frontiers | Frontiers in The Internet of Things

TYPE Review
PUBLISHED 31 October 2022
DOI 10.3389/friot.2022.995233

OPEN ACCESS

EDITED BY
Chang-ai Sun,
University of Science and Technology Beijing, China

REVIEWED BY
Muhammad Asghar Khan,
Hamdard University, Pakistan
Ming Xu,
Hangzhou Dianzi University, China

*CORRESPONDENCE
Yucong Duan,
duanyucong@hotmail.com

SPECIALTY SECTION
This article was submitted to IoT Architectures, a section of the journal Frontiers in the Internet of Things

RECEIVED 15 July 2022
ACCEPTED 18 October 2022
PUBLISHED 31 October 2022

CITATION
Che H, Duan Y, Li C and Yu L (2022), On trust management in vehicular ad hoc networks: A comprehensive review. *Front. Internet. Things* 1:995233. doi: 10.3389/friot.2022.995233

On trust management in vehicular ad hoc networks: A comprehensive review

Haoyang Che[1], Yucong Duan[2]*, Chen Li[1] and Lei Yu[3]

[1]User Digitization Department, Zeekr Group, Hangzhou, China, [2]College of Computer Science and Technology, Hainan University, Haikou, China, [3]Department of Computer Science, Inner Mongolia University, Hohhot, China

Security issues have always posed a major threat and challenge to the Internet of Things (IoTs), especially the vehicular ad-hoc networks (VANETs), a subcategory of IoTs in the automotive field. The traditional methods to solve these ever-growing security issues in VANETs are mainly cryptography-based. As an effective and efficient complement to those solutions, trust management solutions and reputation models have been widely explored to deal with malicious or selfish vehicle intrusion and forged data spoofing, with the aim of enhancing the overall security, reliability, trustworthiness, and impartiality of VANETs. For the integrity of the article, this survey begins with providing the background information of VANETs, including the basic components and general architecture. Then, many attacks in VANETs are investigated, analyzed, and compared to understand the functional relevance of the following trust and reputation methods. Various approaches offer various countermeasures against these types of attacks. At the same time, the latest development of emerging technologies such as blockchain, software-defined network, and cloud computing opens up new possibilities for more and more promising trust and reputation management models and systems in VANETs. After that, the survey reviews the most important trust and reputation models and schemes which are widely mentioned in the literature based on our developed technique-based taxonomy, in contrast to the popular "entity-centric, data-centric, hybrid" taxonomy in the field, to adapt to the recent technological development of these management schemes in VANETs. Finally, discussions and speculations on the future direction of research into the trust and reputation management in VANETs are presented.

KEYWORDS

VANET, trust management, trust model, privacy preservation, reputation management

1 Introduction

As a critical component of intelligent transportation system (ITS), VANET is regarded as a key solution to reduce and eliminate existing energy consumption and traffic congestion problems by generating and disseminating messages about road conditions, such as traffic jams during rush hours, temporary road congestions, urgent road accidents, and short-term roadside repair at intersections. Many efforts

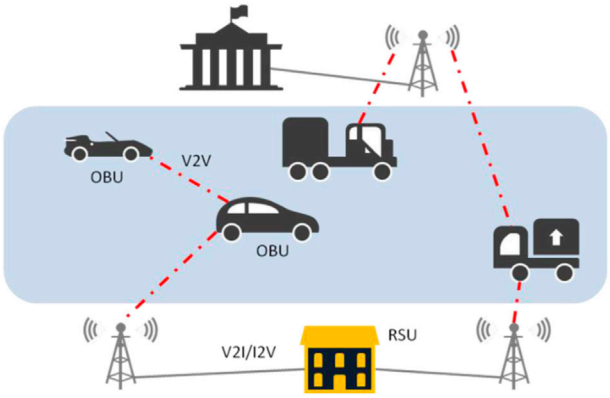


FIGURE 1
The general VANET architecture.

have been spent on the development of such systems in VANETs delivering reliable and secure messages among vehicles, such as safety message sharing (Xu et al., 2004), traffic view systems (Nadeem et al., 2004), cooperative collision warning (Elbatt et al., 2006), and secure crash reporting (Rahman and Hengartner, 2007). Moreover, some car manufacturers like GM have even rolled out proprietary algorithms to collect the position, speed and course of nearby cars and issue a warning to the driver when a crash is imminent (GM, 2016).

Essentially, VANETs (Mejri et al., 2014) are wireless ad-hoc networks of which nodes consist of vehicles equipped with on-board units (OBUs) and fixed road-side units (RSUs), as depicted in Figure 1. In VANETs, vehicles can exchange data and messages with other vehicles (V2V, Vehicle-to-Vehicle), or with RSUs (V2I, Vehicle-to-Infrastructure/I2V, Infrastructure -to- Vehicle), or with pedestrians walking on the street (V2P, Vehicle-to-Person/V2H, Vehicle-to-Human) (see Table 1).

Each in-motion vehicle and the corresponding RSUs simultaneously form a temporary self-organizing network. The VANET allows vehicles and RSUs to periodically transmit their surrounding road conditions (such as road congestion, accident condition, and traffic lights) and vehicle conditions (such as vehicle direction, location, and speed) to other vehicles within their communication ranges through a multi-hop mode, which can not only help improve road safety, but also have an effect on guiding the traffic flow. OBUs are employed by vehicles to communicate and exchange messages with other vehicles and RSUs, like their vehicles' GPS location data, acceleration or deceleration information, brake information, etc.

Broadcasting road information may help vehicles to be aware of the current situation on the road. However, on the opposite side of the coin, intentionally or unintentionally falsified information may cause various consequences, thus securing VANETs becomes very important (Raya and Hubaux, 2005a; Raya et al., 2006). An old and expired notification transmitted by an unintentional vehicle may misdirect the entire traffic and cause the following traffic jam. Moreover, even in the extreme settings, misled information offered by some deliberate vehicles may often lead to life-threatening dire consequences, which poses a number of unique challenges (Parno and Perrig, 2005). If VANETs are to be deployed and applied on a large scale, security, trust, and privacy issues must be addressed in the first place, such two-facet problems have gained remarkable attention and technological development over the last few years. Traditional centralized cryptographic solutions may adapt to addressing security issues like data confidentiality, data integrity, authentication, authorization, and access control. A node (a vehicle) might pass the traditional cryptographic hard security checks, but still be threatened by some other kind of security problems. Trust and reputation-based approaches are devised to detect the internal nodes' physical capture, malicious or selfish behaviors, which are not always so easy to tackle for traditional security schemes. Furthermore, trust and reputation management systems (TRMs) can assist VANETs in uncertain decision-making processes. Overall, TRMs need to tackle three-fold issues which are equally important to support secure communication in VANETs:

TABLE 1 Typical components in a VANET setting and deployment.

Name	Type	Function
Vehicle	Unit	Vehicles are equipped with GPS (Global Positioning System), RFID (Radio Frequency IDentification), RADAR for positioning, identification, and message transmissionetc.
OBU	Unit	A communication device installed on the vehicle, allows for DSRC (Dedicated Short-Range Communication) communications with other OBUs or RSUs
RSU	Unit	A communication unit that is located on the roadside and serves as a gateway between the OBUs and the communication infrastructure
V2V	Communication	Vehicles send and receive messages to and from each other
V2I	Communication	Vehicles can be connected to the infrastructure for some services
V2P	Communication	Vehicles send and receive messages to and from pedestrians walking on the street.

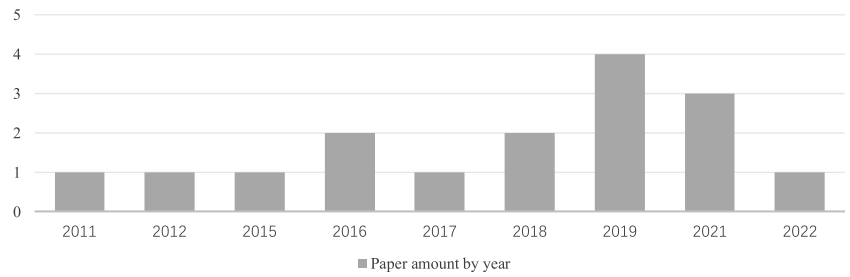


FIGURE 2
Number of published survey papers in VANETs by year.

1. Unreliable messages generated and broadcasted by malicious or benevolent vehicles;
2. Unreliable vehicles as information generators or disseminators;
3. Unreliable human drivers or passengers as information generators or disseminators.

1.1 Previous surveys

Trust is a multidisciplinary concept and has been well-studied from different perspectives for several decades. In the mobile Internet era, research on trust, especially trust management in distributed scenarios gains more and more attention from both academia and industry. Many survey papers that classify and summarize trust management papers have emerged in quite a few research fields, such as MANETs, IoTs, SNS (Social Networking Services), and also VANETs. We used the following query strings on IEEE Xplore Digital Library, ACM Digital Library, and DBLP. com:

- {"trust" or "reputation"} + {"survey" or "review" or "challenges" or "overview"} + {"VANET" or "VANETs" or "internet of vehicles" or "vehicular network" or "vehicular ad hoc network"}

And we combined the searched papers and excluded some irrelevant papers, and finally we obtained about 16 strongly correlated survey papers (from 2011 to the writing of this paper), as shown in Figure 2. Among all these papers, the paper titled "A survey of trust management in the Internet of Vehicles" (Hbaieb et al., 2022) is the most well-written and comprehensive one. The paper systematically summarizes and reviews several topics including the notion of trust, the existing surveys about vehicular security, the security and trust attacks and challenges in vehicular contexts, the most relevant approaches related to trust management in VAENTs, and the trust enabling technologies like blockchain, cloud, and SDN. Mikavica and Kostic-jubisavljevic (2021) surveyed recent blockchain-based trust model advancements in VANETs. Overall, this survey paper is one of the few overview articles focusing on one particular aspect as the topic of discussion.

Similar to other survey papers, the main objective of this survey is to categorize, analyze, and synthesize the research papers on trust management in VANETs, in order to present a summary of the research works done in this area (*cf.* Table 2). By filling in the gaps and providing the most recent VANETs advancements while keeping it self-explanatory, this survey can prevent overlap with existing surveys. Different from the popular "entity-centric, data-centric, hybrid" taxonomy chosen by most survey papers in this field of research, we chose the most intuitive taxonomy, i.e., a technique-based classification method. To the best of our knowledge, this may be the first survey paper that chooses this particular classification method. In addition to this point, the paper also gives a comparatively comprehensive summarization of security attacks in VANETs.

1.2 Survey organization

In this survey, we aim to provide a systematic review of recent advancements on trust and reputation management in the field of VANET. The organization of the survey is presented in Figure 3 with a top-down layout. Section 1 gives a brief introduction of the background information and the comparison with the previous surveys. Following that, in Section 2, we discuss several forms of attacks in VANETs, and then in Section 3, we rapidly introduce the notion of trust and reputation management and explain why it is useful for addressing VANET security issues. Section 4 presents the intrinsic challenges towards VANET scenarios. Afterwards, in Section 5, we classify the different types of trust and reputation models and schemes we have identified in the literature, and elaborate the trust and reputation management solutions from a technological perspective in more detail. Finally, we discuss future research directions on trust management in Section 6. Section 7 concludes the paper in a nutshell.

TABLE 2 Recent surveys on trust management in VANETs.

Ref	Year	Basic content
Hbaieb et al. (2022)	2022	comprehensively surveyed the literature about the trust management topic in vehicular environments
Mahmood et al. (2021)	2021	discussed the convergence of the notion of trust with the IoV (Internet of Vehicles)
Mikavica and Kostic-jubisavljevic, (2021)	2021	reviewed some of recent blockchain-based trust models in VANETs
Hussain et al. (2021)	2021	reviewed the recently proposed trust establishment and management mechanisms (from 2014 to 2019) in VANETs
El-Sayed et al. (2019)	2019	provided a review of the research efforts aimed at enabling trust evaluation, aggregation, propagation, and decision making in vehicular environments
Iqbal et al. (2019)	2019	presented a brief review of the trust models that have the potential to be implemented in Social Internet of Vehicles
Lu et al. (2019)	2019	provided an in-depth review of anonymous authentication schemes implemented by five pseudonymity mechanisms and also gave a comprehensive analysis on various trust management models in VANETs
Souissi et al. (2019)	2019	surveyed the recent advances in trust management for VANETs and showed the importance of an adaptive trust model for each class of applications
Gillani et al. (2018)	2018	presented a comprehensive overview of trust management schemes for routing protocols in VANETs
Sumithra and Vadivel, (2018)	2018	reviewed trust establishment mechanisms so far
Vaibhav et al. (2017)	2017	discussed various issues related to security challenges, security architecture actors, security authentication, application constraints, various trust models in VANETs. trust models etc
Premasudha et al. (2016)	2016	provided a comprehensive survey of security threats, two types of security schemes, and trust management schemes
Kerrache et al. (2016)	2016	provided an adversary-oriented survey of the existing trust models for VANETs and showed trust model evaluation criteria in VANET contexts
Soleymani et al. (2015)	2015	presented a systematic review of the literature between 2005 and 2014 about different trust conceptions, ideas, issues, and solutions in VANETs
Zhang, (2012)	2012	surveyed and evaluated existing trust models in VANETs, pointed out that none of the trust models had achieved all the properties of VANET environments
Zhang, (2011)	2011	examined current trust models in MANETs, VANETs, and multi-agent systems, and recommended desired characteristics for efficient trust management in VANETs

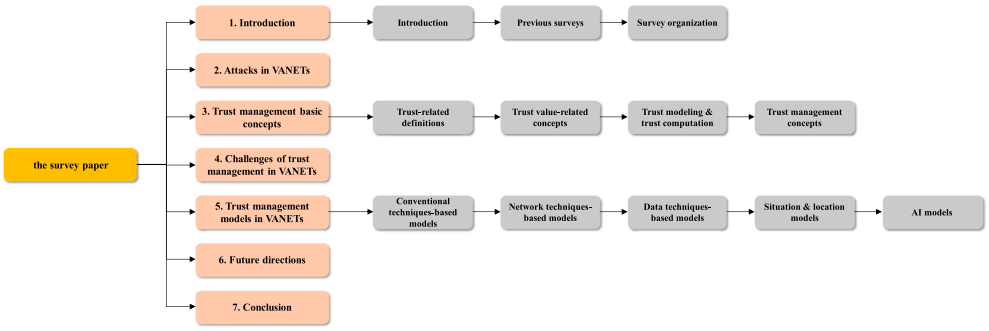


FIGURE 3
The organization of the survey.

2 Types of attacks in VANETs

In order to combat many realistic threats in the intricate vehicular scenarios, trust and reputation-based mechanisms have emerged in VANETs. Vehicles can be easily vulnerable to illegal information injection, malicious messages, falsification, and node impersonation, both inside and externally, due to the enormous volume and very dynamic topology of VANETs. We must first recognize the potential attack types and their behaviors exist in VANETs, so as to comprehend the security issues and remedial measures against them (Sumra et al., 2011a). In terms of privacy, security, and trust, these attacks will make it extremely difficult to develop secure VANET schemes. As a result, in this section we provide a taxonomy of security attacks and problems in VANETs, as shown in Table 3. Also, Figure 4 presents a clear taxonomy of security attacks in an intuitive way.

TABLE 3 Various types of attacks in VANETs.

