# When Trust Meets the Internet of Vehicles: Opportunities, Challenges, and Future Prospects

Adnan Mahmood[1], Quan Z. Sheng[1], Sarah Ali Siddiqui[1,3], Subhash Sagar[1], Wei Emma Zhang[2], Hajime Suzuki[3], and Wei Ni[3]
[1]School of Computing, Macquarie University, NSW 2109, Australia
[2]School of Computer Science, The University of Adelaide, SA 5005, Australia
[3]Cybernetics Group, CSIRO Data61, NSW 2122, Australia

***Abstract*—Recent technological breakthroughs in vehicular ad hoc networks and the Internet of Things (IoT) have transformed vehicles into smart objects thus paving the way for the evolution of the promising paradigm of the Internet of Vehicles (IoV), which is an integral constituent of the modern intelligent transportation systems. Simply put, IoV attributes to the *IoT-on-wheels*, wherein vehicles broadcast safety-critical information among one another (and their immediate ambiences) for guaranteeing highly reliable and efficacious traffic flows. This, therefore, necessitates the need to fully secure an IoV network since a single malicious message is capable enough of jeopardizing the safety of the nearby vehicles (and their respective passengers) and vulnerable pedestrians. It is also pertinent to mention that a malicious attacker, i.e., vehicle, is not only able to send counterfeited safety-critical messages to its nearby vehicles and the traffic management authorities but could further enable a compromised vehicle to broadcast both spoofed coordinates and speed-related information. It is, therefore, of the utmost importance that malicious entities and their messages be identified and subsequently eliminated from the network before they are able to manipulate the entire network for their malicious gains. This paper, therefore, delineates on the convergence of the notion of trust with the IoV primarily in terms of its underlying rationale. It further highlights the opportunities which transpire as a result of this convergence to secure an IoV network. Finally, open research challenges, together with the recommendations for addressing the same, have been discussed.**

***Index Terms*—Smart cities, Internet of vehicles, misbehavior detection, network security, and trust management.**

## I. Introduction

Over the past decade or so, significant cutting edge technological advancements in the promising paradigm of vehicular ad hoc networks and the Internet of Things (IoT) has expedited the emergence of the Internet of Vehicles (IoV) as a highly innovative technology, which has the potential of revolutionizing the intelligent transportation systems that are indispensable for the realization of the futuristic smart cities [1]. Intelligent IoV networks are capable of ensuring highly secure and safe traffic flows on the road by empowering smart vehicles duly equipped with storage and computational resources and next generation communication technologies for communicating safety-critical information with the (a) other vehicles in their neighborhood, (b) supporting roadside infrastructure, (c) backbone network, and (d) pedestrians via Vehicle to Everything (V2X) communication [2], [3]. It is pertinent to highlight that the safety-critical vehicular applications have strict performance requirements in contrast to the non-safety, i.e., infotainment, applications, and hence, a low-latency and highly secure IoV network is, in fact, imperative for the said purpose [4]. Figure 1 depicts an overview of V2X communication in an IoV landscape.

However, just like other ad hoc networks, IoV networks are prone to a number of external and internal security threats [5], and in fact, a single malicious message possesses the capability to compromise the entire network, thereby putting human lives to risk on the road. It is, therefore, indispensable to ensure that these malicious messages and the vehicles broadcasting them in an IoV network are identified within a shortest possible time and subsequently eliminated in an intelligent manner. Thus, the issues pertinent to the security of the IoV networks have gained a considerable level of attention of researchers from academic and industry [6]. As of date, the existing security solutions are categorized into two categories, i.e., cryptographic-based solutions and trust-based solutions. Cryptographic-based solutions usually employ certificates and public key infrastructure for the purposes of vehicles' identification and ensure that messages only broadcast from the authenticated vehicles, however, they are unable to inhibit any legitimate vehicle from broadcasting false information [7], [8]. It is due to this reason that the notion of trust was lately introduced in the literature for intelligently tackling the insider attacks in an IoV network.

Trust within an IoV network is referred to as the confidence of a vehicle, i.e., trustor, over the other vehicle's, i.e., trustee's, capability to share authentic, accurate, and reliable information [8], [9]. It has also been delineated in the research literature in terms of the belief of a trustor in any trustee for intelligently performing a certain task, or the sets of tasks, in an anticipated manner and perhaps within a particular time period [10]. Trust is generally ascertained in terms of the trust components and is usually an amalgamation of the direct trust and indirect trust for each vehicle. Direct trust manifests the direct observation of a trustor for a trustee, whereas, the indirect trust depicts the recommendations (opinions) of remaining one-hop neighbours in the immediate ambience of a trustee, i.e., target vehicle. The resulting trust score primarily depends on the weights assigned to each of the trust components and the quantification of these weights in its own essence is an intricate challenge since only precise weights could result in the accurate trust values. Also, trust is a dynamic entity and depends on numerous key factors, including but not limited to, the trustor's expectation over time, divergent traffic contexts, and varied applications and services.

