligent connected vehicle," in *Proc. Int. Conf. Smart Comput. Commun.*, 2019, p. 73.

[25] I. Souissi, "Trust management in vehicular ad hoc networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 31, no. 4, pp. 230–243, 2019.

[26] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, "Security challenges, authentication, application and trust models for vehicular ad hoc network—A survey," *Int. J. Wireless Microw. Technol.*, vol. 7, no. 3, pp. 36–48, May 2017, doi: 10.5815/ijwmt.2017.03.04.

[27] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022, doi: 10.1109/ACCESS.2022.3198656.

[28] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, Oct. 2019, Art. no. 100179.

[29] Z. A. E. Houda, A. S. Hafid, and L. Khoukhi, "MiTFed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain," *IEEE Trans. Netw. Sci. Eng.*, early access, Jan. 16, 2023, doi: 10.1109/TNSE.2023.3237367.

[30] Z. A. El Houda, B. Brik, and L. Khoukhi, "Ensemble learning for intrusion detection in SDN-based zero touch smart grid systems," in *Proc. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Edmonton, AB, Canada, Sep. 2022, pp. 149–156, doi: 10.1109/LCN53696.2022.9843645.

[31] Z. A. El Houda, L. Khoukhi, and B. Brik, "A low-latency fog-based framework to secure IoT applications using collaborative federated learning," in *Proc. IEEE 47th Conf. Local Comput. Netw. (LCN)*, Edmonton, AB, Canada, Sep. 2022, pp. 343–346, doi: 10.1109/LCN53696.2022.9843315.

[32] Z. A. El Houda and L. Khoukhi, "A hierarchical fog computing framework for network attack detection in SDN," in *Proc. IEEE Int. Conf. Commun.*, May 2022, pp. 4366–4371, doi: 10.1109/ICC45855.2022.9838560.

[33] Z. A. El Houda, L. Khoukhi, and A. S. Hafid, "Bringing intelligence to software defined networks: Mitigating DDoS attacks," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 4, pp. 2523–2535, Dec. 2020, doi: 10.1109/TNSM.2020.3014870.

[34] Y. Fan, X. Xiao, and W. Feng, "An anti-jamming game in VANET platoon with reinforcement learning," in *Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW)*, May 2018, pp. 1–2, doi: 10.1109/ICCE-China.2018.8448435.

[35] S. S. Chhatwal and M. Sharma, "Detection of impersonation attack in VANETs using BUCK filter and VANET content fragile watermarking (VCFW)," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2015, pp. 1–5, doi: 10.1109/ICCCI.2015.7218093.

[36] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, Sep. 2013.

[37] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.

[38] D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of eavesdropping and DDoS attacks in VANET," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–8, doi: 10.1109/ICCCNT45670.2019.8944485.

[39] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020, doi: 10.1109/JIOT.2020.2967568.

[40] M. Hafiz, "A pattern language for developing privacy enhancing technologies," *Softw., Pract. Exper.*, vol. 43, no. 7, pp. 769–787, Jul. 2013.

[41] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8, doi: 10.1109/GLOCOMW.2007.4437823.

[42] A. M. N. Mejri and J. Ben-Othman, "GDVAN: A new greedy behavior attack detection algorithm for VANETs," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 759–771, Mar. 2017.

[43] G.-M. Hoang, B. Denis, J. Harri, and D. T. M. Slock, "Robust data fusion for cooperative vehicular localization in tunnels," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1372–1377, doi: 10.1109/IVS.2017.7995902.

[44] Z. Su, Y. Hui, T. H. Luan, Q. Liu, and R. Xing, "Reputation based content delivery in information centric vehicular networks," in *The Next Generation Vehicular Networks, Modeling, Algorithm and Applications*. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-56827-6_2.

[45] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2020, doi: 10.1109/TIFS.2020.3040876.

[46] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020, doi: 10.1109/ACCESS.2020.3034327.

[47] V. Laxmi, C. Lal, M. S. Gaur, and D. Mehta, "JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET," *J. Inf. Secur. Appl.*, vol. 22, pp. 99–112, Jun. 2015.

[48] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based gray-hole attack minimization for ad-hoc networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2174–2183, Aug. 2017, doi: 10.1109/TMC.2016.2622707.

[49] K. Stepien and A. Poniszewska-Maranda, "Analysis of security methods in vehicular ad-hoc network against worm hole and gray hole attacks," in *Proc. IEEE Int. Conf Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Dec. 2020, pp. 371–378, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00072.