Attack Name	Security Requirement	Description
DoS Attack Hamieh et al. (2009); Verma et al. (2013); Bragagnolo et al. (2019)	Availability	In DoS (Denial of Service) assaults, attackers flood the VANET network with a high number of fictitious or altered messages in an effort to block communication channels and eat up a lot of other nodes' computer power. As a result, communication capabilities may be severely compromised, making it difficult to react swiftly and increasing the risk of dangerous road accidents. The jamming assault is a unique type of denial-of-service attack that interferes with the radio transmission channel by using a powerful signal of an analogous frequency (Hamieh et al., 2009). Additionally, some well-known DoS attacks can be discovered in the literature are JellyFish (Aad et al., 2004), intelligent cheater (Pathan, 2011), and flooding attacks
DDoS Attack Biswas et al. (2012); Pathre et al. (2013)	Availability	DDoS (Distributed DoS), commonly referred to as a flood attack, is a significant DoS attack that will lower the VANET network's overall QoS (Quality of Service)
Wormhole Attack Hu et al. (2003)	Availability	An attacker in a VANET has the ability to tunnel packets broadcast in one area to another location if he has control over at least two entities that are remote from one another and the high-speed communication link that connects them
Tunnel attack	Availability	a.k.a. Wormhole Attack (Hu et al., 2003)
Black Hole Attack Baiad et al. (2014)	Availability	In order to establish routing links, the attacker uses this technique to spread bogus routing information and trick other nodes. The attacker can manage the data transmission and only forward the data he wants to deliver after successfully establishing the routing link
Gray Hole Attack Ya et al. (2015); Sheikh and Liang, (2019)	Availability	This attack, also known as a node misbehaving attack, deceives the network by agreeing to forward packets. The attacker will throw away packets it has received from nearby nodes. A variation of the black hole attack is the gray hole attack
Timing Attack Arsalan and Rehman, (2018); Sumra et al. (2011b)	Availability	The primary goal of the attacker in this attack is to insert some time slots into the original message in order to delay the original message, and these messages are received later. Safety applications, as we all know, are time-sensitive, and if these applications are delayed, their primary objectives are also severely harmed
GPS Spoofing Attack Al-kahtani, (2012); Bittl et al. (2015)	Availability	Spoofing attack, also known as a tunnel attack, tricks GPS receivers in the area into thinking that their coordinates are different from where they actually are. The GPS satellite simulator's signal is stronger than the actual satellite system's signal Al-kahtani, (2012)
Position Spoofing Attack Sakiz and Sen, (2017); Ercan et al. (2022)	Availability	By broadcasting the incorrect position information in the safety warnings, the attacker imitates the "ghost car" on the road
Selective Forwarding Attack Wang and He (2016)	Availability	In this attack, a malicious node impersonates a benign node, purposefully discards data packets, compromises data integrity, and impairs the performance of legitimate VANET applications
Malware Attack Al-kahtani, (2012); Dhamgaye and Chavhan, (2013)	Availability	In such an attack, the attacker infiltrates the VANET network with the aid of OBUs and RSUs, leading to catastrophic system failure
Zig-Zag Attack Ahmad et al. (2021)	Availability	Attackers will employ random patterns to conceal their true objectives in what are also referred to as "on-off" attacks. They will initially act normally in order to build up sufficient confidence inside the network. They will conduct harmful attacks and impose bogus trust ratings on their neighboring vehicles after they have been approved by the network
Sybil Attack Guette and Ducourthial, (2007); Hao et al. (2011)	Authentication	A miscarriage of justice will result from the attacker who begins the Sybil attack creating several virtual vehicles on the road that all have the same identification. Even the attacker can transmit some fake communications using virtual vehicles to further his own goals. According to the antenna type, transmission signal intensity (Guette and Ducourthial, 2007), motion trajectories (Chen et al., 2009), and nearby vehicles (Hao et al., 2011), among other factors, the Sybil attack can be identified
Man-in-the-middle Attack (MiMA) Al-kahtani, (2012)	Authentication	The communication between vehicles is simple to observe due to VANET's openness. Attackers can use their own communications as a substitute for other vehicles to mimic them as usual. The interchange and dissemination of information can be easily controlled by man-in-the-middle attackers, which is a very serious danger to VANET. For instance, an attacker may alter a security message's content after receiving it and send a spoofed message to nearby vehicles informing them that danger is impending and requesting that they take a different route
Node Impersonation Raghav et al. (2013)	Authentication	An attacker can assume a different identity and pose as the message's real sender in a node impersonation attack

(Continued on following page)

TABLE 3 (*Continued*) Various types of attacks in VANETs.

Attack Name	Security Requirement	Description
Replay Attack Sakiz and Sen, (2017)	Authentication	In a replay attack, the attacker broadcasts previously obtained accurate information to the network again, leading to the dissemination of false information to other communication nodes or the destruction of the network's routing rules
Message Tampering Attack Sheikh and Liang, (2019)	Authentication	By keeping an eye on the wireless channel, the attacker can intercept the desired message and change it to its own advantage or purposefully delay its transmission. Many other attacks, including man-in-the-middle and node impersonation attacks, use message tampering as a method
Trust-distortion Attack Movahedi et al. (2016)	Authentication	Trust management mechanisms can be used by new VANET attacks (Movahedi et al., 2016). Nodes can be tricked into accepting inaccurate estimates of the reliability of other nodes by manipulating the trust computation
Eavesdropping Sheikh and Liang, (2019)	Confidentiality	Both stationary and moving vehicles are capable of conducting eavesdropping operations. Attackers can gather details about other vehicles on the network by eavesdropping without the knowledge of other vehicle users
Privacy Violation Sheikh and Liang, (2019)	Confidentiality	Attackers in the VANET typically link the location and identification data gathered by the vehicle, thus compromising the privacy of users
Social Attack Sheikh and Liang, (2019); Raya & Hubaux, (2005b)	Confidentiality	In this attack, the attacker distracts the drivers' attention and influences their driving behaviors and decision-making processes by sending them unethical messages

The above-listed attacks may affect the normal operation of VANETs and many methods are proposed to tackle these attacks in an efficient way. Among these, cryptography-based solutions play an important role in solving traditional security problems, however, due to the intrinsic characteristics of VANETs, these solutions will not suffice to deal with all the attacks. Therefore, the importance of the concept of trust management is obvious. Security problems like fake messages and dishonest users will exceed the capabilities of traditional cryptography-based solutions (Hussain et al., 2021). The goal of incorporating trust is to detect malicious entities and their deceptive information, actively encourage those entities with good behavior and honesty, and prevent dishonest and selfish behaviors among entities. In the next section, for the purpose of the integrity of the survey, we will briefly introduce trust and reputation management, as a fundamental basis for later discussion.

3 Trust and reputation management

Trust is a fundamental tool in human life. It enables people to communicate, coordinate, collaborate, and protect themselves. As equivalents in virtual world, trust and reputation have been discussed, studied, and applied in many other fields, such as P2P network, IoTs, Wireless Sensor Networks (WSNs), and Mobile Ad-hoc Networks (MANETs), even in deployed hardware environments. In order to understand the trust and reputation management approaches presented in this survey, we introduce the basic concepts surrounding trust and reputation management in this section. In addition, through the rest of the survey, we will use the words parties, participants, entities, nodes, or peers interchangeably, as we will do with messages, information, and contents.

3.1 Trust, distrust, and reputation

Trust and reputation are two closely related terms, which often appear in the literature in twin at the same time. At the earliest, they are rooted in sociology and psychology, despite the fact that we are not concerned and interested in their origins.

Trust is defined as the degree to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved. A trust relationship always involves two entities: the trustor and the trustee. The trustor is the party who gives the trust, and the trustee is the party who accepts the trust. The trustor, based on his observation of the trustee, makes a trust decision on the balance between risk and trust in the trustee, and authorizes participation in a binary manner. The opposite of trust is distrust. Sometimes, mistrust also describes the extent to which the trustor does not trust the trustee.

Trust may have many binary attributes or properties of entities, such as direct vs indirect, subjective vs objective, local vs global, symmetric vs asymmetric, historical vs current, static vs dynamic (*cf.* Figure 5). Many methods proposed in the literature are built up around these attributes.

Because of some inherent attributes of trust, trust is easily confused with reputation, and is often used interchangeably in the research literature. Reputation refers to a partys perception of its intention and norms through past actions (Lik et al., 2002). Reputation comes from a community in which members can observe their past behaviors, and members must agree on their shared views on each given party in the community. The most important differences between trust and reputation are:

- Trust is a subjective expectation of trustworthiness calculated based on previous experiences among

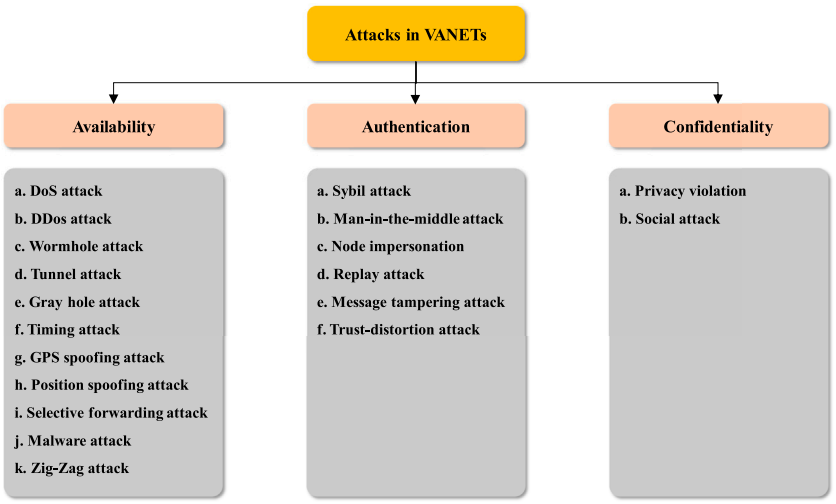


FIGURE 4
Attacks in VANETs.

entities, while reputation is a holistic objective measure of credibility among entities;
- Trust is transitive, while transitivity is rarely considered in reputation modeling;
- Trust is more an active one-to-one judgment of future actions, while reputation is a many-to-one assessment over a period of time;
- Reputation is almost always associated with the concept of recommendation, because an entity reputation is based on the direct or indirect recommendation of other entities in the same network.

Reputation lays the foundation for establishing trust relationships and adopting trust management. In terms of modeling and computing, trust is a more complex concept than reputation.

3.2 Trust value, trust degree, and trust metrics

In order to calculate the degree of trust towards a trustee by a trustor, the trust itself must be quantifiable and computable. When the model assumes whether a trustee is trusted or not, i.e., the model treats the trust in a binary mode, the corresponding trust value will be 1 (trust) or 0 (not trust). When the model calculates the probability or belief that the trustee can be trusted, the trust value for the trustee will be represented as a continuous value or a discrete value between 0 and 1, to represent the degree of trust from completely distrust, partial trust, till to full trust.

Trust metrics are metric parameters used in trust evaluation, according to different design aspects (such as knowledge, node properties, proximity, environment factors, etc.) and design purposes (such as accuracy, dynamicity, scalability, etc.). For example, in proximity-based metrics, the main deployed parameters are time, location, and the distance of the desired entities.

3.3 Trust modeling and trust computation

As mentioned above, the concept of trust is easy to comprehend. The conceptualization of trust modeling and trust computation is based on the basic concepts and metrics of trust. Trust modeling formally defines the trust relationships between entities, and maps the trust entities and relationships to a computational model composed of trust metrics. And trust computation is the process to compute the trust value or the trust degree during the interactions, which is composed of multiple phases (*cf.* Figure 6).

1. Trust bootstrapping: Trust bootstrapping is the trust establishment phase in which initial trust values are assigned in the network.
2. Trust propagation: This phase refers to the process of propagating trust through entities following the principles of trust transitivity and trust fusion.
3. Trust aggregation: Trust aggregation denotes that trust values propagated through different trust paths should be aggregated according to some fusion algorithms.

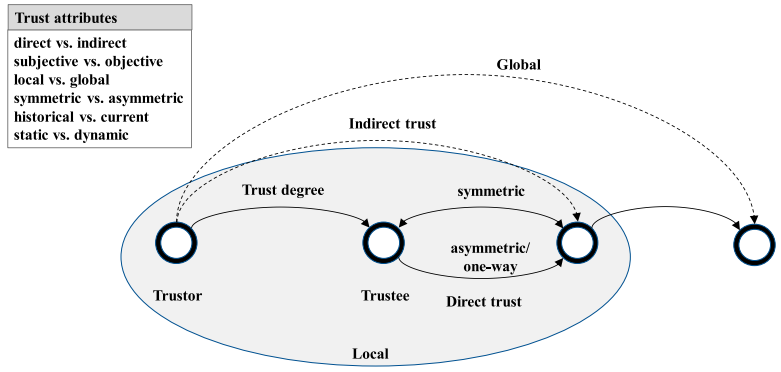


FIGURE 5
Trust attributes.

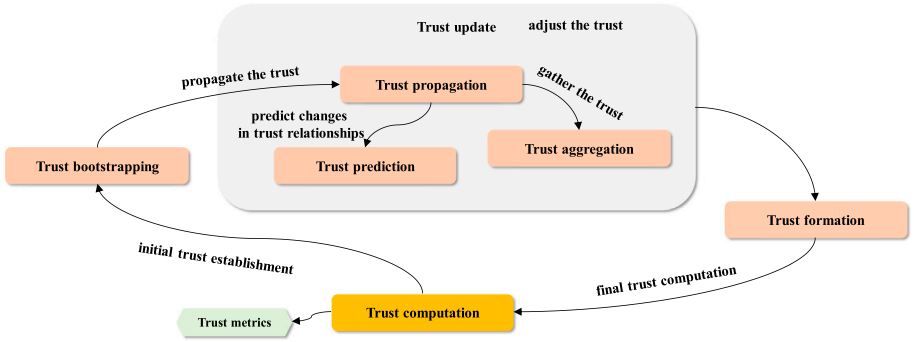


FIGURE 6
Trust computation phases.

Trust propagation and trust aggregation together are called trust inference.

4. Trust update: Trust update refers to updating trust values over time, iterations, or event triggers.
5. Trust prediction: Trust prediction aims to predict the future trust relationships between entities.
6. Trust formation: The formation phase defines how to finally calculate the trust values according to a set of trust properties and metrics.

3.4 Trust management

In order to answer the question, "Does this request, accompanied by these credentials, conform with this user policy?" Blaze (Blaze et al., 1996) originally designed and introduced "Decentralized Trust Management" in 1996. Blaze identified three components of trust management:

- security policies
- security credentials
- trust relationships

Systems that support these components are considered as trust management systems, for example, well-known PolicyMaker (Blaze et al., 1996) and KeyNote (Blaze et al., 1998) (PolicyMaker is the predecessor of KeyNote).

As mentioned above, trust management has traditionally been represented as a unified method for specifying and interpreting security policies, credentials, and relationships. Now, the concept of trust management broadly refers to a general-purpose trust mechanism that calculates and re-calculates the trust value based on past successful transactions between entities in network systems.

3.5 Reputation management

Reputation management and trust management have some internal connections, because they are usually designed to prevent similar security threats. Reputation management pays

TABLE 4 Attacks against reputation systems.

Attack Name	Description
Self-promoting Attack	Attackers take actions to enhance their reputations
Whitewashing Attack	Attackers take advantage of system vulnerabilities to improve their reputations
Slandering Attack	Attackers attempt to plot a frame-up against the reputations of victims
Orchestrated Attack	Attackers attempt to use a variety of attacks against the victims
DoS Attack	Attackers constantly feed the reputation systems with fake reputation values

more attention to users' ratings in specific communities, in order to build trust through recognized reputation. Internet giants such as Alibaba, Amazon, and eBay all have reputation systems that can rate material contents, visitors, and transactions. Reputation systems may be suffered by attacks of different goals and methods, as shown in Table 4.

4 Challenges of trust and reputation management in VANETs

In recent years, trust and reputation have been successfully applied in the research field of VANETs, as a tool to monitor the behaviors of diverse entities in VANETs, so as to alleviate the uncertainty and uncontrollability involved in interaction and collaboration, guard against the aforementioned potential insider and outsider attacks in VANETs, and finally, form a trustworthy vehicular environment to promote and ensure environmental safety.