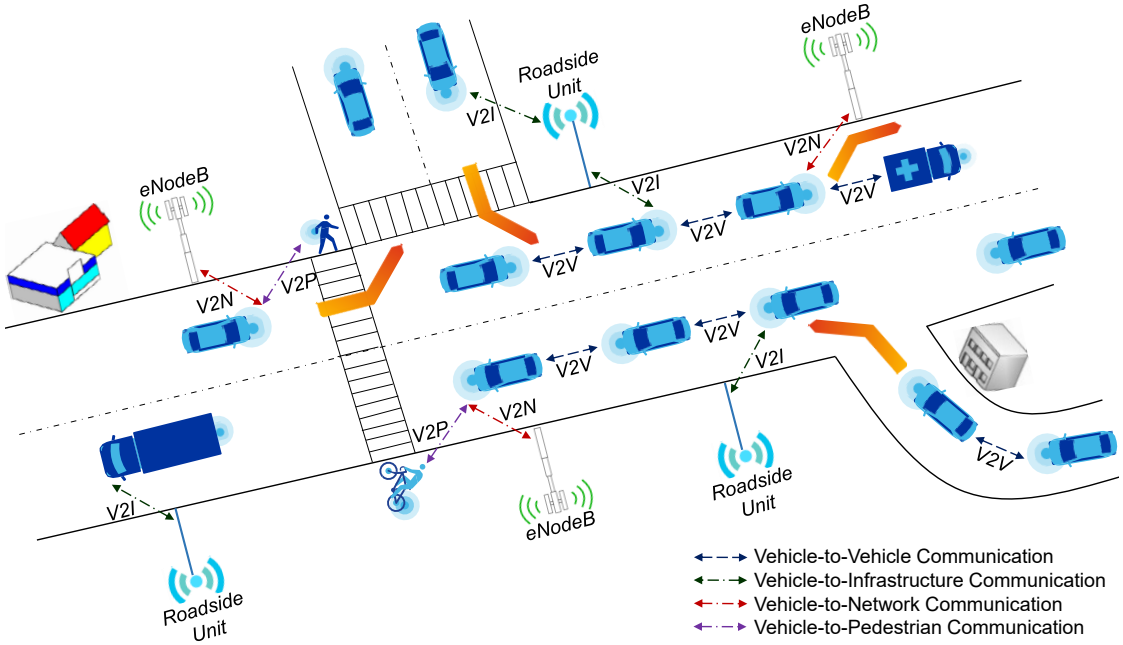


Fig. 1. An overview of V2X communication in an IoV landscape.

Moreover, once the aggregated trust has been ascertained for a trustee, an optimal threshold needs to be determined to identify the malicious vehicles, i.e., vehicles which satisfy the optimal threshold would be regarded as trustworthy, whereas, the ones below the optimal threshold are considered as untrustworthy in their nature. Hence, an optimal threshold is of the essence as if set too high would result in elimination of the trustworthy vehicles. Contrarily, if the optimal threshold is quite low, it would facilitate the untrustworthy vehicles to continue manipulating the IoV network for their malicious gains [11]. Unfortunately, the existing trust-based solutions have not delineated on these and a number of other IoV-related challenges in an appropriate manner and possess numerous inherent limitations, and hence, cannot be really deployed for the practical purposes.

In light of the aforementioned discussions, the paper-at-hand delineates at length the convergence of the notion of trust with the IoV in terms of not only its underlying rationale but also by highlighting the salient opportunities it offers for strengthening the security of an IoV network along with the challenges which should be intelligently addressed for realizing the deployments of trusted IoV networks in the context of the smart cities.

## II. Trust Management in the Internet of Vehicles

### A. Characteristics of an IoV Network

Whilst there are a considerable number of trust management mechanisms that can ascertain the trustworthiness of *users* and *things* within a traditional ad hoc wireless network, intelligent, efficacious, resilient, and scalable trust management solutions are particularly required for IoV primarily owing to its specific characteristics some of which are delineated below [12], [13]:

- Dynamicity – In contrast to traditional MANETs, vehicles in an IoV network are highly dynamic in their nature and traverse at diverse speeds, thereby resulting in a continual change of network topology. This further suggests that the neighbors of any particular vehicle are not permanent and the trust scores are usually ascertained via merely a single encounter instead of being frequently updated over time. Bootstrapping, therefore, is of a considerable significance in an IoV network and needs to be handled carefully.
- Resource Availability – Each vehicle in an IoV network possesses certain computation and storage resources and is primarily reliant on the same for carrying out a number of its safety-critical decisions based on the data accumulated through hundreds of onboard sensors. Furthermore, it is pertinent to highlight here that vehicles also offload data both to the edge and to the centralized clouds for the purposes of heavy computation, nevertheless, this comes at a cost of comprising stringent latency requirements and which are, in fact, highly indispensable for the successful realization of the safety-critical vehicular applications.
- Regulated – Vehicles in an IoV network are obligated to follow traffic regulations put forth by both the centralized and localized traffic management entities, and are further bounded by the road topologies.
- Opportunistic – Vehicles are opportunistic in nature since they are intermittently connected with the other vehicles, pedestrians, and the roadside infrastructure. This implies that vehicles interact with the other vehicles, pedestrians, and the roadside infrastructure if they fall in the communication range of one another.
- Non-deterministic – Unlike a deterministic behavior that could be easily related to its cause and is, therefore, predictable (i.e., just as is the case of deterministic networks, wherein an event could be guaranteed to transpire within