[50] P. K. Singh, A. Agarwal, G. Nakum, D. B. Rawat, and S. Nandi, "MPF-SLP: Masqueraded probabilistic flooding for source-location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11383–11393, Oct. 2020, doi: 10.1109/TVT.2020.3009763.

[51] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," in *Proc. IEEE 3rd Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2020, pp. 394–398, doi: 10.1109/ICICSP50920.2020.9232047.

[52] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller, "Emerging attacks on VANET security based on GPS time spoofing," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 344–352, doi: 10.1109/CNS.2015.7346845.

[53] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA)," in *Proc. 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. (RAECS)*, Dec. 2015, pp. 1–5, doi: 10.1109/RAECS.2015.7453358.

[54] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access*, vol. 7, pp. 183532–183544, 2019, doi: 10.1109/ACCESS.2019.2960367.

[55] W. Ahmed and M. Elhadef, "Securing intelligent vehicular ad hoc networks: A survey," in *Advances in Computer Science and Ubiquitous Computing* (Lecture Notes in Electrical Engineering), vol. 474, J. Park, V. Loia, G. Yi, and Y. Sung, Eds. 2017, Singapore: Springer, 2017, p. 614.

[56] M. Azees, L. J. Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.

[57] H. Xia, S.-S. Zhang, Y. Li, Z.-K. Pan, X. Peng, and X.-Z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7108–7120, Jul. 2019, doi: 10.1109/TVT.2019.2919681.

[58] F. H. Al and N. Mohamed, "Similarity-based trust management system for detecting fake safety messages in VANETs," in *Internet of Vehicles—Safe and Intelligent Mobility* (Lecture Notes in Computer Science), vol. 9502, C. H. Hsu, F. Xia, X. Liu, and S. Wang, Eds. Cham, Switzerland: Springer, 2015, doi: 10.1007/978-3-319-27293-1_24.

[59] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6417–6428, Aug. 2019, doi: 10.1109/JIOT.2019.2895136.

[60] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017, doi: 10.1109/TVT.2016.2565001.

[61] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric rogue node detection in VANETs," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 398–405, doi: 10.1109/TrustCom.2014.51.

[62] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks: Intrusion-aware trust model for vehicular ad hoc networks," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1652–1669, Nov. 2014, doi: 10.1002/sec.862.

[63] R. A. Shaikh and A. S. Alzahrani, "Trust management method for vehicular ad hoc networks," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 115, K. Singh and A. K. Awasthi, Eds. Berlin, Germany: Springer, 2013, doi: 10.1007/978-3-642-37949-9_70.

[64] Y.-C. Wei and Y.-M. Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 393–400, doi: 10.1109/TrustCom.2012.79.

[65] Y.-C. Wei and Y.-M. Chen, "Adaptive decision making for improving trust establishment in VANET," in *Proc. 16th Asia–Pacific Netw. Oper. Manag. Symp.*, Sep. 2014, pp. 1–4, doi: 10.1109/APNOMS.2014.6996523.

[66] W. Li, K. Gong, Q. Li, F. Alber, and X. J. Zhou, "Hi-Corrector: A fast, scalable and memory-efficient package for normalizing large-scale Hi-C data," *Bioinformatics*, vol. 31, no. 6, pp. 960–962, 2015, doi: 10.1093/bioinformatics/btu747.

[67] B. Płaczek and M. Bernas, "Detection of malicious data in vehicular ad hoc networks for traffic signal control applications," in *Computer Networks* (Communications in Computer and Information Science), vol. 608, P. Gaj, A. Kwiecień, and P. Stera, Eds. Cham, Switzerland: Springer, 2016, doi: 10.1007/978-3-319-39207-3_7.

[68] Y. M. Chen and Y. C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, 2013.

[69] J. Pawlick, J. Chen, and Q. Zhu, "iSTRICT: An interdependent strategic trust mechanism for the cloud-enabled Internet of Controlled Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1654–1669, Jun. 2019, doi: 10.1109/TIFS.2018.2883272.

[70] B. K. Chaurasia and K. Sharma, "Trust computation in VANET cloud," in *Transactions on Computational Science XXXIV* (Lecture Notes in Computer Science), vol. 11820, M. Gavrilova and C. Tan, Eds. Berlin, Germany: Springer, 2019, doi: 10.1007/978-3-662-59958-7_5.