However, due to some inherent characteristics of VANETs (Wex et al., 2008), which are different from other ad hoc networks, designing a sound and secure trust and reputation management model for VANETs faces some significant challenges, which can be summarized as follows:

1. Not always online. It seems impossible to permanently connect to a fixed infrastructure in VANETs. On the one hand, fixed RSUs are not everywhere on the road. On the other hand, vehicles roam around at high speed and will connect to the roadside fixed RSUs in a random period of time. Current communicating vehicles will not always be able to communicate with the same vehicles in the near future.
2. High mobility and network dynamics. Vehicles as nodes constantly roam around, joining and leaving the vehicular environment in a free and dynamic mode, which makes it difficult to predict their effective behavior. Following that, the problems of cold start and information fusion may increase the difficulty of model design. In addition, due to the high mobility of vehicles, their location information changes also rapidly.
3. High network volume. Some VANET scenarios can accommodate thousands or even millions of vehicles. For example, VANETs located in a dense urban area may perhaps contain more vehicles than VANETs located in a rural area. During rush hours, people go to work from home and get off work from urban complexes, therefore, the situation will get worse. In this case, there may be more traffic problems such as congestion and accidents, so there is an urgent need for high-performance and high-quality systems and algorithms with scalability and robustness.
4. Decentralization. Vehicles communicating information with each other are geographically dispersed without any established infrastructure or permanent neighbors. This requires us to deal with some technical issues such as locking, synchronization, and real-time constraints in the decentralized scenes. In such an environment, there may be great uncertain in deciding whether or not to trust any vehicle. At the same time, Centralized Certification Authority (CCA) and the Trusted Third Party (TTP) cannot guarantee the long-term trust relationships.
5. Cold start and information sparsity. As mentioned above, the high mobility and dynamics of vehicles lead to the problems of cold start and information sparsity. And cold start is one of the main reasons for information sparsity. In trust computing, the initial direct and indirect trust information is often difficult to harvest. Even with the help of RSUs, useful trust information cannot be easily obtained in a short time. On the other hand, the scale of VANET is often very large. Due to the limited time for real-time decision-making, it may become impossible to search and collect trust evidence from nearby vehicles in the network, which will not only lead to cold start and sparse information, but also worsen the situation.
6. Time criticality. When developing a trust management model, time is a less important consideration; nonetheless, time is critical in VANETs, as many security risks exploit time gaps or time lags to offer falsified information. On a highway, for example, an automobile traveling at 100 kilo-meters per hour must react in one or 2 seconds to an impending emergency such as road work 50 m ahead, based on the transmitted information. Time criticality is equivalent to safety criticality to some extent. As a result, assessing trust in a short amount of time is incredibly difficult (Ahmad et al., 2018; El-Sayed et al., 2019).
7. Challenging trust establishment process. Because VANET is a typical opportunistic network in which vehicles encounter without any prior agreement, traditional trust establishment processes are ineffective in this setting. Therefore, some practical solutions must be found to meet these challenges.
8. Privacy preserving. VANETs, unlike MANETs, must pay more care to privacy because people (drivers, passengers,

and pedestrians) play a key part in their operation. Many data points, such as location or current driving speed, are relevant to personal privacy. In VANETs, location and time are two important context components.

9. Sufficient computing resources. Compared with old-fashioned vehicles, modern intelligent vehicles are always equipped with a large number of computing chips, which have rich computing power. The trust model can effectively use these chips to calculate trust and spread trust information. However, the development of hardware always precedes the development of software, as is the case in the field of trust management. For building a reliable trust or reputation solution, figuring out how to combine the computational capabilities of modern vehicles with a limitless power supply and powerful communication equipment in VANETs will be pressing and demanding.

5 Trust and reputation management models and schemes in VANETs

Since 2008, numerous trust and reputation models and schemes have been proposed (Raya et al., 2008; Serna et al., 2008; Serna et al., 2009). In the literature, there are several different types of trust and reputation taxonomies. The majority of articles classify VANET trust models into three categories: entity-centric, data-centric, and combined trust models (Zhang, 2011). Entity-centric trust models examine each vehicle as a separate entity and assess the entity's trustworthiness. Rather than evaluating the entity itself, data-centric trust models assess the trustworthiness of data or messages delivered by vehicles. The combined trust models combine entity-centric and data-centric trust models to assess the trustworthiness of both vehicles and transmitted data simultaneously. Hussain et al. (2021) provided another classification of trust management schemes: subject trust, trust-based services, and trust's origin. Entity-centric or content-centric trust is referred to as subject trust. Entity-centric trust follows the previous description and employs techniques such as encryption, game theory, and so on, but content-centric trust places a greater emphasis on the content and employs techniques such as data analytics, data statistics, watermarking, and so on. Trust-based services use trust values to provide services including trust-based routing, data aggregation, DDoS detection, and location privacy. The origin of trust assesses the value of trust based on its source, dividing it into three categories: direct trust, indirect trust, and aggregated trust. Since the concept of trust management was created, direct and indirect trust have been the most common types used in trust models. At the same time, the aggregated trust analyzes trust values based on direct and indirect trust. In this survey, however, we opted for the most intuitive and basic technique-based classification method, which is uncommon in most survey papers. The trust management models are divided into five categories: 1) Conventional techniques; 2) Network techniques; 3) Data techniques; 4) Situation and Location; 5) AI-based techniques. Cryptography, PKI-CA, fuzzy logic, and game theory are examples of conventional techniques that are commonly used in early trust management or reputation models in different study areas. Traditional networking strategies such as self-organization and emerging techniques such as 5G or fog/edge computing are used to address trust issues. Database approaches and other cutting-edge techniques, such as blockchain, are used in data-centric trust models. Situation and location methods are used to create trust models that consider spatial factors such as the surrounding environment and vehicle positions. It is also worth noting that these classifications are not mutually exclusive; some approaches may employ techniques classified in other categories. And we just include the most relevant trust and reputation management models here, and do not intend to include every single model given in the VANETs literature (*cf.* Figure 7).

5.1 Conventional techniques

The study of trust management in VANETs makes extensive use of conventional techniques like cryptography. The most significant of them are security-related techniques and concepts, such as cryptography, PKI-CA, and pseudonym. The application of fuzzy logic and game theory methodologies is also quite widespread in this field of research.

5.1.1 Security: Cryptography, PKI-CA, and pseudonym

Many attacks and their defensive measures have been extensively discussed in the VANETs literature. Cryptographic approaches (e.g., asymmetric and symmetric cryptography), PKI-CA, and identity-based procedures are all traditional security methods used for most security assaults. In VANETs, many contemporary trust management systems have also relied on these old methodologies to aid in the building and evaluation of trust (Pham and Yeo, 2018). Pure cryptography-based techniques have a number of flaws, including the fact that they only handle external threats and have very significant network overheads. As a result, the cryptography-based method is frequently utilized as an add-on to a complete trust management system. To protect VANET to a greater extent, Tangade et al. (2020) suggested a trust management strategy based on hybrid cryptography (TMHC). Asymmetric identity-based (ID-based) digital signatures and symmetric hash message authentication codes are included in the hybrid cryptography (HMAC).

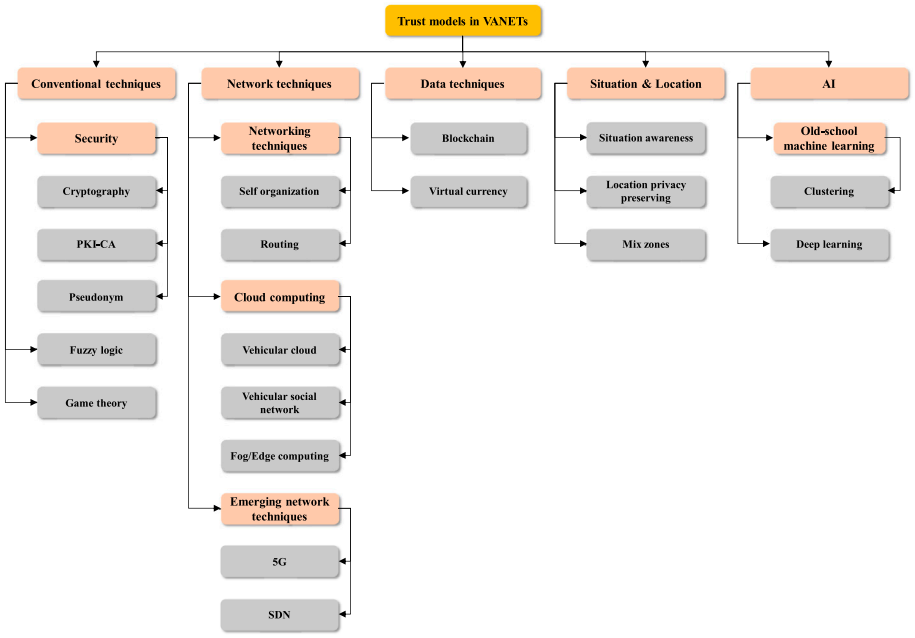


FIGURE 7
Classification of trust models in VANETs in this survey.

They analyzed the trust values of nodes in conjunction with reward points.

Many strategies using group signature to preserve driver privacy have been presented in the research field (Jiang et al., 2020; Yuanpan et al., 2020). The purpose of the group signature technique is to sign a communication on behalf of a group so that the members of the group can maintain their anonymity. Group signatures, like other digital signatures, can be publicly authenticated and can only be authenticated with a single group public key. It can also be used as a group symbol to represent the group's primary functions and types.

To provide a more efficient anonymous authentication service for vehicles, Jiang et al. (2020) adds a region trust authority and uses group signature to accomplish anonymity and conditional privacy. In a reputation-based announcement technique, Chen et al. (2013) used group signature to secure privacy for messages and feedbacks. The reputation of the vehicle that sends the message determines the message's reliability. The reputation is calculated and updated based on the feedback from other vehicles. However, in terms of communication and processing complexity, the technique only gives theoretical proofs. On the other hand, in real-world applications, centralized reputation management in VANETs is roughly unfeasible. Not only can the group signature system provide anonymity and traceability, but it can also provide unforgeability and forward security (Yuanpan et al., 2020).

A public key infrastructure (PKI) is a collection of roles, policies, and procedures for creating, managing, distributing, using, storing, and revoking digital certificates, as well as managing public-key encryption (*cf.* Figure 8). In PKI, CAs are in charge of issuing and managing long-term certificates. CAs are typically entrusted with maintaining the trust scores of vehicles in VANETs.

Raya and Hubaux (2007) presented a PKI-based public key certificate approach in 2007 that allows vehicles to store a large number of public-private key pairings and corresponding certificates. The approach produces certificate management issues by increasing communication and computational overheads. Wu et al. (2011) presented a technique called Roadside-unit Aided Trust Establishment (RATE) that intends to efficiently perform data-centric trust establishment in VANETs, making RATE suitable for a dynamically changing environment. To incorporate direct observable data with feedbacks, RATE uses an ant colony optimization technique.

Gómez Mármol and Martnez Pérez (2012) proposed TRIP, an original approach that attempts to quickly and accurately differentiate malevolent or selfish nodes distributing misleading or spurious messages using a set of design constraints tailored to VANETs. Li et al. (2013) described a system called Reputation-based Global Trust Establishment (RGTE) for sharing trust information in VANETs using dynamic thresholds depending on real-time reputation status.

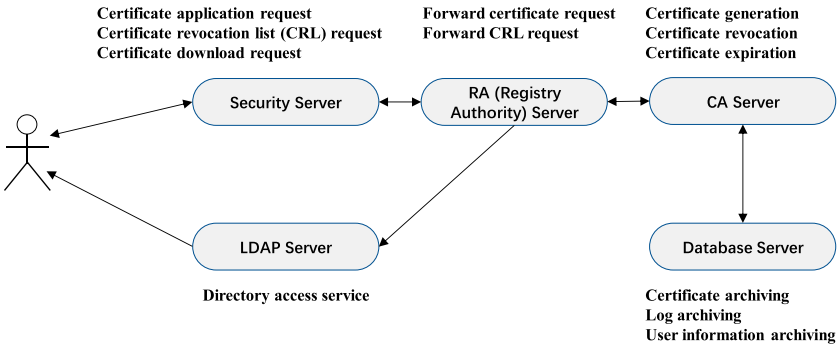


FIGURE 8
PKI-CA architecture.

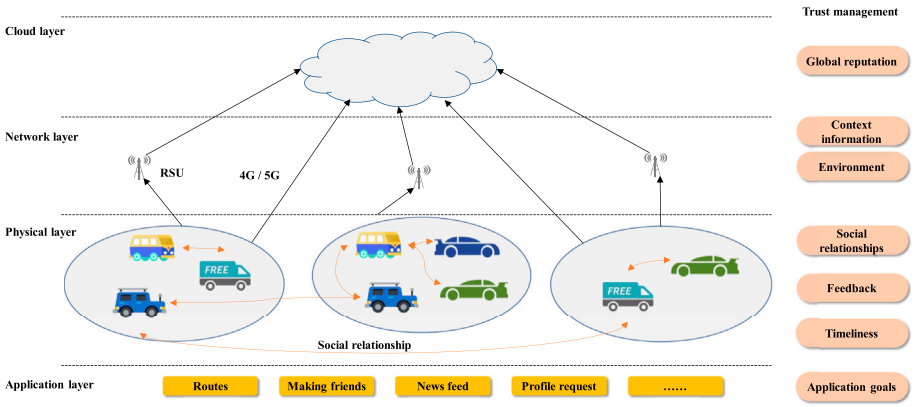


FIGURE 9
Holistic view of trust management in VSN.

Park et al. (2011) presented a Long-Term Reputation (LTR) model based on the repeated daily observation that the majority of people drive their automobiles locally for their daily commute, and that most vehicles have predefined constant daily trajectories. For these local vehicles, long-term reputation rankings are stored in roadside infrastructures.

The pseudonym approach is a type of anonymity and authentication scheme that preserves privacy. Public and private key pairs issued by PKI CAs are similar to pseudonyms. When an entity signs, it employs a unique pseudonym, which may be verified using the public key infrastructure (PKI) or identity-based cryptography (IBC) techniques.

Wang, Jin et al. (2016) combined trust management with the pseudonym technique, incorporating both service and feedback reputation. They proposed hidden-zone and k-anonymity strategies to guard against the reputation link attack during pseudonym changes. To resolve the tension between privacy preservation and reputation evaluation, Shibin and Nianmin (2019) presented a distributed trust framework for pseudonym-enabled privacy preservation in VANETs. The roadside unit gives the reputation label certificate (RLC) to every vehicle in its communication range in this framework to evaluate the message's credibility. To reduce the heavy overhead of RSUs caused by frequent key generating and exchanging, Bellikar et al. (2018) proposed a three-tier architecture for pseudonym-based anonymous authentication (3TAAV) in VANETs, with one more layer named pseudonym server (PSS), rather than a two-tier architecture including vehicles and RSUs.

5.1.2 Fuzzy logic

Fuzzy logic is a science that studies fuzzy thinking, language form, and law utilizing multi-valued logic and the fuzzy set

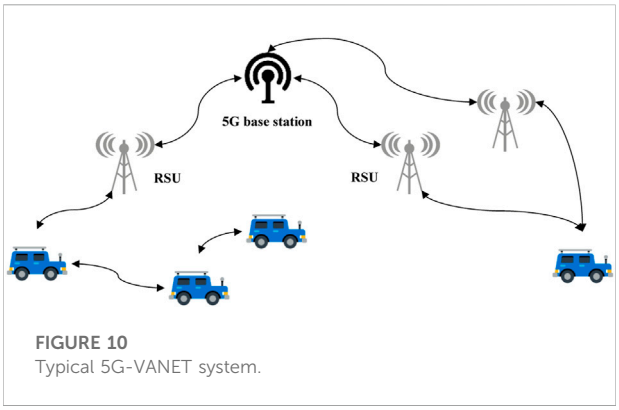


FIGURE 10
Typical 5G-VANET system.

approach. In VANETs, fuzzy logic provides a plausible way to deal with uncertainty and assess data and source reliability (Jalalia and Aghaee, 2011; Guleng et al., 2019; Sumithra and Vadivel, 2019).

Guleng et al. (2019) proposed a fuzzy logic-based strategy for evaluating one-hop neighbors' trust and dealing with vehicles' complex and uncertain behavior. The strategy also includes a Q-learning approach for evaluating indirect trust of nodes that are not directly connected to a trustor node. A model called NB-FTBM, or Naive Bayesian Fuzzy Trust Boundary Model, was suggested by Sumithra and Vadivel (2019). Entity Identification (E-ID) and Entity Reputation are two modules in the NB-FTBM (E-RP). The entity identification score and entity reputation score of an entity can be swiftly determined using NB-FTBM. The trust border line is crossed by these scores. The entity is permitted to make the necessary decision for the information received based on this boundary level. In Ref Jalalia and Aghaee, (2011), Jalalia and Aghaee proposed a fuzzy reputation system to punish selfish behaviors and encourage packet forwarding. Each node in the model has a module called Forward Manager that keeps track of the number of received forwarding requests and the number of packets transferred so far. It also employs a module known as Fuzzy Reputation Manager to determine if each packet's source node is selfish or not. Selfish source node packets are removed from the network.

5.1.3 Game theory

The interaction between formulated incentive structures is the focus of game theory. It is a mathematical theory and approach for investigating events involving struggle or competition. Individuals in the game's prediction and actual conduct are studied in game theory, as are their optimization strategies. Game theory is often used by biologists to better explain and predict some evolutionary outcomes. Because it can be utilized as a useful tool for behavior analysis, game theory appears frequently in the VANET literature (Li et al., 2020).