a particular duration of time), the IoV networks somehow possess non-deterministic characteristics primarily owing to the complicated nature of its entities and their intricate interrelationship. Although the mobility of the vehicles is generally predictable in IoV networks, it is the intelligent dishonest vehicles which remain in disguise, attains sufficient privileges, find an optimal opportunity for launching a sophisticated attack, and jeopardizes the entire network in a matter of no time.

### *B. The Essence of Trust Management in IoV*

As discussed earlier, vehicles within an IoV network communicate (interact) with one another in an attempt to carry out several safety-critical and non-safety vehicular applications. It is, therefore, indispensable that the recipient of such messages are absolutely certain about the quality of these messages, and the vehicles disseminating them, before any sort of subsequent action or decision is taken on the same. For instance, consider the safety-critical applications such as (a) a hazardous location alert intimating any vehicle of a potentially hazardous situation along its anticipated trajectory, and accordingly, recommending it to speed down and diverge towards an alternate route, or (b) a forward collision warning detecting and intimating of imminent collision, and therefore, recommending the emergency brakes to avoid any fatal accident. If the received messages are authentic, accurate, and reliable, a connected or an autonomous vehicle has to either take an alternate route in the scenario of a hazardous alert or has to apply sudden brakes for mitigating an imminent crash in the case of a forward collision alert. On the contrary, if these received messages are inauthentic, inaccurate, and unreliable, and a connected or an autonomous vehicle is unable to ascertain the same and ends up heeding to the wrong information contained therein, then it would either diverge on an unwarranted route, or alternatively, an unwarranted sudden brake on a fast moving highway would be resulting into rear-end collisions and unfortunate road fatalities.

Whilst a number of cryptographic-based solutions have been proposed in the research literature [8], [14], [15], nevertheless, cryptographic-based solutions on their own are unable to tackle the entire vehicular security aspects, and particularly, the inside attackers since they are in possession of valid certificates, have a considerable knowledge of the network, are insidious in their nature, and, therefore, can cause a catastrophic damage. Trust-based solutions are hence considered as an additional security mechanism in order to overcome the inherent shortcomings of the cryptographic-based solutions. Literature also suggests that the cryptographic-based solutions and the trust-based solutions could be employed to tackle a single attacker or even a group of attackers, and rational and irrational attacks [16]. However, the cryptographic-based solutions have high network overhead and are known for introducing excessive delays in contrast to the trust-based solutions and are, therefore, not optimal for the delay sensitive safety-critical vehicular applications.

Trust, as one of the solutions for realizing security in IoV, still remains in its infancy. In an IoV environment, the rationale behind the trust models is to guarantee a trusted dissemination of the data by identifying and subsequently revoking malicious vehicles and the compromised messages generated from them. Trust models are particularly categorized into (a) entity-centric trust models, (b) data-centric trust models, and (c) hybrid trust models, and a brief illustration pertinent to them is delineated as follows [17]–[19]:

- Entity-centric Trust Models – Entity-centric trust models primarily intend to eliminate the malicious vehicles from an IoV network by ascertaining the trustworthiness of the vehicles (entities) disseminating messages. They rely on a reputation-based trust evaluation mechanism, and hence, the opinions from the neighboring vehicles are taken into consideration in order to ascertain the trustworthiness of the source vehicles.
- Data-centric Trust Models – Contrary to the entity-centric trust models, data-centric trust models intend to eliminate the malicious messages from an IoV network instead of eliminating the vehicles. This could be, therefore, realized in two ways, i.e., either the messages disseminated by the malicious vehicles could be eliminated or messages could be verified provided they are not encrypted.
- Hybrid Trust Models – Hybrid trust models encompass the characteristics of both the entity-centric trust models and the data-centric trust models. Accordingly, the trustworthiness of both the vehicles and the data disseminated via them is ascertained.

It is also pertinent to note that a number of trust management mechanisms primarily falling into one of the above stipulated categories have already been proposed in the research literature and leverages either the game theory, blockchain, fuzzy logic, machine learning, or other similar approaches. An overview of such schemes is beyond the scope of this paper. Nevertheless, the readers may like to refer to our recent survey [20] depicting the state-of-the-art of trust management in IoV.