[71] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017, doi: 10.1109/ACCESS.2017.2670024.

[72] S. S. Mudengudi and M. S. Kakkasageri, "Establishing trust between vehicles in vehicular clouds: An agent based approach," in *Proc. Int. Conf. Smart Technol. For Smart Nation (SmartTechCon)*, Aug. 2017, pp. 529–533, doi: 10.1109/SmartTechCon.2017.8358428.

[73] D. Zhang, F. R. Yu, and R. Yang, "A machine learning approach for software-defined vehicular ad hoc networks with trust management," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647426.

[74] D. Zhang, F. R. Yu, and R. Yang, "Software-defined vehicular networks with trust management: A deep reinforcement learning approach," *IEEE Trans. Intell. Transp.*, vol. 23, no. 2, pp. 1400–1414, Feb. 2022, doi: 10.1109/TITS.2020.3025684.

[75] D. Zhang, F. R. Yu, Z. Wei, and A. Boukerche, "Software-defined vehicular ad hoc networks with trust management," in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, 2016, p. 4149.

[76] L. Alouache, M. Maachaoui, and R. Chelouah, "Securing hybrid SDN-based geographic routing protocol using a distributed trust model," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 5, no. 2, pp. 567–577, 2020.

[77] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[78] F. Dewanta and M. Mambo, "Bidding price-based transaction: Trust establishment for vehicular fog computing service in rural area," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 882–887, doi: 10.1109/PERCOMW.2019.8730830.

[79] S. A. Soleymani, S. Goudarzi, M. H. Anisi, N. Kama, S. A. Ismail, A. Azmi, M. Zareei, and A. Hanan Abdullah, "A trust model using edge nodes and a cuckoo filter for securing VANET under the NLoS condition," *Symmetry*, vol. 12, no. 4, p. 609, Apr. 2020, doi: 10.3390/sym12040609.

[80] R. J. Atwa, P. Flocchini, and A. Nayak, "A fog-based reputation evaluation model for VANETs," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2021, pp. 1–7, doi: 10.1109/ISNCC52172.2021.9615820.

[81] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[82] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu, "Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–6, doi: 10.1109/WCNC49053.2021.9417347.

[83] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021, doi: 10.1109/JIOT.2020.3044296.

[84] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019, doi: 10.1109/JIOT.2018.2836144.

[85] S. Oubabas, R. Aoudjit, J. J. Rodrigues, and S. Talbi, "Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme," *Veh. Commun.*, vol. 13, pp. 128–138, Jul. 2018.

[86] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A hybrid trust management heuristic for VANETs," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 748–752, doi: 10.1109/PERCOMW.2019.8730675.

[87] F. A. Ghaleb, F. Saeed, M. Al-Sarem, B. A. S. Al-Rimy, W. Boulila, A. E. M. Eljialy, K. Aloufi, and M. Alazab, "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, no. 9, p. 1411, 2020, doi: 10.3390/electronics9091411.

[88] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, Jul. 2021, doi: 10.1109/TITS.2020.3041746.

[89] S. A. Soleymani, A. H. Abdullah, M. Zareei, and M. H. Anisi, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, 2017, doi: 10.1109/ACCESS.2017.2733225.

[90] M. M. Hasan, M. Jahan, S. Kabir, and C. Wagner, "A fuzzy logic-based trust estimation in edge-enabled vehicular ad hoc networks," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Jul. 2021, pp. 1–8, doi: 10.1109/FUZZ45933.2021.9494428.

[91] C. Gomathy, "Fuzzy based trusted communication in vehicular ad hoc network," in *Proc. 2nd Int. Conf. Intell. Technol. (CONIT)*, Jun. 2022, pp. 1–4, doi: 10.1109/CONIT55038.2022.9847823.

[92] Y. Inedjaren, B. Zeddini, M. Maachaoui, and J.-P. Barbot, "Securing intelligent communications on the vehicular adhoc networks using fuzzy logic based trust OLSR," in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2019, pp. 1–6, doi: 10.1109/AICCSA47632.2019.9035241.

[93] T. Halabi and M. Zulkernine, "Trust-based cooperative game model for secure collaboration in the Internet of Vehicles," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8762069.

[94] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi layered intrusion detection framework for VANET," *Future Gener. Comput. Syst.*, vol. 82, pp. 12–28, May 2018.

[95] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of Internet of Vehicles based on evolutionary game theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5971–5980, Jun. 2019, doi: 10.1109/TVT.2019.2910217.