Li et al. (2020) suggested a novel trust evaluation scheme for vehicles and RSUs based on the use of other vehicles to monitor actions during the content delivery process. The approach employs a bargaining game-based pricing model to encourage vehicles and RSUs to behave well in the network. Simultaneously, the proposed model is analyzed using a backward induction method. In VANETs, game theory can also be used to control reputation. Tian et al. (2019) used evolutionary game theory to simulate the dynamical evolution of malevolent users' assaulting techniques as well as a reputation management scheme with numerous utility functions.

Mehdi et al. (2017) presented a game theory-based trust model for VANETs. With respect to the following parameters: majority opinion, betweenness centrality, and node density, the suggested model devises an attacker and defender security game to discover and counter the attacker/malicious nodes. The game matrix, which holds the cost (payoff) values for each potential action-reaction combination, determines the game's outcome. To determine the appropriate strategy for attacker and defender vehicles, the model uses Nash equilibrium.

5.2 Network techniques

The application of network techniques is inseparable for trust management in vehicular contexts due to its intrinsic distributed nature. Overall, the research in this field can be roughly divided into the following three directions: conventional networking techniques, cloud computing, and emerging network techniques.

5.2.1 Networking techniques: Self-organization

MANETs and VANETs both have self-organization and node movement as common features (Hamieh et al., 2009). Self-organizing models are better suited to VANETs' distributed and highly dynamic environment. In self-organized models, each node assesses the target node's trust value based on local knowledge gained from previous experiences and suggestions from neighbors over a short period of time.

For recognizing similar messages or vehicles, Yang (2013) employed a similarity mining technique called Trust and Reputation Management Framework based on the Similarity Mining Technique (TRMFS). For computing a vehicle's recommendation-based reputation, similarities from different recommenders are employed as weights. Bamberger et al. (2010) proposed an Inter-vehicular Communication trust model based on Belief Theory (ICBT). The ICBT model focuses on an individual's direct experiences rather than a system-wide reputation that would be dependent on a central unit. To respond to quickly changing conditions, infrastructure failure, and attacks, a Situation-Aware Trust (SAT) model has been developed in Ref Hong et al. (2008), which has three primary components: an attribute-based policy control model, a proactive trust model, and a social network. Zhiquan et al.

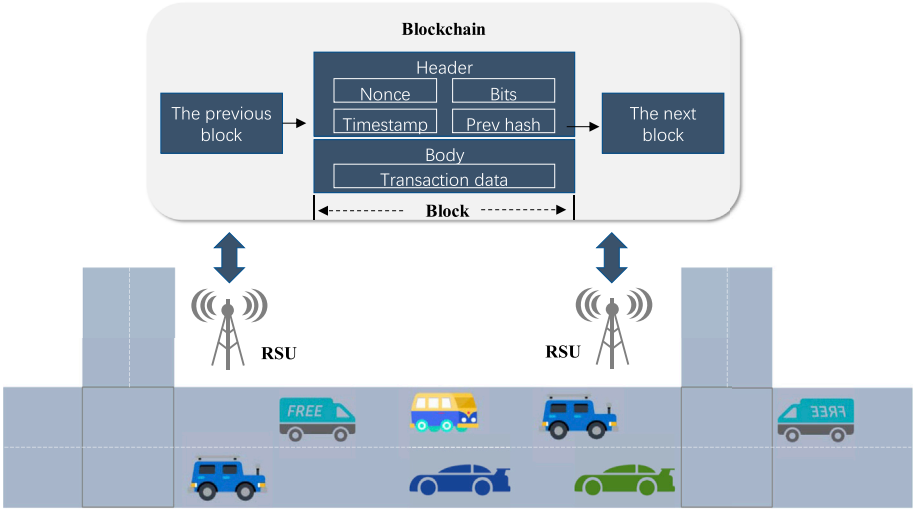


FIGURE 11
Typical blockchain-based model.

(2016) split VANET trust models into two groups: infrastructure-based and self-organized approaches. Following an analysis of current models' flaws, Liu proposed the Lightweight Self-Organized Trust (LSOT) model, which is devoid of super nodes or CAs, to make collusion attacks employing trust certificates-based evaluation and testing methods easier. In recommendation-based trust evaluation, the maximum local trust (MLT) method was included in LSOT to identify trustworthy recommenders.

5.2.2 Networking techniques: Routing

The unique characteristics of VANETs, such as centerless infrastructure, high mobility, and frequent network topology changes, create challenging and critical technical issues such as routing reliability, routing QoS, and link failure in order to avoid attackers for a variety of reasons, such as faked location, man-in-the-middle tampering, and malicious information (Chuan, 2012; Eiza & Ni, 2012; Sagar et al., 2012).

Eiza and Ni (2012) described a strategy for selecting the most reliable route to the destination from among all other routes based on link reliability. Chuan (2012) offered a comprehensive security for the geographic information routing protocol (GPSR) in order to effectively prevent malicious conduct, particularly tampering with the routing protocol or neighbor location table (NLT). Sagar et al. (2012) compared the performance of one proactive routing protocol, Destination Sequenced Distance Vector (DSDV), and two reactive routing protocols, Dynamic Source Routing (DSR) and Dynamic MANET On-Demand (DYMO), using three performance parameters: PDR, effect of link duration over End-to-End Delay (E2ED), and Normalized Routing Overhead (NRO). Many jobs are aimed at determining the best routing protocol for delivering data to destination nodes on time and with flawless packet exchange. Ahmed et al. (2018) presented a security-aware routing strategy called VANSec, and it was compared to existing techniques in terms of Trust Computation Error (TCE), E2ED, Average Link Duration (ALD), and NRO. TROPHY (Trustworthy VANET ROuting with grouP autHentication keYs) is a system proposed by Pedro et al. (2018). Using the WAVE architecture and the patented routing technique, the Service-Based Layer-2 Routing Protocol, the collection of protocols can manage the authentication of routing messages in a VANET under extremely demanding timing conditions, capable of securing the dissemination of routing information. Using Bayesian theory and fuzzy logic theory, Xia et al. (2018) presented a trust-based multicast routing system (TMR). Slama et al. (2018) presented the AIMD (Additive Increase Multicative Decrease) algorithm with the TCSR (Trusted Cryptographic Secure Routing) protocol. In VANETs, delay reduction is crucial for vehicle routing. In terms of the trust calculation, route selection, minimum message reachable time (MMRT) calculation, and route decision, Sataraddi and Kakkasageri (2019) proposed a trust-based minimum delay routing algorithm to achieve high trust and minimal routing delay. Regarding the trust between vehicles and MMRT, Sataraddi and Kakkasageri (2020) tried to build a trust- and delay-based routing for hybrid communication in sparse VANET to minimize network assaults by hostile nodes. Some recent VANET routing research has focused on actual services and applications. Ref Shaik and Ratnam, (2022) is similar in that it focuses on infotainment services like as video streaming and emergency message distribution. Energy and Mobility Aware

Routing Protocol (EM-ARP) is a suggested protocol for improving infotainment services on VANETs by minimizing delay and energy usage. EM-ARP chooses Cooperative Relay Vehicles (CRVs) dynamically based on battery power and node mobility in the destination direction. Three essential criteria, such as Link Expiration Time (LET), Hop Count, and Congestion along the path, are used to estimate route selection. Venitta Raj and Balasubramanian, (2021) provided a Similarity-based Trustworthy Routing algorithm that incorporates social factors for determining the appropriate forwarder for executing trustworthy routing. To improve the updating process of trust value, the algorithm uses two approaches: Acknowledgment during Encounter Strategy (AES) and Game-theoretic Broadcasting Strategy (GTBS). Zhiquan et al. (2020) proposed a trust cascading-based emergency message dissemination (TCEMD), which incorporates entity-oriented trust values (which are evaluated and updated by leveraging the trust certificates and are carried in the messages) into data-oriented trust evaluation in an efficient manner.

5.2.3 Cloud computing: Vehicular cloud

Cloud computing technologies are popular in VANETs because they can adapt to some of the network's fundamental qualities, such as high mobility, decentralization, and quick and ephemeral interaction (Bitam et al., 2015). For example, Qin et al. (2012) proposed VehiCloud to address unstable inter-vehicle communications and expand mobile devices' limited processing capabilities.

Hatzivasilis et al. (2019) proposed MobileTrust, a hybrid trust paradigm that allows for safe resource sharing. Using cloud computing and 5G technologies, MobileTrust can provide a secure trust foundation with global scalability. Chen and Wang (2017) proposed a cloud-based trust management paradigm for vehicular social networks. The authors presented a layered trust management technique that takes advantage of efficient physical resource use (e.g., computation, storage, and communication costs) and investigated its implementation in a VSN scenario based on a three-layer cloud computing architecture.

Vehicular cloud (VC) is a new VANET paradigm in which cloud computing and features are used to improve applications and services (Hussain et al., 2021), and vehicular cloud computing (VCC) is required to operate as service infrastructure in VANETs and vehicular social networks (VSN). The administration of trust between entities is critical and more difficult than in a standard VANET (Yan et al., 2013).

Because most VC trust models can't accurately describe the uncertainty, Sun et al. (2016) proposed a membership cloud-based trust model for T-CPS (Transportation Cyber-Physical System) VC, which considers the trust uncertainty of fuzziness and randomness in vehicle interactions and uses membership cloud to describe the uncertainty in unified formats. It also includes an algorithm for calculating cloud droplets and trust evaluation values pooled. The general architecture of VCC has been studied by Bitam et al. (2015). The paper also looked into the use of cloud computing in vehicle networks. Furthermore, the paper explored a variety of VCC-supported transportation services, including security and privacy, energy efficiency, resource management, and interoperability. RA-VTrust (Reputation-based Adaptive Vehicular Trust Model) was proposed in ref (Lee and Bae, 2014) for quickly evaluating the competency of a vehicular cloud service based on numerous trust attributes mined from evidence utilizing rough sets. J. Shen et al. (2019) introduced the CATE (Cloud-Aided Trustworthiness Evaluation Scheme) model, which uses session key generation to guarantee lightweight trustworthiness level confirmation. The uploaded region information in IPNs must be encrypted and signed by a group of vehicles in the same region (Incompletely Predictable vehicular ad hoc Networks). The trust mechanisms can assist VC manage resource scheduling more successfully. Wang J. et al. (2021) investigated the DI-Trust (Trust Model Based on Dynamic Incentive Mechanism) trust mechanism, which focuses on the following scenario: a parking lot with static vehicle nodes.

5.2.4 Cloud computing: Vehicular social cloud

The Vehicular Social Network (VSN), as shown in Figure 9, also known as SIoV, is a new ITS trend influenced by SIoT- and cloud-based VANETs (Vegni, & Loscrí, 2015; Sun et al., 2016; Iqbal et al., 2019). Human behaviors and social traits have a significant impact on VANET applications, leading to the classification of vehicular communication as a social network of vehicles. Yang and Wang (2015) were among the first to focus on trust in VSNs, introducing the core theory of trust management in a VSN context.

In most VSN trust management schemes, a vehicle cloud system serves as the social service provider (Bitam et al., 2015; Chen and Wang, 2017). Chen and Wang (2017) proposed a layered trust management technique based on a three-layer cloud computing architecture, and investigated its deployment in a VSN scenario. It is worth noting that the proposed model's performance is modelled using a revolutionary formal compositional approach called Performance Evaluation Process Algebra (PEPA), which can represent systems with layered structures and complex behaviors effectively. Hussain et al. (2016) presented a hybrid trust establishment and management paradigm that comprises two trust management solutions for distinct mobile applications: email-based social trust and social network-based trust. In their research, Li and Song (2016) presented an attack-resistant trust management scheme called ART for vehicular networks to detect and handle malicious attacks as well as assess the trustworthiness of both data and mobile nodes of networks. The trustworthiness of nodes is measured in two ways in ART: functional trust and recommendation trust.

5.2.5 Cloud computing: Fog/Edge computing

Edge computing refers to an open platform integrating network, computing, storage and application core capabilities on the side close to the object or data source to provide nearest end services. Its application program is initiated on the edge side to produce faster network service response and meet the basic needs of the industry in real-time business, application intelligence, security and privacy protection. Edge computing is between physical entities and industrial connections, or at the top of physical entities. In VANETs, vehicles cannot support mass data storage and computing power, therefore, the computing tasks are usually been transferred to RSUs with strong computing and storage capabilities to alleviate the workload and storage through edge computing.

VEC (Vehicular Edge Computing) is a popular study subject as a new networking paradigm (Raza et al., 2019), in which service providers directly host services in close proximity to mobile vehicles for significant gains. In blockchain-based vehicular edge computing (BloVEC), Maskey et al. (2021) presented a reputation-based mining node selection (RbMNS) and employed an artificial neural network (ANN) to assess the reputation of the miner nodes. Huang et al. (2017) proposed a distributed reputation management solution (DREAMS) for secure and efficient vehicular edge computing and networks, in which VEC servers are used to carry out local reputation management activities for vehicles. Soleymani et al. (2020) provided a trust model based on plausibility, experience, and vehicle type to deal with erroneous, partial, and ambiguous data in both line of sight (LoS) and none-line of sight (NLoS) situations. The k-nearest neighbor (kNN) classification technique is used to determine the NLoS state, which includes parameters such as the Radio Signal Strength Indicator (RSSI), Packet Reception Rate (PDR), and the distance between two vehicle nodes. In VANETs, the Cuckoo filter is employed to protect secure communication between vehicles and edge nodes while avoiding massive data computing.

Fog computing, in which data, data processing, and applications are concentrated in devices at the network's edge rather than being nearly entirely stored in the cloud, is a Cisco-proposed extension of cloud computing. The term "fog" comes from the well-known phrase "fog is a cloud that is closer to the ground."

Fog nodes have been used as coordinator resources in the trust evaluation process by Atwah et al. (2020). Event detection, cluster head selection, and misbehavior detection are some of the functions fog nodes can provide to relieve the burden on agents. Iqbal et al. (2019) examined existing trust management technologies that could be used in the Social Internet of Vehicles (SIoV), such as Blockchain-based and fog computing-based trust solutions. To deal with the dynamic nature of fog computing, trust management models can take advantage of its benefits for context management and job offloading. A novel bidding price-based transaction (BPT) mechanism for ensuring trusted Fog service transactions in rural areas was developed in Ref Dewanta & Mambo, (2019). Vehicles that use BPT do not need to interact with any trusted third parties in order to conduct fog computing transactions with other vehicles.

5.2.6 Emerging network techniques: 5G

5G (short for fifth-generation mobile communication technology) is a next generation broadband mobile communication technology with high rate, low delay, and massive connection capabilities (Khan et al., 2022). The network infrastructure for man-machine and object interconnection is the 5G communication facility.

Arif et al. (2020) suggested a paradigm for automotive ad-hoc network management that incorporates both 5G and Blockchain. Low latency communication provided by 5G improves both V2V and V2I connections, potentially increasing their trustworthiness. Instead of TCP/IP, Ortega et al. (2018) proposed content-centric networking (CCN) and permissioned blockchains, which allow for dynamic control of source reliability, as well as the integrity and validity of the information shared. VANETs based on CCN could theoretically be created using 5G network slicing without incurring additional deployment expenditures. Xie et al. (2019) implemented software-defined network (SDN) architecture into the 5G-VANET (Figure 10), allowing for global data gathering and network control to provide real-time IoT services on transportation monitoring and reporting.

5.2.7 Emerging network techniques: SDN

Through the separation of control and forwarding, the notion of SDN is adopted to concentrate the control logic of switching devices in the network on one computer device, bringing new ideas to improve the ability of network management and configuration. The separation of the control and data planes, as well as open programmability, are key features of SDN. According to current study, SDN can handle the time-varying nature of VANETs at a significantly reduced cost due to simplified hardware, software, and maintenance, as well as large-scale unified abstraction optimization (Xie et al., 2019; Mao et al., 2021).

Mao et al. (2021) established a hierarchical hybrid trust management architecture using an efficient flow forwarding mechanism of the RSU close to the controller in the Software-Defined Vehicular Network (SDVN), with the goal of overcoming the problems of high communication delay and low recognition rate of malicious nodes. To provide a uniform policy and global administration for the 5G-VANET, Xie et al. (2019) used a centralized SDN controller with OpenFlow protocol to control RSUs and gNBs (5G base stations) using high-capacity fiber optic backhaul lines. Qafzezi et al. (2021) designed and compared two Fuzzy-based Systems for Assessment of Nearby Vehicle Processing Capabilities (FS-ANVPC1 and FS-ANVPC2) to identify the processing

TABLE 5 Summary of trust models using blockchain in VANETs.