### *C. Trust Attributes*

Trust attributes are considered as one of the most indispensable constituents of a trust-based solution. They are essentially the quality metrics which facilitate the vehicles in ascertaining the trust of any other vehicle within an IoV network. The more the number of trust attributes employed by a trustor in the trust computation process, the more accurate would be the resulting trust segment. However, too many trust attributes also implies introducing a considerable computational overhead which can prove risky in safety-critical vehicular scenarios. Therefore, it is imperative to identify the influential trust attributes that can facilitate a trustor in ascertaining an accurate trust score of a trustee in a shortest possible time. Some of such attributes that should be a part of any trust-based IoV solution are delineated as follows:

- Similarity – Similarity generally implies the state of being similar in terms of a particular aspect. The same is true for the IoV networks, wherein similarity has been ascertained in two different ways, i.e., how well the travelling patterns of a trustor resembles to that of a trustee, and the degree

TABLE I
A COMPARISON OF THE TRUST ATTRIBUTES IN HUMANS VIS-À-VIS INTERNET OF VEHICLES

| Trust Attribute | Humans | Internet of Vehicles |
|---|---|---|
| Similarity | Similarity amongst the behavior of two humans is primarily ascertained in terms of their biases (personal preferences – likes and dislikes), rationale for such personal preferences, emotional reactions, decision making, cultures, friends, etc. | Similarity in vehicles is measured in terms of (a) how well the travelling patterns of a trustor and a trustee resembles to one another, or (b) the degree of similar content or services accessed by both the trustor and the trustee. |
| Familiarity | Humans, unconsciously, tend to accord preference to other humans that they are usually familiar with. In fact, the more often a human see another human, the more attraction they tend to develop over time. Even if the stimuli they are being exposed to overtime is itself negative, humans tend to find comfort in the familiarity of the same. Hence, humans don't risk the unfamiliar owing to the fear of getting hurt. | Familiarity between any two vehicles manifest how well a trustor is acquainted with a trustee and is measured in terms of the frequency of interactions between them. It has also been ascertained in terms of the degree of trust and distrust of a trustor on a trustee, confidence of a trustor's knowledge pertinent to a trustee, and willingness of a trustor to believe in a trustee. |
| Timeliness | Human behavior primarily relates to the way a human act or interact with other humans in its ambient environment and is dependent on and influenced by a number of factors. It can change gradually and even drastically, and therefore, humans tend to believe more in the recent observations and interactions as compared to the historical ones. | Timeliness in an IoV network implies freshness of any reputation segment. The more fresh is the reputation segment, the more recent behavior of a vehicle could be ascertained. This is of key essence since the recent reputation segments could be matched with the historical ones to figure out any abnormal behavior. |
| Duration of Interactions | Humans truly believe in the duration of their interactions since this is largely known to facilitate them in ascertaining the strength of their relationship, and in turn, the feasibility of continuing the same. This is the most important attribute as other trust attributes are somehow impacted owing to it. | In an IoV network, the longer is the duration of any interaction amongst a trustor and a trustee, the more conclusive trust score of a trustee can be ascertained. This assessment could be positive or negative, and in fact, computationally intensive but indisputable for making a judgment. |
| Effective Distance | Long-distance relationships amongst humans are somewhat prone to failure. The greater is the distance among any two individuals, the less likely they are able to relate over time with one another. | The greater is the distance between a trustor and a trustee reporting a particular event, the more improbable it would be for a trustor (and it's immediate neighbors) to ascertain the legitimacy of the said event. |

of similar content or services accessed by both the trustor and the trustee [21], [22].

- Familiarity – Familiarity delineates a close acquaintance with something. In simpler terms, the more knowledge we possess about something, the more aware we are with the characteristics of that particular thing. In an IoV network, familiarity suggests how well a trustor is acquainted with a trustee and is ascertained in terms of the frequency of the interactions between a trustor and a trustee [23]. It has also been ascertained via subjective logic which employs opinions for representing the subjective belief and models belief, disbelief, uncertainty, and base rate, wherein belief and disbelief suggests a measure of the degree of trust and distrust of a trustor on a trustee respectively, uncertainty refers to the confidence of a trustor's knowledge pertinent to a trustee, and base rate here implies the willingness of a trustor to believe in a trustee [24], [25].
- Timeliness – Timeliness is one of the most indispensable attributes in determining the trust of a trustee and is ascertained in terms of the freshness of a reputation segment. The more fresh is the reputation segment, the more recent behavior of a trustee could be established. This, therefore, could be employed to identify the presence of a malicious vehicle within an IoV network. For instance, an intelligent malicious vehicle with historically low trust scores might attract high trust scores as it begins to actively participate in the network in its disguise mode. Accordingly, the most recent reputation segments are usually compared with the previous reputation segments to trace the abrupt patterns. On the contrary, in the case of honest vehicles, the recent reputation segments are issued a relatively higher weight as compared to the old reputation segments primarily for the purpose of trust aggregation. This, in turn, provides a much clearer situation pertinent to the current state of the honest vehicles and subsequently facilitates in deciding as to which ones of those could be used for primarily routing safety-critical information in an IoV network [26]–[28].
- Duration of the Interactions – The duration of an interaction between a trustor and a trustee is of the essence since it is proportional to the cooperative behavior between the two. The longer is the duration of an interaction between a trustor and a trustee, the more conclusive trust score of a trustee could be ascertained. On the contrary, the shorter time a trustor and a trustee spend interacting between one another, the less knowledge a trustor possess pertinent to a trustee's behavior and strengths [29].
- Effective Distance – Effective distance between a trustor and a trustee is yet another intelligent geographical measure to ascertain the trust of a trustee reporting a particular event. The greater is the distance between a trustor and a trustee reporting an event, the more improbable it would be for a trustor and it's immediate neighbors to ascertain the legitimacy of the said event. Contrarily, if the distance between a trustor and a trustee reporting a certain event is less, the trustor and its immediate neighbors would be capable of attesting the legitimacy of the said event since they are much likely to be aware of the events transpiring in their message evaluation range [1], [30].