[96] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101740.

[97] A. Haddaji, S. Ayed, and L. Chaari, "Federated learning with blockchain approach for trust management in IoV," in *Advanced Information Networking and Applications* (Lecture Notes in Networks and Systems), vol. 449, L. Barolli, F. Hussain, and T. Enokido, Eds. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-030-99584-3_36.

[98] G. Khayat, C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla, H. Maalouf, and E. Pallis, "VANET clustering based on weighted trusted cluster head selection," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 623–628, doi: 10.1109/IWCMC48107.2020.9148339.

[99] H. N. Abdulrazzak, N. M. L. Tan, and N. A. Mohd, "Minimizing energy consumption in roadside unit of zigzag distribution based on RS-LS technique," in *Proc. IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS)*, Jun. 2021, pp. 169–173, doi: 10.1109/I2CACIS52118.2021.9495853.

HOUDA AMARI received the engineering degree in computer networking and telecommunications from the Private School of Applied Science and Technology of Gabes, Tunisia, and the bachelor's degree in computer science and multimedia from the Higher Institute of Computer Science and Multimedia Gabes, Tunisia. She is currently pursuing the Ph.D. degree with the University of Caen Normandie, France, and the University of Sfax, Tunisia. Her current research interests include vehicular ad-hoc networks (VANETs), SDN, and DDoS.

ZAKARIA ABOU EL HOUDA (Member, IEEE) received the M.Sc. degree in computer networks from Paul Sabatier University, Toulouse, France, in 2017, the Ph.D. degree in computer science from the University of Montreal, Montreal, QC, Canada, in 2021, and the Ph.D. degree in computer engineering from the University of Technology of Troyes, Troyes, France, in 2021. His current research interests include applied machine/deep learning for intrusion detection systems, security of distributed machine learning, and blockchain for network security.

LYES KHOUKHI (Senior Member, IEEE) received the Ph.D. degree in computer engineering from the University of Sherbrooke, Canada, in 2006. From 2007 to 2008, he was a Researcher with the Department of Computer Science and Operations Research, University of Montreal, in collaboration with Bell-Canada. In 2008, he also worked with Dialexia Corporation-Montreal, in the development of safe communications solutions. In 2009, he joined the University of Technology of Troyes, France, as an Assistant Professor. Since 2020, he has been a Full Professor with the GREYC, CNRS, UMR 6072 Laboratory/SAFE Team, ENSICAEN, University of Caen Normandie, Caen, France. His research interests include attacks detection and prediction and malicious behaviors modeling. His target areas are the IoT, V2X, and SDN/5G. He has participated as the general chair, program chair, or TPC member of many conferences. He served as the Symposium Chair for IEEE LCN, in 2019; the Co-Chair for the IEEE LCN on-move for several years, from 2013 to 2018, and QoSQoE of IWCMC, from 2017 to 2019; and the General Chair for NOTERE' 16 (13ème Francophone Conference, in 2016) and UBIROADS'2012. He is the General Chair of IEEE LCN 2022, the Program Co-Chair of LCN'20 and CyberWorlds'21, and the Symposium Chair of Globecom'21 (track mobile and wireless networks). He is also the Guest Editor of *Annals of Telecomunications* (Springer) of the SI (Internet of Vehicles and Smart City), in 2020, about security and protocols issues in V2X. He has been the SIG Leader of ''Machine Learning for IoT and Ad Hoc Networks'' of the IoT ASHN ComSoc Committee of IEEE Communications Society, since 2020.

LAMIA HADRICH BELGUITH received the Diploma (master's) degree in computer science from the Faculty of Economics and Management of Sfax (FSEGS), University of Sfax, Tunisia, in 1990, the master's degree in management information systems from the High School of Management-Tunis (ISG), in 1992, and the Ph.D. degree from the Faculty of Sciences of Tunis, Tunisia, in 1999. She has been teaching at the Department of Computer Science, FSEGS, since 1992. Since 2015, she has been a Full Professor of computer science and the Director of the Doctoral School EGI, FSEGS, University of Sfax. She is also the Head of the Arabic Natural Language Processing Research Group (ANLP-RG) and the Co-Director of the Multimedia, Information Systems, and Advanced Computing Laboratory (MIRACL). Her research interests include Arabic text analysis, automatic abstracting, question-answering systems, and human–machine spoken dialog systems. She served as a reviewer for many national and international journals, conferences, and projects.