Ref	Model	Class	Trust metrics	Used methods	Feature	Simulation
Han et al. (2021)	Trust management model	Entity	Node properties	HMM + alliance chain	Malicious behavior detection	• HMM-based distance-based Bayesian inference • Alliance chain vs public chain • Fabric-iot Han et al. (2020)
Kudva et al. (2021)	Trust score framework	Entity	Node properties	Consortium blockchain + aggregate trust score	Insider attacks mitigation in routing	• NS-2 • OpenStreetMaps (OSM) • SUMO 1.23 • AWK scripts + PDR
Chukwuocha et al. (2021)	Bayesian trust inference model	Hybrid	Time + Distance + knowledge + Node properties	Bayesian inference + Beta distribution + Hyperledger Fabric	Trustworthiness of message exchanging	• Real data • NodeJs + python • Beta priors
Wang C. et al. (2021)	B-TSCA	Entity	Node properties	Blockchain	Identity re-authentication of vehicles	• GNU Multiple Precision Arithmetic (GMP) lib • Pairing-Based Cryptography (PBC) lib
Li B. et al. (2021)	Blockchain-based trust management model	Entity	Node properties + Location	Blockchain + Location Based Service (LBS) + Dirichlet distribution	Location privacy preserving	• Hyperledger fabric • thermal reactor consensus mechanism • Elliptic Curve Cipher (ECC)
Li F. et al. (2021)	ATM	Hybrid	Node properties + energy consumption + throughput	Blockchain	Active detection of malicious nodes	• NS-3
Inedjaren et al. (2021)	Blockchain-based distributed management system	Entity	Reputation + Multi-point Relay (MPR)	Blockchain + Optimized link state routing protocol (OLSR) + Fuzzy logic	Secure routing in VANETs	• NS-3 • FT-OLSR
Zhang & Xu, (2021)	Trust-based certificateless anonymous authentication scheme	Entity	Node properties	Blockchain + Bilinear pairing operations + ECC + Certificateless signature	anonymous authentication	• Java
Liu et al. (2020)	BTCPS	Hybrid	Node properties + Reputation	Blockchain + Group signature	privacy-preserving announcement	• Python + Golang • PBC lib
Luo et al. (2020)	Trust-based location privacy protection scheme	Entity	Node properties + Location	Blockchain + LBS + Dirichlet distribution + anonymous cloaking region + ECC	Location privacy preserving	• Hyperledger • OPNET Modeler 14.5
Ma et al. (2020)	Traffic information sharing system	Data	Traffic event	Blockchain + Real-Time Transport Protocol (RTP)	Secure traffic information sharing	• vDLT • FFmpeg API • AODV
Zeng et al. (2020)	Fengyi	Data	Accountability + Conditional privacy +	Trusted Ledger Model (TLM)	Trusted data sharing	• HydraOne

(Continued on following page)

TABLE 5 (*Continued*) Summary of trust models using blockchain in VANETs.

Ref	Model	Class	Trust metrics	Used methods	Feature	Simulation
			Transmission confidentiality			
Ayobi et al. (2020)	Lightweight blockchain-based decentralized trust model	Data	Reputation + Distance + Location + Event	DS theory + Cloud computing + Blockchain	Trusted message transmitting	• N/A
Xie et al. (2019)	Blockchain-based security framework	Data	Distance + context (road condition)	SDN + 5G VANET + Blockchain	Secure broadcasting and sharing	• OMNeT++ 4.5 • crypto++ lib 5.6.2 • SHA-256
Yang et al. (2019)	BTEV (Blockchain-based Traffic Event Validation)	Data	Event	Proof-of-event (PoE)	Traffic event validation	• Real data from Taiwan • NS-3
Khan et al. (2019)	Secure trust-based blockchain architecture	Hybrid	Probability of event	Blockchain + timestamps + hashing + message rating and credibility	Attacks prevention	• Veins • OMNeT++ • SUMO
Javaid et al. (2019)	DrivMan	Hybrid	Identity + Linkability	Blockchain + PKI-CA + physical unclonable functions (PUFs)	Secure inter- and intra-network communication	• Ethereum • No experimental results
Lu et al. (2018a); Lu et al. (2018b)	BARS	Hybrid	Reputation + knowledge	Two blockchains (CerBC and RevBC) + PKI	Attacks	• Python

capability of neighboring vehicles in Software Defined Vehicular Ad hoc Networks (SDN-VANETs). In a layered Cloud-Fog-Edge architecture, the model uses cloud computing, fog computing, and edge computing, as well as SDN, to make up the edge computing resources.

5.3 Data techniques

In the study area of trust management in VANETs, the use of data approaches, particularly blockchain, has gained popularity recently.

5.3.1 Data techniques: Blockchain

Blockchain, which was originally created for crypto-currency exchange in financial transactions, provides a distributed append-only public record that does not require a central authority (N. Satoshi, 2019). Due to the inherent characteristics of blockchain (M. Atzori, 2017), there has been a lot of study in trust management for various distributed frameworks using blockchain to achieve high security agreement levels and decentralized governance in recent years (Figure 11). Table 5 summarizes the current advancement in blockchain-based trust management systems in VANETs since 2016 based on relevance. Following that, we'll look at some noteworthy research findings in the subject of VANETs.

Lu et al. (2018a); Lu et al. (2018b) presented a blockchain-based anonymous reputation system (BARS) to enable distributed trust management, with the goal of protecting vehicle privacy. BARS gives the LEA (Law Enforcement Authority) with the responsibility of registering, monitoring, and evaluating the reputation scores of each vehicle. Meanwhile, BARS provides blockchain to record all of CA's actions without disclosing sensitive vehicle information. BARS incorporates a trust model that relies on the sender's reputation based on both direct prior encounters and indirect judgments about the sender to improve the trustworthiness of messages. Yang et al. (2019) introduced the BTEV framework, which consists primarily of a two-pass threshold-based event validation mechanism and a two-phase sequential blockchain transaction. Xie et al. (2019) developed a blockchain-based security framework to support vehicular IoT applications, such as real-time cloud-based video reporting and vehicular message trust management. Patel et al. (2019) presented "VehicleChain", a protocol that integrates blockchain with elliptic curve cryptography to increase VANET security without raising processing expenses. Insider, server spoofing, modification, man-in-the-middle, plaintext, replay, and impersonation are all attacks that the VehicleChain can defend against.

5.3.2 Data techniques: Virtual currency

In VANETs, virtual currency is employed as a motivator to encourage cooperation and identify selfish nodes. However, there are only a few examples where the trust or reputation mechanism is solely based on virtual currency.

Li and Wu (2009) introduced FRAME, a virtual currency-based approach for enhancing collaboration in vehicular networks. Their incentive program is based on the number of direct sprays and the amount of time a node keeps a packet.

To combat selfish behavior, Caballero-Gil et al. (2009) used a virtual currency scheme. When a packet arrives at its destination, each node involved in the forwarding process should report its contribution to the source node. The total of each node in the forwarding tree's partial contributions is used to compute the final contribution. Based on the ultimate contribution and the number of relay nodes, each intermediate node will be rewarded.

5.4 Situation and Location

Information about situation and location is intricately linked to user privacy, which is crucial for the extensive application of VANETs. However, according to our search results, there are not many research findings that pertain to this research topic.

5.4.1 Situation and Location: Situational awareness

Situational awareness is the ability to comprehend the environment and effectively forecast and respond to future difficulties. The Situation-Aware Trust Paradigm (SAT) (Hong et al., 2008) is a situation-aware model for establishing trust in vehicular networks.

S-Aframe (Zhiquan et al., 2016) is an agent-based multilayer framework with context-aware semantic service (CSS) to support the development and deployment of context-aware applications for vehicular social networks (VSNs) formed by in-vehicle or mobile devices used by drivers, passengers, and pedestrians. The framework architecture is made up of three layers: framework service layer, software agent layer, and owner application layer. It is built on top of the operating systems of mobile devices.

Oluoch (2016) proposed a reputation strategy in which each receiving vehicle asks other cars in its communication range for their opinion on the sending vehicle's trustworthiness, and then uses conditional probability to identify hostile peers.

5.4.2 Situation and Location: Location privacy preserving

Many VANET services and applications rely on location data, which necessitates anonymity to safeguard a driver's privacy, as well as identity and traceability for deeper application.

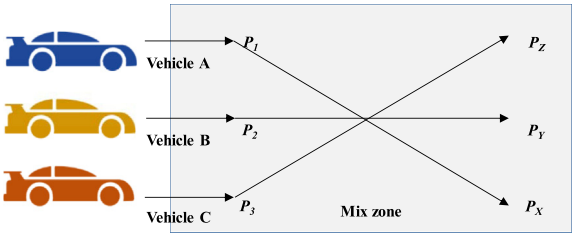


FIGURE 12
Mix zone model.

To ensure location privacy, Ref Yu Chih et al. (2011) and Yu Chih and Chen, (2012) provided a secure broadcast authentication protocol and beacon-based trust management system, and Dempster-Shafer theory was used to merge event message trustworthiness with vehicle trustworthiness from numerous vehicles.

The SLOW technique is defined in Ref Levente et al. (2009) as being based on the assumptions that if pseudonyms are changed at an inopportune time or location, frequent pseudonym changes cannot ensure location privacy. The main notion is that when a vehicle's speed falls below a certain level, it should not transmit heartbeat messages and should change pseudonym for each such silent interval. This does not have to happen in a specific physical area (i.e., a static mix zone).

5.4.3 Situation and Location: Mix zones

The Mix Zone technique is a special type of real-time location privacy preserving mechanism used in VANETs that can break location exposure continuity and prevent attackers from linking beacons while altering the vehicle's pseudonym (*cf.* Figure 12). Vehicles can alter their pseudonyms in mix zones, which are pre-determined areas.

Ying and Makrakis (2015) presented RPCLP (Reputation-based Pseudonym Change for Location Privacy), which motivates users (even those who are selfish) to gain reputation "credit" by changing their pseudonym. Sun et al. (2015) explain how to deploy mix-zones optimally in a large metropolis and provide a statistics-based criteria for evaluating a mix-effectiveness zone's and selecting mix-zone candidates based on privacy needs. In addition, the paper presents a cost-effective mix-zone deployment scheme that ensures that cars in each location can travel through an effective mix-zone in a specific amount of time. Hou et al. (2021) presented two categories of Mix-Zone tracking methods based on basic BP (Back Propagation) and tailored artificial neural networks, both of which may considerably increase the tracking result while revealing the Mix-Zone privacy preserving level more realistically.

5.5 AI

In recent years, several fields have incorporated artificial intelligence approaches, and the research field of trust management can be improved by making further use of recent advancements in AI. AI approaches can be used to create trust management models for VANETs to help with the design of safety and non-safety applications for moving vehicles.

5.5.1 AI: Old-school machine learning and clustering

Old-school machine learning algorithms like SVM (Support Vector Machine), LR (Logistic Regression), KNN, and RF (Random Forest) were widely used before the invention of deep learning. Machine learning methods are commonly employed in VANETs to detect misbehavior (Zhang C. et al., 2018; Bangui et al., 2022; Ercan et al., 2022), such as Wormhole Attacks, Position Falsification Attacks, and intrusion detection, among other things. To assure the identification and elimination of malicious vehicles from the network, approaches combining trust models and traditional machine learning algorithms have gradually increased in the literature (Siddiqui et al., 2019; El-Sayed et al., 2020; Gyawali et al., 2020; Jordan et al., 2020).

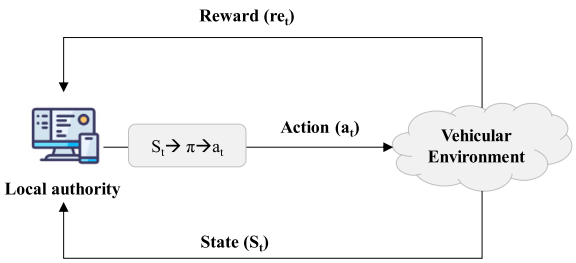
These trust models mainly rely on the accumulation of both direct and indirect observations and evict the malevolent vehicles in accordance with a specific threshold defined on this composite trust value. By using machine learning approaches to identify misbehaving nodes based on false position attacks, Jordan et al. (2020) seek to analyze the parameters utilized for the computation of trust metrics. In Ref Siddiqui et al. (2019), a hybrid trust management heuristic based on machine learning called Poster was proposed. Poster computes the aggregate trust score for identifying and removing rogue vehicles from a vehicular network using machine learning. El-Sayed et al. (2020) proposed a novel entity-centric trust framework using artificial neural networks (to self-train the vehicular nodes) and decision tree classification (to develop rules for trust calculation). At the same time, the model calculates the trust using a variety of roles and distance-based metrics like Euclidean distance. To improve the identification of internal attacks and to guarantee the dependability of both cars and communications, Gyawali et al. (2020) have developed a reputation-based MDS (Misbehavior Detection System) based on machine learning. The Dempster-Shafer (DS)-based feedback combination uses the reputation score of each vehicle as a belief value, and the reputation update and revocation are based on a beta distribution.

Clustering algorithms are widely used in the VANET trust model study as a type of traditional machine learning technique. Cluster algorithms are frequently used in VANETs to choose the node with the highest trust value as the cluster leader among all groups of entities for the purpose of receiving additional data requests. A network architecture that is appropriate for effective communication can be achieved with the help of appropriate clustering algorithms (Gaber et al., 2018; Oubabas et al., 2018; Mahmood et al., 2019; Zhang C. et al., 2022).

Oubabas et al. (2018) put forward a method for choosing the reliable cluster heads in the event that a malicious or hacked node is elected as the cluster head. In contrast to other schemes that use a static trust function, the approach uses a new adaptive trust function to evaluate the data trust between nodes according to the reported event's requirement in terms of trust severity. A timer is also used to reduce the control traffic during a clustering process by removing the competition between nodes to become cluster-heads. A bio-inspired and trust-based cluster head selection strategy for WSN used in ITS applications has been artistically proposed by Gaber et al. (2018). The Bat Optimization Algorithm (BOA) is used to pick the cluster heads based on three parameters: residual energy, trust value, and the number of neighbours. The trust level for each node is computed. Mahmood et al. (2019) presented a hybrid trust management strategy that uses intermittent elections to select the cluster head and proxy cluster head based on a composite measure (i.e., trust values assigned to the cars along with their resource availability). Zhang C. et al. (2022) described a variant of the cluster head selection problem, i.e., how to choose a suitable and trustworthy head vehicle while maintaining the privacy of user cars in a vehicle platoon when the vehicles join the vehicle platoon. To help potential user vehicles avoid choosing the malevolent head vehicles, a recommendation method known as TPPR is provided. Pseudonyms and the Paillier cryptosystem are used to protect the anonymity of the vehicles. A trust-based anomaly detection system for intelligent vehicles on the road was put forward by Yang et al. (2016), while also taking leader-based detection and the usefulness of RSUs into account. In order to guarantee robustness and fairness in the detection process, a central reputation arbitrator is proposed as a distributed supervisor. A reputation-based weighted clustering protocol (RWCP) for VANETs has been proposed in Ref Joshua et al. (2019) that takes into account each node's reputation as well as the position, velocity, number of close vehicles, direction, and number of vehicles. The various RWCP control settings are optimized using the Multi Objective Firefly Algorithm (MOFA).

5.5.2 AI: Deep learning

Deep learning algorithms, particularly deep reinforcement learning algorithms, have received a lot of attention recently and are being used in VANETs (Zhang D. et al., 2018; Tangade et al., 2019; Gyawali et al., 2021; Zhang D. et al., 2022). The Deep Reinforcement Learning algorithm combines the perception ability of deep learning with the decision-making capacity of reinforcement learning and is used extensively coupled with trust or reputation models in VANETs (Zhang D. et al., 2018; Gyawali et al., 2021). A typical deep reinforcement learning based trust management scheme is shown in Figure 13. In this scheme, the



Notation	Description
S_t	State of the local authority at time t
a_t	Action of the agent at time t
Re_t	Reward at time t
π	the optimum reputation update policy

FIGURE 13
A typical reinforcement learning based reputation update policy.

local authority functions as an agent who not only gathers feedback but also chooses the best reputation policy, by interacting with the vehicular environment. Using the prior reputation policy, the average amount of true messages, and the typical reputation score of malicious vehicles, the local authority can estimate the current condition. The local authority can then decide on the action, or reputation policy, in order to maximize the reward based on the optimal policy.