If carefully observed, these trust attributes are pretty similar to the ones that humans employ for ascertaining the trust of the

other humans. Surprisingly enough, there is a sharp similarity between the two and this makes perfect sense since trust is an intrinsic characteristic of humans and which subconsciously is also reflected in their engineered trust models. This, therefore, implies that some additional influential trust attributes for IoVs could be extracted from the domain of human behavior which has been well researched for numerous decades. A comparison of the trust attributes in humans vis-à-vis IoV is illustrated in Table I.

### D. Trust-related Attacks in an IoV Network

There are numerous sorts of sophisticated attacks that could have a direct impact on the trustworthiness of any vehicle in an IoV network. Such sorts of attacks include (a) self-promoting attacks, on-off attacks, opportunistic service attacks, selective behavior attacks – manifesting the class of attacks with the underlying rationale of *self-interest*; and (b) bad mouthing attacks and good mouthing attacks – classified as the *reputation-based attacks*. These attacks are briefly delineated as follows:

- Self-promoting Attack – In a self-promoting attack, a malicious vehicle continuously enhances its own reputation for acquiring considerable privileges in an IoV network in a bid to manipulate the entire network for its malicious gains. In order to materialize such an attack, a malicious vehicle can generate Sybil identities to augment its trust, thereby cheating the conventional reputation mechanisms.
- On-off Attack – In an on-off attack, a malicious vehicle alters between a good and a bad behavior in a randomized manner. This not only facilitates a malicious vehicle as to remain undetected while engaging in malign activities but further guarantees that it is able to manage an appropriate reputation score in an IoV network. If remains undetected for an extended duration, such sort of malicious vehicles may end up gaining significant privileges in the network.
- Opportunistic Service Attack – In an opportunistic service attack, a malicious vehicle lay quite low by acting primarily in disguise mode until it has been presented with some sort of an opportunity for launching a sophisticated attack in an IoV network. Therefore, a malicious vehicle keeps on providing a better service as to gain a higher reputation and perhaps the trust of its neighboring vehicles, and once it has duly established the same, it acts opportunistically and begins furnishing the bad services.
- Selective Behavior Attack – In a selective behavior attack, a malicious vehicle performs good for a particular set of services, whereas, bad for the others. For instance, in the case of network services demanding lower computational requirements, a malicious vehicle might perform good in order to preserve its key resources in an IoV network. It is pertinent to highlight here that vehicles in a collaborative network cooperate with one another in a bid to facilitate the network to execute its services in an efficient manner, and accordingly, justify their due participation within this process. Hence, even with a selective behavior, wherein a malicious vehicle turns down the cooperation for computational intensive services, it is still able to maintain a reasonable level of reputation for itself in an IoV network.
- Bad-mouthing Attack – In the scenario of a bad-mouthing attack, malicious vehicles deliberately furnish a bad reputation to the trustworthy vehicles in an attempt to damage their reputation in an IoV network. This, thus, minimizes the probability of the trustworthy vehicles to acquire their due privileges in an IoV network. Bad-mouthing attacks are generally sophisticated in nature as malicious vehicles intelligent collude with one another with the key intent to target the trustworthy vehicles, thereby eliminating them out of an IoV network over time.
- Ballot Stuffing Attack – In the case of a ballot stuffing attack, the malicious vehicles collude with one another in a bid to enhance the trustworthiness of another malicious vehicle in an IoV network. The risk manifolds if the malicious vehicle, i.e., whose reputation has been augmented, ends up becoming a cluster head in a cluster as this could jeopardize the safety of not only the occupants of vehicles but also the vulnerable pedestrians.

## III. Research Challenges and Future Prospects

Although the notion of trust has been well researched over the past decade, its convergence with the promising paradigm of IoV still remains in its infancy primarily owing to a number of bottlenecks. Accordingly, in this section, we have identified several such bottlenecks together with some probable solutions to expedite the true realization of a trusted IoV network in the context of the futuristic smart cities.

