data

Data Descriptor

TM–IoV: A First-of-Its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles

Yingxun Wang [1,2,*], Adnan Mahmood [3], Mohamad Faizrizwan Mohd Sabri [1] and Hushairi Zen [4]

[1] Faculty of Engineering, Universiti Malaysia Sarawak, Kota Samarahan 94300, Sarawak, Malaysia; msmfaizrizwan@unimas.my
[2] Faculty of Computer and Information Engineering, Qilu Institute of Technology, Jinan 250200, China
[3] School of Computing, Macquarie University, Sydney, NSW 2109, Australia; adnan.mahmood@mq.edu.au
[4] Faculty of Engineering and Technology, i-CATS University College, Kuching 93350, Sarawak, Malaysia; zhushair@feng.unimas.my
* Correspondence: 21010376@siswa.unimas.my or wyx8586@qlit.edu.cn

Abstract: The emerging and promising paradigm of the Internet of Vehicles (IoV) employ vehicle-to-everything communication for facilitating vehicles to not only communicate with one another but also with the supporting roadside infrastructure, vulnerable pedestrians, and the backbone network in a bid to primarily address a number of safety-critical vehicular applications. Nevertheless, owing to the inherent characteristics of IoV networks, in particular, of being (a) highly dynamic in nature and which results in a continual change in the network topology and (b) non-deterministic owing to the intricate nature of its entities and their interrelationships, they are susceptible to a number of malicious attacks. Such kinds of attacks, if and when materialized, jeopardizes the entire IoV network, thereby putting human lives at risk. Whilst the cryptographic-based mechanisms are capable of mitigating the external attacks, the internal attacks are extremely hard to tackle. Trust, therefore, is an indispensable tool since it facilitates in the timely identification and eradication of malicious entities responsible for launching internal attacks in an IoV network. To date, there is no dataset pertinent to trust management in the context of IoV networks and the same has proven to be a bottleneck for conducting an in-depth research in this domain. The manuscript-at-hand, accordingly, presents a first of its kind trust-based IoV dataset encompassing 96,707 interactions amongst 79 vehicles at different time instances. The dataset involves nine salient trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward/punishment, and context, which play a considerable role in ascertaining the trust of a vehicle within an IoV network.

Dataset: https://github.com/wangyingxun/IoV.

Dataset License: Creative Commons Attribution 4.0 International.

Keywords: internet of vehicles; malicious behavior; trust management; trust-based IoV simulator; trust parameters

check for updates

Citation: Wang, Y.; Mahmood, A.; Sabri, M.F.M.; Zen, H. TM–IoV: A First-of-Its-Kind Multilabeled Trust Parameter Dataset for Evaluating Trust in the Internet of Vehicles. *Data* **2024**, *9*, 103. https://doi.org/10.3390/data9090103

Academic Editor: Keke Chen

Received: 7 July 2024
Revised: 22 August 2024
Accepted: 30 August 2024
Published: 31 August 2024

1. Introduction and Background

Over the past decade or so, the rapid evolution and advancements in a number of cutting-edge technologies, including but not limited to, the Internet of Things (IoT), artificial intelligence, and fifth-generation communication, has led to the transformation of the conventional intelligent transportation systems into Internet of Vehicles (IoV) networks [1,2]. The IoV networks facilitate seamless connectivity for a real-time exchange of safety-critical and non-safety information amongst vehicles, and between vehicles and vulnerable pedestrians, supporting roadside infrastructure, and the backbone network via vehicle-to-everything communication [3,4]. Despite the low latency advantages associated with the IoV networks, they are prone to a number of malicious attacks that are not only capable of jeopardizing the entire network but also poses a considerable risk to human lives. Hence, it is of paramount importance to ensure the resilience of IoV networks [5,6]. Figure 1 portrays an IoV landscape.