A software-defined trust based deep reinforcement learning framework (TDRL-RP) that integrates a deep Q-learning algorithm into a logically centralized SDN controller has been proposed by Zhang D. et al. (2018). The trust model is created to assess neighbors' packet-forwarding behaviors, and the SDN controller is utilized as an agent to learn the highest routing path trust value of a VANET environment. A unique software-defined trust based VANET architecture (SD-TDQL) has been developed in another study by Zhang D. et al. (2022), in which the centralized SDN controller serves as a learning agent to obtain the most advantageous communication link policy utilizing a deep Q-learning strategy. In a joint optimization problem, which is treated as a Markov decision process with state space, action space, and reward function, the trust of each vehicle and the reverse delivery ratio are taken into account. The anticipated transmission count (ETX) statistic measures the effectiveness of the communication link for connected vehicles. The dynamic reputation update policy developed by Gyawali et al. (2021) uses deep reinforcement learning to estimate the average amount of true messages by combining vehicle feedbacks with DS theory on VEC servers. To encourage cars to submit genuine feedback and prevent them from taking advantage of weak or strong reputation update methods, VEC uses deep reinforcement learning to establish the best reputation update policy. Tangade et al. (2019) proposed a Deep Neural Network (DNN)-based driver classification and trust computation (DL-DCTC) method that can distinguish fraudulent and non-fraudulent message/driver during V2V interactions and generate reward-points depending on driver behaviors.

While safeguarding their unique data sets, VANETs can employ federated learning (FL) to cooperatively train and update a shared machine learning model. By using a consensus approach in the blockchain, Otoum et al. (2020) provided a FL framework along with blockchain techniques to decentralize the shared machine learning models on end devices without any centralized training of the data or coordination.

6 Future directions for trust management in VANETs

There are still a lot of real-world problems that have not been solved, despite the fact that many trust and reputation models have been put forth in VANETs recently. On the other hand, these problems may be seen as opportunities in terms of research, infrastructure, product development, business, and commercialization. The issues facing VANETs are discussed in this part, along with a summary of possible prospective research areas for trust and reputation management models in VANETs. These challenges will undoubtedly have an impact on the evolution of VANETs.

1. **Lack of *in-situ* measured results and data. B**ecause physical resources were not readily available to researchers on university or even practitioners in automakers, many suggested models and methodologies had not been tested in VANET testing yards. For future large-scale deployment, only modeling results are insufficient. That is another obstacle to the commercialization of trust management methods in VANETs in the real world. The second aspect of this statement is that without this data, it will be difficult to compare results, and as a result, some approaches might not seem as tenable in theory as they do in practice. Field experiments should receive increased attention in future research endeavors, and *in-situ* measurable results and open data are eagerly anticipated.

2. I**nadequate deployed infrastructure for VANETs.** Even in industrialized nations, critical VANET components like RSUs have not been widely implemented. Some options, particularly those that rely on RSUs as central CAs, are currently impractical due to inadequate infrastructure deployment. In a reasonably long length of time, this also results in the "cold start" and "information sparsity" concerns in VANET scenarios. The ultimate goal of

VANETs is large-scale deployment, although widespread inadequacies in infrastructure deployment will be present.

3. **Less prominent human factors in the models.** Few proposed models in the literature consider the human element; instead, many proposed systems concentrate more on vehicles, messages sent between vehicles, and fancy trust computing techniques. This is partially due to the difficulty of putting subjective human behavior into a monetary or numerical context. On the other hand, cars behave on behalf of humans in VANETs as entities, and in certain ways, the actions of vehicles in models can be seen as representing human behavior on them. Researchers in the field have not given robustness much attention despite it being a crucial component for life-critical applications of VANET, which is another concrete example of certain shortcomings in the consideration of the human factor. In this situation, hybrid solutions with various human dimension features and metrics should be taken into account and used.

4. **Inexistent one-size-fits-all solution.** A model for a global perspective has not been provided, hence almost all trust and reputation management strategies respond to singular attacks. As we can see from the survey above, a variety of strategies have been employed in the field, but no universally applicable solution has yet been developed. At various levels, including network architecture, protocols, communication standards, and computer resources, the integration of enabling approaches causes heterogeneity difficulties (Hussain et al., 2021). Dynamism, personalization, context-aware computing, multiscale information fusion, and multiple network fusion need to be prioritized as research directions (i.e., cloud, fog, edge, 5G, IoT, and so on).

5. **Lack of co-design between hardware and software.** As far as the current situation is concerned, the majority of suggested VANET schemes begin with software design and infrequently make any mention of the shallow or deep integration with hardware components. To implement the functions of key secure storage, authentication, trust root, and other related functions, realistic security solutions like trusted computing or TEE (Trusted Execution Environment) provide physical security features. In terms of reliability for end users, hardware design will make the solutions more secure and less susceptible to threats like viruses and malware. Therefore, it is safe to say that hardware design and integration with software will be a popular area of study in the future for VANET researchers.
6. **Insufficient performance considerations.** The majority of the solutions and methods used in this industry are security-focused rather than providing suitable performance guarantee. These models provide less attention to performance problems and more attention to network designs, network protocols, trust negotiation, trust boosting, and security solutions. Some proposed trust models may not be applicable for time-critical and safety-critical scenarios when performance issues are fully considered in the models. In addition, a number of criteria, including entity cooperation, user privacy, location privacy, data exchange efficiency, and others, have an impact on how well trust solutions perform. In order to do this, a credible performance review may evaluate several of the aforementioned criteria as well as other recently developing factors that were not anticipated beforehand.
7. **Green energy-efficient computing.** These frequent data exchanges between entities and the increasing size of digital contexts in VANETs will result in significant levels of energy consumption and carbon emissions, necessitating the use of lightweight trust management frameworks and even green energy-efficient computing. Machine learning techniques, forecasting algorithms, power-saving strategies, on-demand protocols, and other techniques can all be deeply utilized in green energy-efficient computing. Future studies in this area might concentrate further on the energy consumption effectiveness of trust bootstrapping, trust negotiation, trust evaluation, and trust updating models.
8. T**rust in emerging technologies.** As VANET contexts become more intricate and detailed, research efforts are increasingly focusing on exploiting cutting-edge technologies including fog computing, edge computing, reinforcement learning, federated learning, blockchain, and SDN. In addition to the qualities of scalability, traceability, resilience, dynamics, autonomy, complexity, routing effectiveness, and resource restrictions, these technologies can also offer high QoS and QoE (Quality of Experience) assurances. Decentralized traceability, for instance, can be achieved using blockchain technology, while localized processing and storage are possible with fog computing. Emerging technologies may cross-pollinate to produce fresh insights and scientific discoveries.

7 Conclusion

Since secure communication assures accurate information transmission among vehicles in VANETs, many researchers, especially those in the security research field, are interested in improving the security of VANETs. This survey provides a succinct summary of recent developments in the field of trust and reputation management in VANETs in a technique-based taxonomy, which is different from many other surveys in the field of research. The survey begins by outlining the current attack types in VANETs and outlining the key issues that

surround trust management in VANETs. In the survey, the current trust management models are divided into five categories: 1) Traditional techniques, 2) Network techniques, 3) Data techniques, 4) Situation and Location, and 5) AI-based models. Each trust management model in its category handles many aspects of trust difficulties from its own perspective, and can be utilized as a reference model for solutions to models of other categories. In addition to this, this kind of classification offers a unique opportunity for researchers and practitioners in this research field to scrutinize problems from a purely technical perspective. Although numerous models and schemes have been put forward for various objectives, there are still difficulties and significant problems that need to be overcome. In order to ensure higher levels of trust in the vehicular environment with a balanced trade-off in terms of security, QoS, performance, and privacy, the VANET research community may be expected to broadly research and apply hybrid schemes combining various variations of currently available technical solutions in the future.

We think that by providing new perspectives and studies in the area of trust and reputation management in VANETs, our work will help other researchers and professionals better understand the most recent research developments and directions in VANETs and establish clear research goals for themselves.

Author contributions

HC is the main contributor of the manuscript and has finished the main body of the manuscript. YC helped che finish Section IV and Section V of the survey. YC also helped polish the whole survey and provided many insightful suggestions about the manuscript. CL authored the original Section II of the manuscript. LY authored the original Section III of the manuscript. All authors contributed to the final version of the manuscript.

Acknowledgments

Thanks to our paper reviewers for their generous comments and help in reviewing the original version of this paper. We acknowledge Hainan Province Key R&D Program (ZDYF2022GXJS007, ZDYF2022GXJS010), Hainan Province Higher Education and Teaching Reform Research Project (Hnjg2021ZD-3) and Hainan Province Key Laboratory of Meteorological Disaster Prevention and Mitigation in the South China Sea Project (SCSF202210).

Conflict of interest

HC and CL were employed by the company Zeekr Group.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Aad, I., Hubaux, J. P., and Knightly, E. W. (2004). "Denial of service resilience in ad hoc networks," in Proceedings of the 10th annual international conference on Mobile computing and networking, 202–215.

Ahmad, F., Franqueira, V. N. L., and Adnane, A. (2018). Team: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks. *IEEE Access* 6, 28643–28660. doi:10.1109/ACCESS.2018.2837887

Ahmad, F., Kurugollu, F., Kerrache, C. A., Sezer, S., and Liu, L. (2021). Notrino: A novel hybrid trust management scheme for internet-of-vehicles. *IEEE Trans. Veh. Technol.* 70 (9), 9244–9257. doi:10.1109/tvt.2021.3049189

Ahmed, S., Rehman, M. U., Ishtiaq, A., Khan, S. U., Ali, A., and Begum, S. (2018). VANSec: Attack-Resistant VANET security algorithm in terms of trust computation error and normalized routing overhead. *J. Sens.* 2018, 6576841. doi:10.1155/2018/6576841

Al-kahtani, M. S. (2012). "Survey on security attacks in vehicular ad hoc networks (VANETs)," in Proceedings of the 6th International Conference on Signal Processing and Communication Systems, 1–9. doi:10.1109/ICSPCS.2012.6507953

Arif, M., Balzano, W., Fontanella, A., Stranieri, S., Wang, G., and Xing, X. (2020). "Integration of 5G, VANETs and blockchain technology," in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2007–2013. doi:10.1109/TrustCom50675.2020.00275

Arsalan, A., and Rehman, R. A. (2018). "Prevention of timing attack in software defined named data network with VANETs," in International Conference on Frontiers of Information Technology (FIT), 247–252. doi:10.1109/FIT.2018.00050

Atwah, R. J., Flocchini, P., and Nayak, A. (2020). "Towards smart trust management of VANETs," in 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 1–5. doi:10.1109/CCECE47787.2020.9255766

Atzori, M. (2017). Blockchain-based architectures for the internet of things: A survey. *Soc. Sci. Electron. Publ.* 2017.

Ayobi, S., Wang, Y., Rabbani, M., Ali, D., Jelodar, H., Huang, H., et al. (2020). A lightweight blockchain-based trust model for smart vehicles in VANETs. *SpaCCS* 2020, 276–289.

Baiad, R., Otrok, H., Muhaidat, S., and Bentahar, J. (2014). "Cooperative cross layer detection for blackhole attack in VANET-OLSR," in 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), 863–868. doi:10.1109/IWCMC.2014.6906469

Bamberger, W., Schlittenlacher, J., and Diepold, K. (2010). "A trust model for intervehicular communication based on belief theory," in Proceedings of the 2nd IEEE International Conference on Social Computing (SocialCom '10) (Minneapolis, Minn, USA: IEEE), 73–80.

Bangui, H., Ge, M., and Buhnova, B. (2022). A hybrid machine learning model for intrusion detection in VANET. *Computing* 104 (2022), 503–531. doi:10.1007/s00607-021-01001-0

Bellikar, G., Bhatia, A., Hansdah, R. C., and Singh, S. (2018). "3TAAV: A three-tier architecture for pseudonym-based anonymous authentication in VANETs," in Proceedings of the 32nd International Conference on Information Networking (ICOIN 2018) (Chiang Mai, Thailand: IEEE Computer Society), 420–425.

Biswas, S., Mišić, J., and Mišić, V. (2012). "DdoS attack on WAVE-enabled VANET through synchronization," in IEEE Global Communications Conference (GLOBECOM), 1079–1084. doi:10.1109/GLOCOM.2012.6503256

Bitam, S., Mellouk, A., and Zeadally, S. (2015). VANET-cloud: A generic cloud computing model for vehicular ad hoc networks. *IEEE Wirel. Commun.* 22 (1), 96–102. doi:10.1109/mwc.2015.7054724

Bittl, S., Gonzalez, A. A., Myrtus, M., Beckmann, H., Sailer, S., and Eissfeller, B. (2015). "Emerging attacks on VANET security based on GPS Time Spoofing," in 2015 IEEE Conference on Communications and Network Security (CNS), 344–352. doi:10.1109/CNS.2015.7346845

Blaze, M., Feigenbaum, J., and Keromytis, A. D. (1998). *KeyNote: Trust management for public-key infrastructures*. Berlin, Heidelberg: International Workshop on Security Protocols Springer.

Blaze, M., Feigenbaum, J., and Lacy, J. (1996). "Decentralized trust management," in Proceedings of the 17th Symposium on Security and Privacy (Oakland, USA: IEEE Computer Society Press), 164–173.

Bragagnolo, M. C., Messai, N., and Manamanni, N. (2019). "Attack detection in a cluster divided consensus network," in Proceedings of the 18th Eur. Control Conf. (ECC), Jun. 2019, 1091–1096.

Caballero-Gil, P., Molina-Gil, J., Hernandez-Goya, C., and Caballero-Gil, C. (2009). "Stimulating cooperation in self-organized vehicular networks," in APCC'09 Proceedings of the 15th Asia-Pacific conference on Communications, 2009.

Chen, C., Wang, X., Han, W., and Zang, B. (2009). "A robust detection of the sybil attack in urban VANETs," in Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops, 270–276. doi:10.1109/ICDCSW.2009.48

Chen, L., Li, Q., Martin, K., and Ng, S. (2013). "A privacy-aware reputation-based announcement scheme for VANETs," in IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC), 1–5.

Chen, X., and Wang, L. (2017). A cloud-based trust management framework for vehicular social networks. *IEEE Access* 5, 2967–2980. doi:10.1109/access.2017.2670024

Chuan, D. (2012). Towards a trusted vehicular routing in VANET. *Inf. Technol. Convergence, Secure Trust Comput. Data Manag.* 2012, 103–117.

Chukwuocha, C., Thulasiraman, P., and Thulasiram, R. K. (2021). Trust and scalable blockchain-based message exchanging scheme on VANET. *Peer. Peer. Netw. Appl.* 14, 3092–3109. doi:10.1007/s12083-021-01164-9

Dewanta, F., and Mambo, M. (2019). "Trust establishment for vehicular fog computing service in rural area," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom workshops (Kyoto, Japan: IEEE), 882–887.

Dhamgaye, A., and Chavhan, N. (2013). Survey on security challenges in VANET. *Int. J. Comput. Sci.* 2, 88–96.

Eiza, M. H., and Ni, Q. (2012). "A reliability-based routing scheme for vehicular ad hoc networks (VANETs) on highways," in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 1578–1585. doi:10.1109/TrustCom.2012.53

El-Sayed, H., Chaqfeh, M., El-Kassabi, H., Serhani, M. A., and Alexander, H. (2019). Trust enforcement in vehicular networks: Challenges and opportunities. *IET Wirel. Sens. Syst.* 9, 237. doi:10.1049/iet-wss.2018.5211

El-Sayed, H., Ignatious, H. A., Kulkarni, P., and Bouktif, S. (2020). Machine learning based trust management framework for vehicular networks. *Veh. Commun.* 25, 100256. doi:10.1016/j.vehcom.2020.100256

Elbatt, T., Goel, S. K., Holland, G., Krishnan, H., and Parikh, J. (2006). "Cooperative collision warning using dedicated short range wireless communications," in VANET'06: Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks, 1–9.

Ercan, S., Ayaida, M., and Messai, N. (2022). Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access* 10 (2022), 1893–1904. doi:10.1109/ACCESS.2021.3136706

Gaber, T., Abdelwahab, S., Elhoseny, M., and Hassanien, A. E. (2018). Trust-based secure clustering in WSN-based intelligent transportation systems. *Comput. Netw.* 146, 151–158. doi:10.1016/j.comnet.2018.09.015

Gillani, M., Ullah, A., and Niaz, H. A. (2018). "Trust management schemes for secure routing in VANETs-a survey," in 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics, MACS (Karachi, Pakistan: IEEE), 1–6.