### A. Lifetime of the Trust Score

As discussed earlier, vehicles in an IoV network are required to keep a record of the trust scores of all the other vehicles with which they have interacted during their respective trajectories. Unlike static networks, the IoV networks are highly dynamic in their nature, and consequently, vehicles usually come across hundreds and thousands of other vehicles within their immediate neighborhood once they traverse along the roads. However, vehicles possess limited onboard storage, and keeping in view a number of important operations that simultaneously transpire within the connected and autonomous vehicles with competing storage requirements, it is not only impossible but impractical for any vehicle to store the trust scores of all of its neighboring vehicles for an extended time period. Hence, it is indispensable to decide on the duration for which a vehicle should record the trust score of its neighboring vehicles in a given context since a vehicle may interact with some vehicles frequently over time but may never encounter others again. For instance, vehicles in dense traffic conditions are expected to come across frequently as opposed to those within sparse traffic conditions. Similarly, vehicles travelling to a similar destination or to the destinations which fall along a similar trajectory have a higher probability of coming in contact with one another. Hence, context-aware schemes which are capable of intelligently deciding an optimal duration for which a vehicle should maintain the record of the

trust score of a neighboring vehicle (that it has interacted with) needs to be devised and deployed in a trust-based IoV network.

### B. Decay in the Trust Score

As discussed earlier, the trust score of a vehicle is dependent on the quality of its interactions with the neighboring vehicles in an IoV network. Furthermore, the trust score of a vehicle is frequently updated as long as it remains in an interactive mode, i.e., the trust score gets incremented or decremented primarily depending on its respective interacting behavior. Nevertheless, the trust of a vehicle should also be subject to some form of a decay if it has not come in an interaction with any other vehicle for a certain duration of time. This is of key essence in order to ensure fairness in the trust system since vehicles which violate the intrinsic collaborative behavior of an IoV network (wherein vehicles cooperate in the traffic routing mechanisms or at least have willingness to cooperate in the routing mechanism) needs to be penalized to a certain extent. Therefore, it is imperative to come up with a decay strategy which would allow the network to penalize the trust score of such a vehicle by a certain factor. The literature suggests that similar decaying strategies have been proposed for conventional social IoT networks [10], [31] and the same could be appropriately tweaked for the IoV networks, however, the real challenge lies in deciding the factor by which a trust score has to be decayed. Existing research in the domain of IoV has yet not accounted for the same in its true essence. Hence, appropriate trust management policies need to devised and subsequently implemented in this regard.

### C. Incentivizing Selfish Vehicles

Similar to some humans which are classified as being selfish primarily owing to their ulterior motives, vehicles may possess a selfish behavior too. Selfish vehicles are usually referred to as the ones that opt not to interact with their neighboring vehicles on a continual basis, i.e., they only participate within a network when it best suits their interests, and in that occurrence, might interact actively so as to build a favorable reputation in an IoV network in a bid to attain privileges. Such a selective behavior, in turn, degrades the combined trust evaluation mechanism in an IoV network since the recommendation of the neighboring nodes, i.e., indirect trust, is essential for evaluating a particular node. It is, therefore, indispensable to incentivize such vehicles for stimulating their participation in an IoV network. Although a number of incentivization mechanisms have been envisaged over the years within the research literature, nevertheless, they need to be considerably tweaked for addressing the highly non-deterministic behavior of IoV networks. In fact, a careful study of the selfish behavior in humans would undoubtedly facilitate in devising better incentivization strategies for the trust-based IoV networks too.

### D. Adaptive Trust Thresholds

It is pertinent to highlight here that the existing trust-based IoV mechanisms engage a pre-defined static threshold to determine the trustworthiness of a vehicle in an IoV network, i.e., as either trustworthy or untrustworthy in nature. Nevertheless, the static thresholds deliberated in the existing literature have no underlying rationale with a number of trust-based mechanisms evaluating the trustworthiness against varied thresholds. If the said threshold is set too high, it would result in the elimination of the honest vehicles. On the contrary, if this threshold is set too low, it would facilitate the malicious vehicles to manipulate the IoV network for an extended period of time. Even if a static threshold has been optimally calculated and then subsequently set, the intelligent malicious vehicles could still manipulate it for their malicious gains, i.e., an intelligent malicious vehicle could act malicious for a certain duration of time, and as soon as it realizes that its trust evaluation has started dropping and is near to the static threshold, it could go into disguise by acting honestly, thereby gaining trust in an IoV network. Hence, it is indispensable to devise an adaptive threshold mechanism that is capable of identifying the intelligent malicious vehicles once they are busy pursuing malicious activities in an attacking time window so that they could be eliminated from an IoV network in a timely manner.

However, there are a number of bottlenecks that may impede the realization of such adaptive threshold mechanisms since it is extremely inefficient to continuously monitor and adjust the adaptive threshold of each vehicle within an IoV network, and particularly, in dense scenarios. One possible alternative could be to instigate an adaptive threshold only when the trust score of a particular vehicle falls within an inspection threshold, i.e., an inspection threshold is a threshold in a certain range of the original (base) threshold and plays the role of a trigger.