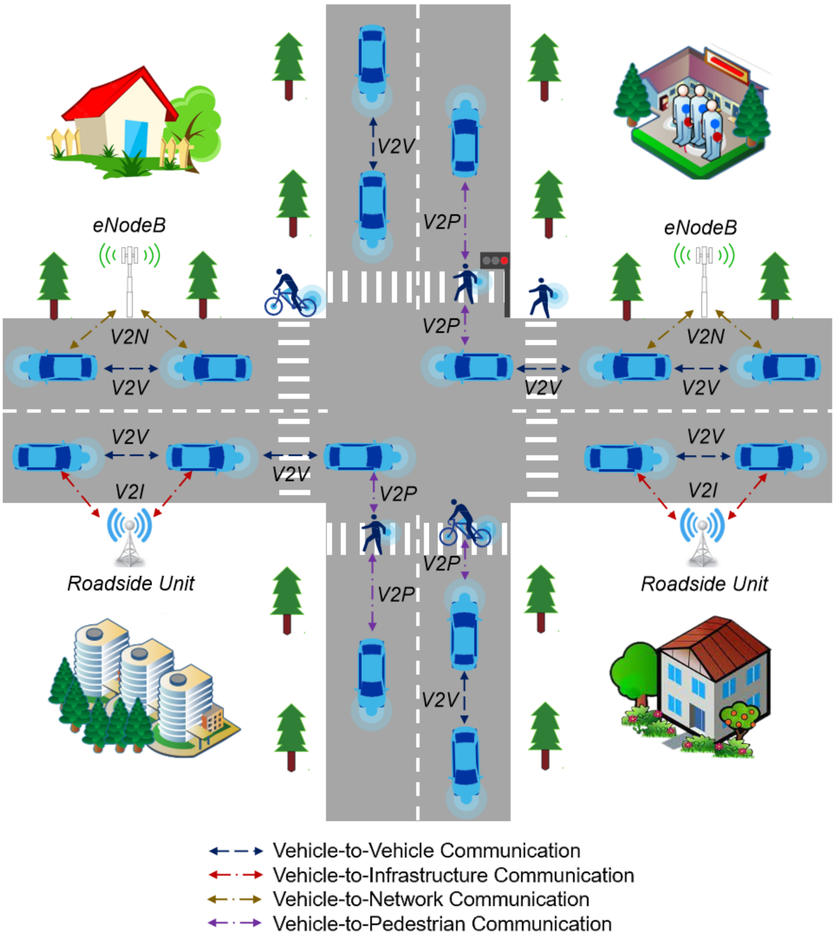
V2V
V2P
eNodeB
eNodeB
V2N
V2V
V2P
V2V
V2N
V2V
V2V
V2V
V2V
V2V
V2I
V2P
V2I
V2P
V2P
Roadside Unit
Roadside Unit
V2V
Vehicle-to-Vehicle Communication
Vehicle-to-Infrastructure Communication
Vehicle-to-Network Communication
Vehicle-to-Pedestrian Communication

Figure 1. An IoV landscape.

A brief glimpse of the state-of-the-art reveals that a number of mechanisms have been proposed over the years in order to strengthen the security of an IoV network. Such mechanisms can be broadly classified into two categories, i.e., cryptography-based approaches and trust-based approaches [7,8]. Whilst the cryptography-based approaches safeguard IoV networks against a number of malicious attacks, including but not limited to data tampering, identity theft, and eavesdropping, they are prone to a number of internal attacks [9,10]. Trust-based approaches, on the contrary, can intelligently address the challenges pertinent to internal attacks [11] since they leverage the reputation of entities within an IoV network in order to guarantee secure communication amongst them, thereby facilitating intelligent traffic flows [12,13].