GM (2016). Threat assessment algorithm. Available at: http://www.nhtsa.dot.gov/people/injury/research/pub/acas/acas-fieldtest/.

Gómez Mármol, F., and Martínez Pérez, G. (2012). Trip: A trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *J. Netw. Comput. Appl.* 35 (3), 934–941. doi:10.1016/j.jnca.2011.03.028

Guette, G., and Ducourthial, B. (2007). "On the Sybil attack detection in VANET," in 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, 1–6.

Guleng, S., Wu, C., Chen, X., Wang, X., Yoshinaga, T., and Ji, Y. (2019). Decentralized trust evaluation in vehicular internet of things. *IEEE Access* 7, 15980–15988. doi:10.1109/access.2019.2893262

Gyawali, S., Qian, Y., and Hu, R. Q. (2021). Deep reinforcement learning based dynamic reputation policy in 5G based vehicular communication networks. *IEEE Trans. Veh. Technol.* 70 (6), 6136–6146. doi:10.1109/TVT.2021.3079379

Gyawali, S., Qian, Y., and Hu, R. Q. (2020). Machine learning and reputation based misbehavior detection in vehicular communication networks. *IEEE Trans. Veh. Technol.* 69 (8), 8871–8885. doi:10.1109/TVT.2020.2996620

Hamieh, A., Ben-Othman, J., and Mokdad, L. (2009). "Detection of Radio interference attacks in VANET," in GLOBECOM 2009: 2009 IEEE Global Telecommunications Conference, 1–5. doi:10.1109/GLOCOM.2009.5425381

Han, L., Han, D., and Li, D. (2021). Behavior analysis and blockchain based trust management in VANETs. *J. Parallel Distrib. Comput.* 151 (2021), 61–69. doi:10.1016/j.jpdc.2021.02.011

Han, L., Han, D., and Li, D. (2020). Fabric-iot: A blockchain-based access control system in IoT. *IEEE Access* 8 (2020), 18207–18218. doi:10.1109/access.2020.2968492

Hao, Y., Tang, J., and Cheng, Y. (2011). "Cooperative sybil attack detection for position based applications in privacy preserved VANETs," in 2011 IEEE Global Telecommunications Conference – GLOBECOM 2011, 1–5. doi:10.1109/GLOCOM.2011.6134242

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Spanoudakis, G., Demetriou, G., and Katos, V. (2019). MobileTrust: Secure knowledge integration in VANETs. *ACM Trans. Cyber-Phys. Syst.* 4 (3), 1–25. doi:10.1145/3364181

Hbaieb, A., Ayed, S., and Chaari, L. (2022). A survey of trust management in the Internet of Vehicles. *Comput. Netw.* 203, 108558. doi:10.1016/j.comnet.2021.108558

Hong, X., Huang, D., Gerla, M., and Cao, Z. (2008). "SAT: Situation-aware trust architecture for vehicular networks," in Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture, MobiArch'08, USA, 31–36.

Hou, L., Yao, N., Lu, Z., Zhan, F., and Liu, Z. (2021). Tracking based mix-zone location privacy evaluation in VANET. *IEEE Trans. Veh. Technol.* 70 (10), 10957–10969. doi:10.1109/TVT.2021.3109065

Hu, Y. C., Perrig, A., and Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless networksTwenty-second annual joint conference of the IEEE computer and communications. *IEEE INFOCOMIEEE Soc.* 3, 1976–1986. doi:10.1109/INFCOM.2003.1209219

Huang, X., Yu, R., Kang, J., and Zhang, Y. (2017). Distributed reputation management for secure and efficient vehicular edge computing and networks. *IEEE Access* 5, 25408–25420. doi:10.1109/ACCESS.2017.2769878

Hussain, R., Lee, J. Y., and Zeadally, S. (2021). Trust in VANET: A survey of current solutions and future research opportunities. *IEEE Trans. Intell. Transp. Syst.* 22 (5), 2553–2571. doi:10.1109/tits.2020.2973715

Hussain, R., Nawaz, W., Lee, J. Y., Son, J., and Seo, J. T. (2016). A hybrid trust management framework for vehicular social networks. *Proc. Cso Net.* 2016, 214–225.

Inedjaren, Y., Maachaoui, M., Zeddini, B., and Barbot, J. P. (2021). Blockchain-based distributed management system for trust in VANET. *Veh. Commun.* 30, 100350. doi:10.1016/j.vehcom.2021.100350

Iqbal, R., Butt, T. A., Afzaal, M., and Salah, K. (2019). Trust management in social Internet of Vehicles: Factors, challenges, blockchain, and fog solutions. *Int. J. Distrib. Sens. Netw.* 15 (1), 155014771982582. doi:10.1177/1550147719825820

Jalalia, M., and Aghaee, N. G. (2011). A fuzzy reputation system in vehicular ad hoc networks. *Procedia Comput. Sci.* 5, 951–956. doi:10.1016/j.procs.2011.07.134

Javaid, U., Aman, M. N., and Sikdar, B. (2019). "DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart

contracts," in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 1–5. doi:10.1109/VTCSpring.2019.8746499

Jiang, Y., Ge, S., and Shen, X. (2020). AAAS: An anonymous authentication scheme based on group signature in VANETs. *IEEE Access* 8, 98986–98998. doi:10.1109/ACCESS.2020.2997840

Jordan, M., Paredes, C. I., and Aguilar-Igartua, M. (2020). "Detection of position falsification attacks in VANETs applying trust model and machine learning," in MSWiM '20: 23rd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 9–16.

Joshua, C. J., Duraisamy, R., and Varadarajan, V. (2019). A reputation based weighted clustering protocol in VANET: A multi-objective firefly approach. *Mob. Netw. Appl.* 24, 1199–1209. doi:10.1007/s11036-019-01257-z

Kerrache, C. A., Calafate, C. T., Cano, J. C., Lagraa, N., and Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access* 4, 9293–9307. doi:10.1109/access.2016.2645452

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., and Abdullah, J. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors* 19 (22), 4954. doi:10.3390/s19224954

Khan, M. A., Kumar, N., Mohsan, S. A. H., Khan, W. U., Nasralla, M. M., Alsharif, M. H., et al. (2022). Swarm of UAVs for network management in 6G: A technical review. *IEEE Trans. Netw. Serv. Manage.* 2022, 3213370. doi:10.1109/TNSM.2022.3213370

Kudva, S., Badsha, S., Sengupta, S., Hung, M. L., Khalil, I., and Atiquzzaman, M. (2021). A scalable blockchain based trust management in VANET routing protocol. *J. Parallel Distrib. Comput.* 152, 144–156. doi:10.1016/j.jpdc.2021.02.024

Lee, E. J., and Bae, I. H. (2014). A reputation-based adaptive trust management system for vehicular clouds. *TRIDENTCOM* 2014, 77–86.

Levente, B., Holczer, T., Weimerskirch, A., and Whyte, W. (2009). "Slow: A practical pseudonym changing scheme for location privacy in VANETs," in Vehicular Networking Conference (VNC) (Tokyo, Japan: IEEE).

Li, B., Liang, R., Zhu, D., Chen, W., and Lin, Q. (2021). Blockchain-based trust management model for location privacy preserving in VANET. *IEEE Trans. Intell. Transp. Syst.* 22 (6), 3765–3775. doi:10.1109/TITS.2020.3035869

Li, F., Guo, Z., Zhang, C., Li, W., and Wang, Y. (2021). ATM: An active-detection trust mechanism for VANETs based on blockchain. *IEEE Trans. Veh. Technol.* 70 (5), 4011–4021. doi:10.1109/TVT.2021.3050007

Li, J., Xing, R., Su, Z., Zhang, N., Hui, Y., Luan, T. H., et al. (2020). Trust based secure content delivery in vehicular networks: A bargaining game theoretical approach. *IEEE Trans. Veh. Technol.* 69 (3), 3267–3279. doi:10.1109/tvt.2020.2964685

Li, W., and Song, H. (2016). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* 17 (4), 960–969. doi:10.1109/tits.2015.2494017

Li, X., Liu, J., Li, X., and Sun, W. (2013). "RGTE: A reputation-based global trust establishment in VANETs," in Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13) (Xi'an, China: IEEE), 210–214.

Lik, M., Mohtashemi, M., and Halberstadt, A. (2002). *A computational model of trust and reputation* in Hawaii International Conference on System Sciences IEEE.

Liu, X., Huang, H., Xiao, F., and Ma, Z. (2020). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. *IEEE Internet Things J.* 7 (5), 4101–4112. doi:10.1109/JIOT.2019.2957421

Lu, Z., Liu, W., Wang, Q., Qu, G., and Liu, Z. (2018b2018). A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* 6, 45655–45664. doi:10.1109/access.2018.2864189

Lu, Z., Qu, G., and Liu, Z. (2019). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* 20 (2), 760–776. doi:10.1109/tits.2018.2818888

Lu, Z., Wang, Q., Qu, G., and Liu, Z. (2018a). Bars: A blockchain-based anonymous reputation system for trust management in VANETs. *TrustCom/BigDataSE* 2018, 98–103.

Luo, B., Li, X., Weng, J., Guo, J., and Ma, J. (2020). Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Trans. Veh. Technol.* 69 (2), 2034–2048. doi:10.1109/TVT.2019.2957744

Ma, Z., Richard Yu, F., Jiang, X., and Boukerche, A. (2020). "Trustworthy traffic information sharing secured via blockchain in VANETs," in DIVANet '20: Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 33–40.

Mahmood, A., Butler, B., Zhang, W. E., Sheng, Q. Z., and Siddiqui, S. A. (2019). "A hybrid trust management heuristic for VANETs," in 2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops (Kyoto, Japan: IEEE), 748–752.

Mahmood, A., Sheng, Q. Z., Ali Siddiqui, S., Sagar, S., Zhang, W. E., Suzuki, H., et al. (2021). When trust meets the internet of vehicles: Opportunities, challenges, and future prospects. *CIC* 2021, 60–67.

Mao, M., Peng, Y., Hu, T., Zhang, Z., Lu, X., and Lei, J. (2021). Hierarchical hybrid trust management scheme in SDN-enabled VANETs. *Mob. Inf. Syst.* 2021, 7611619. doi:10.1155/2021/7611619

Maskey, S. R., Badsha, S., Sengupta, S., and Khalil, I. (2021). Reputation-based miner node selection in blockchain-based vehicular edge computing. *IEEE Consum. Electron. Mag.* 10 (5), 14–22. doi:10.1109/MCE.2020.3048312

Mehdi, M. M., Raza, I., and Hussain, S. A. (2017). A game theory based trust model for vehicular ad hoc networks (VANETs). *Comput. Netw.* 121, 152–172. doi:10.1016/j.comnet.2017.04.024

Mejri, M. N., Ben-Othman, J., and Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* 1 (2), 53–66. doi:10.1016/j.vehcom.2014.05.001

Mikavica, B., and Kostic-Ljubisavljevic, A. (2021). Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. *J. Supercomput.* 77 (9), 9520–9575. doi:10.1007/s11227-021-03659-x

Movahedi, Z., Hosseini, Z., Bayan, F., and Pujolle, G. (2016). Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey. *IEEE Commun. Surv. Tutorials* 18 (2), 1287–1309. doi:10.1109/comst.2015.2496147

Nadeem, T., Dashtinezhad, S., Liao, C., and Iftode, L. (2004). Trafficview: Traffic data dissemination using car-to-car communication. *Sigmob. Mob. Comput. Commun. Rev.* 8 (3), 6–19. doi:10.1145/1031483.1031487

Oluoch, J. (2016). "A distributed reputation scheme for situation awareness in Vehicular Ad Hoc Networks (VANETs)," in IEEE International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (San Diego, CA, USA: IEEE).

Ortega, V., Bouchmal, F., and Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. *IEEE Veh. Technol. Mag.* 13 (2), 121–127. doi:10.1109/mvt.2018.2813422

Otoum, S., Al Ridhawi, I., and Mouftah, H. T. (2020). "Blockchain-supported federated learning for trustworthy vehicular networks," in GLOBECOM 2020 – 2020 IEEE Global Communications Conference, 2020, 1–6. doi:10.1109/GLOBECOM42002.2020.9322159

Oubabas, S., Aoudjit, R., Rodrigues, J. J., and Talbi, S. (2018). Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Veh. Commun.* 13, 128–138. doi:10.1016/j.vehcom.2018.08.001

Park, S., Aslam, B., and Zou, C. C. (2011). "Long-term reputation system for vehicular networking based on vehicle's daily commute routine," in Proceedings of the 2011 IEEE Consumer Communications and Networking Conference (CCNC '11), Las Vegas, Nev, USA, 436–441.

Parno, B., and Perrig, A. (2005). *Challenges in securing vehicular networks*. College Park, MD, USA: Proc. Workshop HotNets-IV, 1–6.

Patel, A., Shah, N., Limbasiya, T., and Das, D. (2019). "VehicleChain: Blockchain-based vehicular data transmission scheme for smart city," in 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), 661–667. doi:10.1109/SMC.2019.8914391

Pathan, A. S. K. (2011). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. Boca Raton, Fla: CRC Press, Auerbach, 200.

Pathre, A., Agrawal, C., and Jain, A. (2013). "A novel defense scheme against DDOS attack in VANET," in Proceedings of the 10th International Conference on Wireless and Optical Communications Networks (WOCN), 1–5. doi:10.1109/WOCN.2013.6616194

Pedro, C., Zúquete, A., and Sargento, S. (2018). TROPHY: Trustworthy VANET routing with group authentication keys. *Ad Hoc Netw.* 71, 45–67. doi:10.1016/j.adhoc.2017.12.005

Pham, T. N. D., and Yeo, C. K. (2018). Adaptive trust and privacy management framework for vehicular networks. *Veh. Commun.* 13, 1–12. doi:10.1016/j.vehcom.2018.04.006

Premasudha, B. G., Ravi Ram, V., Miller, J., and Suma, R. (2016). A review of security threats, solutions and trust management in VANETs. *Int. J. Next-Generation Comput.* 7 (1).

Qafzezi, E., Kevin, B., Ampririt, P., Ikeda, M., Matsuo, K., and Leonard, B. (2021). A fuzzy-based approach for resource management in SDN-VANETs: Effect of trustworthiness on assessment of available edge computing resources. *J. High. Speed Netw.* 27 (1), 33–44. doi:10.3233/jhs-210650

Qin, Y., Huang, D., and Zhang, X. (2012). "VehiCloud: Cloud computing facilitating routing in vehicular networks," in 2012 IEEE 11th International

Conference on Trust, Security and Privacy in Computing and Communications, 1438–1445. doi:10.1109/TrustCom.2012.16

Raghav, R. S., Danu, R., Ramalingam, A., and Krishna Kumar, G. (2013). Detection of node impersonation for emergency vehicles in VANET. *Int. J. Eng. Res. Technol.* 02 (12).

Rahman, S., and Hengartner, U. (2007). "Secure vehicle crash reporting in vehicular Ad hoc networks," in SecureComm 2007, 443–452.

Raya, M., Aziz, A., and Hubaux, J. (2006). "Efficient secure aggregation in VANETs," in VANET'06: Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks, 67–75.

Raya, M., and Hubaux, J. (2007). Securing vehicular ad hoc networks. *J. Comput. Secur.* 15 (1), 39–68. doi:10.3233/JCS-2007-15103

Raya, M., and Hubaux, J. (2005b). "Security aspects of inter-vehicle communications," in Proceedings of the 5th Swiss Transport Research Conference (STRC), Ascona, Switzerland, March 2005.

Raya, M., and Hubaux, J. (2005a). "The security of vehicular ad hoc networks," in SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 11–21.

Raya, M., Papadimitratos, P., Gligor, V., and Hubaux, J. P. (2008). "On datacentric trust establishment in ephemeral ad hoc networks," in IEEE INFOCOM 2008. The 27th Conference on Computer Communications, 1238–1246.