### E. Trust-based IoV Threat Models

An overarching and a realistic threat model is of the essence in a bid to carefully examine the structural vulnerabilities of an IoV network, attackers' profiles in terms of their complex sets of attributes along with their probable dynamic attack vectors under varying contexts, and the absence of optimal safeguards in an IoV environment that should have been put into place for mitigating the impacts of adversaries. It is extremely pertinent to mention that such threat models are completely non-existent in the domain of IoV and should be devised and subsequently improved over time in view of any emerging threats.

### F. Trust-based IoV Testbed

As-of-date, the existing trust-based IoV solutions employed different simulation tools, including but not limited to, Veins[1], SUMo[2], OMNeT++[3], network simulator 3[4], VanetMobiSim[5], ONE simulator[6], and mobility simulators programmed in Java, MATLAB, and Python, for evaluating the performance of their respective trust models. Whilst a number of these simulations are comprehensive on their own, the simulators employed do

[1]https://veins.car2x.org/
[2]https://www.eclipse.org/sumo/
[3]https://omnetpp.org/
[4]https://www.nsnam.org/
[5]http://vanet.eurecom.fr/
[6]https://akeranen.github.io/the-one/

not capture well the true essence of an IoV environment. Also, the existing trust-based IoV solutions have employed different trust attributes for ascertaining the trust scores of the vehicles and additionally measured their performance against somewhat a varying sets of metrics too. A realistic testbed is, therefore, indispensable for evaluating and comparing these trust models and to subsequently come up with an optimum solution. Also, designing of such testbeds is a complicated task on its own. It is interesting to note that trust testbeds have started appearing within the research literature for the social IoT networks [32], and although they cannot be employed for the IoV networks, they could still serve as a guidance for conceiving testbeds for the highly dynamic IoV environments.

### *G. Digital Twins and Resiliency of Trust-based IoV Networks*

The notion of digital twins has lately emerged as one of the disruptive technologies for addressing a number of challenges of the automotive sector [33], [34]. It is refereed to as a digital representation of any physical entity which has the ability to be continuously updated via a real-time data, and uses simulation, machine learning, and reasoning ability for intelligent decision making purposes. To put simply, it facilitates in simulating the proposed models much ahead of their implementation, thereby unveiling complex problems before they even become a reality. In the case of IoV, digital twins can be employed for simulating the malicious behaviors of an unwarranted intruder in a bid to develop intelligent decision making and appropriate mitigation strategies to detect, and accordingly, respond to such malicious behaviors. This subsequently facilitates the system designers to test diverse sets of simultaneous trust-based attacks along with the attackers' dynamic strategies vis-à-vis diversified contexts. However, for this to transpire well, the digital twins themselves need to be protected first. For instance, digital twin of a smart city traffic management relies on the data streams accumulated from several end points, i.e., IoT sensors, and each of this end point may prove vulnerable to various attacks if not equipped with robust security mechanisms. Hence, it is indispensable to devise and deploy secure digital twins so that they could be of essence in strengthening the resiliency of the trust-based IoV networks.

## IV. Conclusion

A secure and trusted environment is extremely indispensable for the realization of futuristic smart cities, wherein connected and autonomous vehicles are expected to be the primary mode of personal and commercial transportation, and whose success is primarily dependent on factors such as the resiliency of the IoV networks and the dissemination of authentic, accurate, and reliable information within the same. Trust, in this regard, can play its strategic role by strengthening the resiliency of an IoV networks, in particular, against the insider attacks. This paper, thus, delineates on the convergence of trust with the IoV networks primarily in terms of its underlying rationale, highlights the opportunities that transpire as a result of this convergence, and finally, discusses the open research challenges along with some key recommendations.

## Acknowledgment

Adnan Mahmood's research work is supported via the Macquarie University's Postdoctoral Fellowship. Quan Z. Sheng's work has been partially supported by the Australian Research Council (ARC) Discovery Project Grant: DP200102298, ARC LIEF Project Grant: LE180100158, and ARC Future Fellowship Grant: FT140101247.

## References

[1] F. Ahmad, F. Kurugollu, C. Kerrache, S. Sezer, and L. Liu, "NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9244 – 9257, 2021.

[2] A. Mahmood, W. E. Zhang, and Q. Z. Sheng, "Software-defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges," *Future Internet*, vol. 11, no. 3, p. 70, 2019.

[3] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based Trust Model for Vehicle-to-Everything (V2X)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440 – 450, 2020.

[4] C. R. Storck and F. Duarte-Figueiredo, "A 5G V2X Ecosystem Providing Internet of Vehicles," *Sensors*, vol. 19, no. 3, p. 550, 2019.

[5] J. Li, R. Xing, Z. Su, N. Zhang, Y. Hui, T. H. Luan, and H. Shan, "Trust Based Secure Content Delivery in Vehicular Networks: A Bargaining Game Theoretical Approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3267 – 3279, 2020.

[6] S. Abbasi, A. Rahmani, A. Balador, and A. Sahafi, "Internet of Vehicles: Architecture, Services, and Applications," *International Journal of Communication Systems*, vol. 34, no. 10, p. e4793, 2021.