Raza, S., Wang, S., Ahmed, M., and Anwar, M. R. (2019). A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions. *Wirel. Commun. Mob. Comput.* 2019, 3159762. doi:10.1155/2019/3159762

Sagar, S., Javaid, N., Khan, Z. A., Saqib, J., Bibi, A., and Bouk, S. H. (2012). "Analysis and modeling experiment performance parameters of routing protocols in MANETs and VANETs. in "2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 1867–1871. doi:10.1109/TrustCom.2012.89

Sakiz, F., and Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Netw.* 61, 33–50. doi:10.1016/j.adhoc.2017.03.006

Sataraddi, M. J., and Kakkasageri, M. S. (2020). Hybrid routing protocol for VANETs: Delay and trust based approach. *J. High Speed Netw.* 26 (4), 275–290. doi:10.3233/jhs-200644

Sataraddi, M. J., and Kakkasageri, M. S. (2019). "Trust and delay based routing for VANETs," in 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS 2019) (Goa, India: IEEE), 1–6. doi:10.1109/ANTS47819.2019.9118159

Satoshi, N. (2019). Bitcoin—open source P2P money. Available at: https://bitcoin.org/en/.

Serna, J., Luna, J., and Medina, M. (2009). Geolocation-based trust for vanet's privacy. *J. Inf. Assur. Secur.* 4, 432–439.

Serna, J. M., Jesus, L., and Manel, M. (2008). "Geolocation-based trust for vanet's privacy," in 2008 The Fourth International Conference on Information Assurance and Security, 287–290.

Shaik, S., and Ratnam, D. V. (2022). A trust based energy and mobility aware routing protocol to improve infotainment services in VANETs. *Peer-to-Peer Netw. Appl.* 15 (1), 576–591. doi:10.1007/s12083-021-01272-6

Sheikh, M. S., and Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. *Wirel. Commun. Mob. Comput.* 2019, 2423915. doi:10.1155/2019/2423915

Shen, J., Wang, C., Lai, J. -F., Xiang, Y., and Li, P. (2019). CATE: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* 68 (11), 11213–11226. doi:10.1109/TVT.2019.2938968

Shibin, W., and Nianmin, Y. (2019). A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs. *Wirel. Netw.* 25 (3), 1099–1115. doi:10.1007/s11276-018-1681-8

Siddiqui, S. A., Mahmood, A., Zhang, W. E., and Sheng, Q. Z. (2019). "Poster: A machine learning based hybrid trust management heuristic for vehicular ad hoc networks," in MobiCom '19: The 25th Annual International Conference on Mobile Computing and Networking, 1–3.

Slama, A., Lengliz, I., and Belghith, A. (2018). "TCSR: An AIMD trust-based protocol for secure routing in VANET," in 2018 International Conference on Smart Communications and Networking (SmartNets 2018), 1–8. doi:10.1109/SMARTNETS.2018.8707389

Soleymani, S. A., Abdullah, A. H., Hassan, W. H., Hossein Anisi, M., Goudarzi, S., Baee, M. A. R., et al. (2015). Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* 2015, 146. doi:10.1186/s13638-015-0353-y

Soleymani, S. A., Goudarzi, S., Anisi, M. H., Kama, N., Ismail, S. A., Azmi, A., et al. (2020). A trust model using edge nodes and a Cuckoo filter for securing VANET under the NloS condition. *Symmetry* 12 (4), 609. doi:10.3390/sym12040609

Souissi, I., Ben Azzouna, N., and Berradia, T. (2019). Trust management in vehicular ad hoc networks: A survey. *Int. J. Ad Hoc Ubiquitous Comput.* 31 (4), 230–243. doi:10.1504/ijahuc.2019.10022743

Sumithra, S., and Vadivel, R. (2018). "An overview of various trust models for VANET security establishment," in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–7.

Sumithra, S., and Vadivel, R. (2019). "NB-FTBM model for entity trust evaluation in vehicular ad hoc network security," in *Ubiquitous communications and network computing. UBICNET 2019. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering.* Editors N. Kumar and R. Venkatesha Prasad (Cham: Springer), Vol. 276.

Sumra, I. A., Ahmad, I., Hasbullah, H., and bin Ab Manan, J. -l. (2011a). "Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET)," in Proceedings of the 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 1–8.

Sumra, I. A., Manan, J. A. B., and Hasbullah, H. (2011b). "Timing attack in vehicular network," in Proceedings of the 15th WSEAS international conference on Computers, 151–155.

Sun, D., Zhao, H., and Cheng., S. (2016). A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS. *Secur. Comm. Netw.* 9 (18), 5710–5723. doi:10.1002/sec.1730

Sun, Y., Zhang, B., Zhao, B., Su, X., and Su, J. (2015). Mix-zones optimal deployment for protecting location privacy in VANET. *Peer. Peer. Netw. Appl.* 8, 1108–1121. doi:10.1007/s12083-014-0269-z

Tangade, S., Manvi, S. S., and Hassan, S. (2019). "A deep learning based driver classification and trust computation in VANETs," in 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 1–6. doi:10.1109/VTCFall.2019.8891462

Tangade, S., Manvi, S. S., and Lorenz, P. (2020). Trust management scheme based on hybrid cryptography for secure communications in VANETs. *IEEE Trans. Veh. Technol.* 69 (5), 5232–5243. doi:10.1109/TVT.2020.2981127

Tian, Z., Gao, X., Su, S., Qiu, J., Du, X., and Guizani, M. (2019). Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory. *IEEE Trans. Veh. Technol.* 68 (6), 5971–5980. doi:10.1109/tvt.2019.2910217

Vaibhav, A., Shukla, D., Das, S., Sahana, S., and Johri, P. (2017). Security challenges, authentication, application and trust models for vehicular ad hoc network- A survey. *Int. J. Wirel. Microw. Technol.* 7 (3), 36–48. doi:10.5815/ijwmt.2017.03.04

Vegni, V. M., and Loscrí, V. (2015). A survey on vehicular social networks. *IEEE Commun. Surv. Tutorials* 17 (4), 2397–2419.

Venitta Raj, R., and Balasubramanian, K. (2021). RETRACTED article: Trust aware similarity-based source routing to ensure effective communication using game-theoretic approach in VANETs. *J. Ambient. Intell. Humaniz. Comput.* 12, 6781–6791. doi:10.1007/s12652-020-02306-2

Verma, K., Hasbullah, H., and Kumar, A. (2013). Prevention of DoS attacks in VANET. *Wirel. Pers. Commun.* 73 (1), 95–126. doi:10.1007/s11277-013-1161-5

Wang, C., Shen, J., Lai, J. F., and Liu, J. (2021). B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs. *IEEE Trans. Emerg. Top. Comput.* 9 (3), 1386–1396. doi:10.1109/TETC.2020.2978866

Wang, J., Zhang, M., Gu, X., Wang, T., Wang, J., and Chen, L. (2021). Research of vehicular cloud storage resource management based on trust mechanism. *Int. J. Distrib. Sens. Netw.* 17 (3), 155014772110063. doi:10.1177/15501477211006346

Wang, J., Zhang, Y., Wang, Y., and Gu, X. (2016). RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs. *Int. J. Distributed Sens. Netw.* 2016, 6138251. doi:10.1155/2016/6138251

Wang, S., and He, Y. (2016). "A trust system for detecting selective forwarding attacks in VANETs," in *Big data computing and communications. BigCom 2016.* Editors Y. Wang, G. Yu, Y. Zhang, Z. Han, and G. Wang (Cham: Springer), Vol. 9784. doi:10.1007/978-3-319-42553-5_32

Wex, P., Breuer, J., Held, A., Leinmuller, T., and Delgrossi, L. (2008). "Trust issues for vehicular ad hoc networks," in Proceedings of the 67th IEEE Vehicular Technology Conference (VTC Spring).

Wu, A., Ma, J., and Zhang, S. (2011). "RATE: A RSU-aided scheme for data-centric trust establishment in VANETs," in Proceedings of the 7th International

Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '11) (Wuhan, China: IEEE), 1–6.

Xia, H., Zhang, S., Li, B., Li, L., and Cheng, X. (2018). Towards a novel trust-based multicast routing for VANETs. *Secur. Commun. Netw.* 2018, 7608198. doi:10.1155/2018/7608198

Xie, L., Ding, Y., Yang, H., and Wang, X. (2019). Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. *IEEE Access* 7, 56656–56666. doi:10.1109/ACCESS.2019.2913682

Xu, Q., Mak, T., Ko, J., and Sengupta, R. (2004). "Vehicle-to-vehicle safety messaging in DSRC," in VANET'04: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, Philadelphia, 19–28.

Ya, X., Shihui, Z., and Bin, S. (2015). Trusted GPSR protocol without reputation faking in VANET. *J. China Univ. Posts Telecommun.* 22 (5), 22–55. doi:10.1016/s1005-8885(15)60676-8

Yan, G., Wen, D., Olariu, S., and Weigle, M. C. (2013). Security challenges in vehicular cloud computing. *IEEE Trans. Intell. Transp. Syst.* 14 (1), 284–294. doi:10.1109/tits.2012.2211870

Yang, N. (2013). A similarity based trust and reputation management framework for VANETs. *Int. J. Future Generation Commun. Netw.* 6 (2), 25–34.

Yang, Q., and Wang, H. (2015). Toward trustworthy vehicular social networks. *IEEE Commun. Mag.* 53 (8), 42–47. doi:10.1109/mcom.2015.7180506

Yang, S., Liu, Z., Li, J., Wang, S., and Yang, F. (2016). Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation. *Mob. Inf. Syst.* 2016, 5254141. doi:10.1155/2016/5254141

Yang, Y. T., Li-Der, C., Tseng, C. W., Tseng, F. H., and Liu, C. C. (2019). Blockchain-based traffic event validation and trust verification for VANETs. *IEEE Access* 7, 30868–30877. doi:10.1109/access.2019.2903202

Ying, B., and Makrakis, D. (2015). "Reputation-based pseudonym change for location privacy in vehicular networks," in Proceedings of IEEE Int. Conf. Commun. (ICC), Jun. 2015, 7041–7046.

Yu Chih, W., and Chen, Y. M. (2012). "Efficient self-organized trust management in location privacy enhanced VANETs," in International Workshop on Information Security Applications 2012.

Yu Chih, W., Chen, Y. M., and Shan, H. L. (2011). "Beacon-based trust management for location privacy enhancement VANETs," in 2011 13th Asia-Pacific Network Operations and Management Symposium.

Yuanpan, Z., Chen, G., and Guo, L. (2020). An anonymous authentication scheme in VANETs of smart city based on certificateless group signature. *Complexity* 2020, 1378202. doi:10.1155/2020/1378202

Zeng, C., Wang, Y., Liang, F., and Peng, X. (2020). "Fengyi: Trusted data sharing in VANETs with blockchain," in 2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC), 11–20. doi:10.1109/PRDC50213.2020.00012

Zhang, C., Chen, K., Zeng, X., and Xue, X. (2018). Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in VANETs. *IEEE Access* 6, 59860–59870. doi:10.1109/ACCESS.2018.2875678

Zhang, C., Zhu, L., Xu, C., Sharif, K., Guizani, M., Liu, X., et al. (2022). Tppr: A trust-based and privacy-preserving platoon recommendation scheme in VANET. *IEEE Trans. Serv. Comput.* 15 (2), 806–818. doi:10.1109/TSC.2019.2961992

Zhang, D., Yu, F. R., and Yang, R. (2018). "A machine learning approach for software-defined vehicular ad hoc networks with trust management," in 2018 IEEE Global Communications Conference (GLOBECOM), 1–6. doi:10.1109/GLOCOM.2018.8647426

Zhang, D., Yu, F. R., Yang, R., and Zhu, L. (2022). Software-defined vehicular networks with trust management: A deep reinforcement learning approach. *IEEE Trans. Intell. Transp. Syst.* 23 (2), 1400–1414. doi:10.1109/TITS.2020.3025684

Zhang, J. (2011). "A survey on trust management for VANETs," in 2011 IEEE International Conference on Advanced Information Networking and Applications, 105–112.

Zhang, J. (2012). Trust management for VANETs: Challenges, desired properties and future directions. *Int. J. Distributed Syst. Technol.* 3 (1), 48–62. doi:10.4018/jdst.2012010104

Zhang, L., and Xu, J. (2021). "Anonymous authentication scheme based on trust and blockchain in VANETs," in *algorithms and architectures for parallel processing. ICA3PP 2021, LNCS*. Editors Y. Lai, T. Wang, M. Jiang, G. Xu, W. Liang, and A. Castiglione (Cham: Springer), 13156, 473–488. doi:10.1007/978-3-030-95388-1_31

Zhiquan, L., Ma, J., Jiang, Z., Zhu, H., and Miao, Y. (2016). Lsot: A lightweight self-organized trust model in VANETs. *Mob. Inf. Syst.* 2016, 1–15. doi:10.1155/2016/7628231

Zhiquan, L., Weng, J., Ma, J., Guo, J., Feng, B., Jiang, Z., et al. (2020). Tcemd: A trust cascading-based emergency message dissemination model in VANETs. *IEEE Internet Things J.* 7 (5), 4028–4048. doi:10.1109/JIOT.2019.2957520

Glossary

3TAAV three-tier architecture for pseudonym-based anonymous authentication

5G fifth-generation mobile communication technology

AES Acknowledgment during Encounter Strategy

AI artificial intelligence

AIMD additive increase multicative decrease

ALD average link duration

ANN artificial neural network

BARS blockchain-based anonymous reputation system

BloVEC blockchain-based Vehicular Edge Computing

BOA bat optimization algorithm

BP back Propagation

ABPT bidding price-based transaction

CA certificate authority

CATE cloud-aided trustworthiness evaluation scheme

CCA centralized certification authority

CCN content-centric networking

CRL certificate revocation list

CRV cooperative relay vehicles

CSS context-aware semantic service

DDoS distributed denial of service

DI-Trust trust model based on dynamic incentive mechanism

DoS denial of service

DREAMS distributed reputation management solution

DL deep learning

DL-DCTC deep learning-based driver classification and trust computation

DNN deep neural network

DS dempster-shafer

DSDV destination sequenced distance vector

DSR dynamic source routing

DYMO dynamic manet on-demand

E2ED end-to-end delay

ECC elliptic curve cipher

E-ID entity identification

EM-ARP energy and mobility aware routing protocol

ETX expected transmission count

FL federated learning

FS-ANVPC fuzzy-based systems for assessment of nearby vehicle processing capabilities

GM general motors

GMP gnu multiple precision arithmetic lib

GPS global positioning system

GPSR geographic information routing protocol

GTBS game-theoretic broadcasting strategy

IBC identity-based cryptography

ICBT inter-vehicular communication trust model based on belief theory

IoTs internet of things

IoV internet of vehicles

kNN k-nearest neighbor

LSOT lightweight self-organized trust

ITS intelligent transportation system

LEA law enforcement authority

LET link expiration time

LoS line of sight

LR logistic regression

LTR long-term reputation

MANETs mobile ad-hoc networks

MDS misbehavior detection system

MLT maximum local trust

MMRT minimum message reachable time

MOFA multi objective firefly algorithm

NB-FTBM naive bayesian fuzzy trust boundary model

NLoS none-line of sight

NLT neighbor location table

NRO normalized routing overhead

OBU on-board units

P2P peer to peer

PBC pairing-based cryptography

PDR packet reception rate

PEPA performance evaluation process algebra

PKI public key infrastructure

PKI-CA public key infrastructure - certificate authority

PoE proof-of-event

PSS pseudonym server

PUFs physical unclonable functions

RATE roadside-unit aided trust establishment

RA-VTrust reputation-based adaptive vehicular trust model

RbMNS reputation-based mining node selection

RF random forest

RGTE reputation-based global trust establishment

RLC reputation label certificate

RPCLP reputation-based pseudonym change for location privacy

RSSI radio signal strength indicator

RSU fixed road-side units

RTP real-time transport protocol

RWCP reputation-based weighted clustering protocol

SAT situation-aware trust

SDN software-defined network

SDN-VANETs software defined vehicular ad hoc networks

SD-TDQL software defined and trust-based deep q-learning framework

SDVN software-defined vehicular network

SIoV social internet of vehicles

SNS social networking services

SVM support vector machine

TCE trust computation error

TCEMD trust cascading-based emergency message dissemination

T-CPS transportation cyber-physical system

TCSR trusted cryptographic secure routing

TDRL-RP trust-based deep reinforcement learning—routing protocol

TLM trusted ledger model

TRM trust and reputation management systems

TRMFS trust and reputation management framework based on the similarity mining technique

TROPHY trustworthy VANET routing with group authentication keys

TTP trusted third party

V2H vehicle-to-human

V2I vehicle-to-infrastructure

V2P vehicle-to-person

V2V vehicle-to-vehicle

VANETs vehicular ad-hoc networks

VCC vehicular cloud computing

VEC vehicular edge computing

VSNs vehicular social networks

WSNs wireless sensor networks