[7] F. Ahmad, V. Franqueira, and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 6, pp. 28 643 – 28 660, 2018.

[8] S. Tangade, S. Manvi, and P. Lorenz, "Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5232 – 5243, 2020.

[9] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, "A Hybrid Trust Management Heuristic for VANETs," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019, pp. 748 – 752.

[10] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things," in *GLOBECOM 2017 – 2017 IEEE Global Communications Conference*, 2017, pp. 1 – 7.

[11] C. A. Kerrache, N. Lagraa, R. Hussain, S. H. Ahmed, A. Benslimane, C. T. Calafate, J.-C. Cano, and A. M. Vegni, "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5870 – 5877, 2019.

[12] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET – A Survey of Current Solutions and Future Research Opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553 – 2571, 2021.

[13] M. T. Abbas, A. Muhammad, and W.-C. Song, "SD-IoV: SDN Enabled Routing for Internet of Vehicles in Road-aware Approach," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1265 – 1280, 2020.

[14] C. Zhang, L. Zhu, C. Xu, K. Sharif, K. Ding, X. Liu, X. Du, and M. Guizani, "TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET," *IEEE Transactions on Services Computing*, 2019.

[15] R. Mühlbauer and J. H. Kleinschmidt, "Bring Your Own Reputation: A Feasible Trust System for Vehicular Ad Hoc Networks," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 37, 2018.

[16] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, vol. 4, pp. 9293 – 9307, 2016.

[17] A. Mahmood, W. E. Zhang, Q. Z. Sheng, S. Siddiqui, and A. Aljubairy, "Trust Management for Software-Defined Heterogeneous Vehicular Ad Hoc Networks," in *Security, Privacy and Trust in the IoT Environment*, Z. Mahmood, Ed. Cham, Switzerland: Springer International Publishing, 2019, pp. 203 – 226.

[18] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," *IEEE Access*, vol. 8, pp. 21 077 – 21 090, 2020.

[19] M. Sohail, R. Ali, M. Kashif, S. Ali, S. Mehta, Y. B. Zikria, and H. Yu, "TrustWalker: An Efficient Trust Assessment in Vehicular Internet of Things (VIoT) with Security Consideration," *Sensors*, vol. 20, no. 14, p. 3945, 2020.

[20] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A Survey of Trust Management in the Internet of Vehicles," *Electronics*, vol. 10, no. 18, p. 2223, 2021.

[21] A. Mahmood, S. A. Siddiqui, W. E. Zhang, and Q. Z. Sheng, "A Hybrid Trust Management Model for Secure and Resource Efficient Vehicular Ad hoc Networks," in *20th International Conference on Parallel and Distributed Computing, Applications, and Technologies (PDCAT)*, 2019, pp. 154 – 159.

[22] S. A. Siddiqui, A. Mahmood, W. E. Zhang, and Q. Z. Sheng, "Machine Learning Based Trust Model for Misbehaviour Detection in Internet-of-Vehicles," in *Neural Information Processing*, T. Gedeon, K. W. Wong, and M. Lee, Eds. Cham: Springer International Publishing, 2019, pp. 512 – 520.

[23] H. Xia, F. Xiao, S.-s. Zhang, C.-q. Hu, and X.-z. Cheng, "Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach," in *IEEE INFOCOM 2019 – IEEE Conference on Computer Communications*, 2019, pp. 838 – 846.

[24] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," *IEEE Access*, vol. 5, pp. 25 408 – 25 420, 2017.

[25] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware Trust Management for Social Internet of Things," *Computer Networks*, vol. 178, p. 107254, 2020.

[26] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1238 – 1246.

[27] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust Management in Social Internet of Vehicles: Factors, Challenges, Blockchain, and Fog Solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2019.

[28] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust Model for Secure Group Leader-based Communications in VANET," *Wireless Networks*, vol. 25, no. 8, pp. 4639 – 4661, 2019.

[29] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39 – 52, 2019.

[30] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310 – 3322, 2020.

[31] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, X. Wang, and B. Zhou, "SC-TRUST: A Dynamic Model for Trustworthy Service Composition in the Internet of Things," *IEEE Internet of Things Journal*, 2021.

[32] S. Sagar, A. Mahmood, Q. Z. Sheng, and S. A. Siddiqui, "SCaRT-SIoT: Towards a Scalable and Robust Trust Platform for the Social Internet of Things: Demo Abstract," in *Proceedings of the 18th International Conference on Embedded Networked Sensor Systems*, ser. SenSys'20. New York, NY, USA: Association for Computing Machinery, 2020, p. 635 – 636.

[33] S. Almeaibed, S. Al-Rubaye, A. Tsourdos, and N. P. Avdelidis, "Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 40 – 46, 2021.

[34] T. Zhang, X. Liu, Z. Luo, F. Dong, and Y. Jiang, "Time Series Behavior Modeling with Digital Twin for Internet of Vehicles," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 271, 2019.