In the context of an IoV network, vehicles are classified as either trusted or untrusted [14,15]. Trusted vehicles exhibit legitimate behavior by primarily disseminating accurate information in an IoV network, whereas untrusted vehicles engage in malicious activities by intentionally transmitting and facilitating the relay of incorrect information and recommendations in an IoV network in an intelligent manner, thereby posing a grave threat to vehicular passengers and vulnerable pedestrians [16,17]. Hence, an accurate and real-time identification of malicious vehicles in such a highly dynamic network is highly indispensable [18]. The state-of-the-art methodologies employed for the identification of such vehicles in an IoV network typically involve threshold-based and decision boundary-based mechanisms [19,20]. In the case of threshold-based mechanisms, a vehicle's trust value is compared with a predetermined trust threshold, i.e., if the trust value of a vehicle exceeds the predetermined trust threshold, it is regarded as a trusted vehicle, or else, it is classified as a malicious vehicle. On the contrary, in case of decision boundary-based mechanisms, the trust values derived from vehicular interactions are clustered and classified via learning algorithms, and an optimal decision boundary is subsequently employed to segregate the trusted vehicles from the malicious ones [21,22]. However, regardless of the methodology employed for the identification of the malicious vehicles in an IoV network, vehicles should have an associated precise trust value. Therefore, trust-related data hold considerable significance for securing highly dynamic IoV networks.

Trust, in essence, implies a degree of belief or disbelief that a trustor has on a trustee in carrying out a particular task or a set of tasks in an anticipated manner [23]. It mandates quantification, and to realize the same, it relies on several trust-based parameters which are not only context-dependent but are also highly dynamic in nature since they transpire as a result of the frequent interactions amongst the vehicles in an IoV network [24–26]. Whilst a number of IoV-based trust parameters have already been delineated in the research literature, as of date, there is no dedicated publicly available trust-based IoV dataset that researchers from both academia and industry can predominantly employ in order to carry out an in-depth research and subsequently expand upon within this particular domain. In order to address this particular challenge, the manuscript-at-hand presents a pioneering trust-based IoV dataset, which is discussed in detail in Section 2 (Data Description) and Section 3 (Methods).

2. Data Description

The manuscript-at-hand introduces a trust-based IoV dataset, which has been made available for the readers at https://github.com/wangyingxun/IoV, accessed on 1 August 2024. This particular dataset has been employed for not only ascertaining the trust values of vehicles in an IoV network but also for segregating the trustworthy vehicles from the untrustworthy ones by means of an optimal decision boundary. Accordingly, a detailed description of the key features of this particular dataset is indispensable so as to enable researchers in both academia and the industry to employ and extend the same in a bid to investigate open research directions of this emerging and promising domain.

It is pertinent to mention here that, to date, there is no public dataset pertinent to trust management in IoV networks. Therefore, the dataset proposed in the manuscript-at-hand represents a pioneering contribution within this particular domain. In order to realize the same, Java has been employed for designing an IoV-based simulator, whereas Python was employed for analyzing the simulation results. Figure 2 herein depicts a realistic urban mobility scenario for Jinan, i.e., a city in the Shandong province of the People’s Republic of China. The IoV simulator, accordingly, takes into account the said urban mobility scenario since it encompasses several interconnected road segments with vehicles traversing on the same along diverse paths at random speeds in disparate directions. Moreover, the speed of a vehicle remains constant throughout its travelling trajectory along a single path and only changes once the respective vehicle opts for a new path. Vehicles, therefore, interact with one another, i.e., the time of interaction amongst them depends on their respective speeds, and frequently exchange indispensable information to realize a number of both safety-critical and non-safety applications. Moreover, the proposed IoV-based simulator incorporates not only honest vehicles but also intelligent malicious ones that dynamically alternate between honest and dishonest behaviors in a bid to execute malicious acts so as to evade detection by the IoV-based trust models [27,28].

For the readers’ reference, the trust-based IoV dataset proposed in the manuscript-at-hand encompasses 79 vehicles, i.e., trustors and trustees, that engage in a total of 96,707 interactions over different time instances. In total, we ascertained nine key trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward/punishment, and context. A trust authority [29] here plays an indispensable role as it facilitates in ascertaining the trust parameters, which (a) cannot transpire as a result of the interactions between a trustor and a trustee or (b) requires the opinion of a global entity with an overarching view of the entire IoV network in a bid to determine the credibility of the information exchanged between a trustor and a trustee and their respective recommendations. These parameters thus not only depict the dynamic interactions amongst the trustors and trustees in an IoV network but further offer valuable insights pertinent to the behavior of the same.

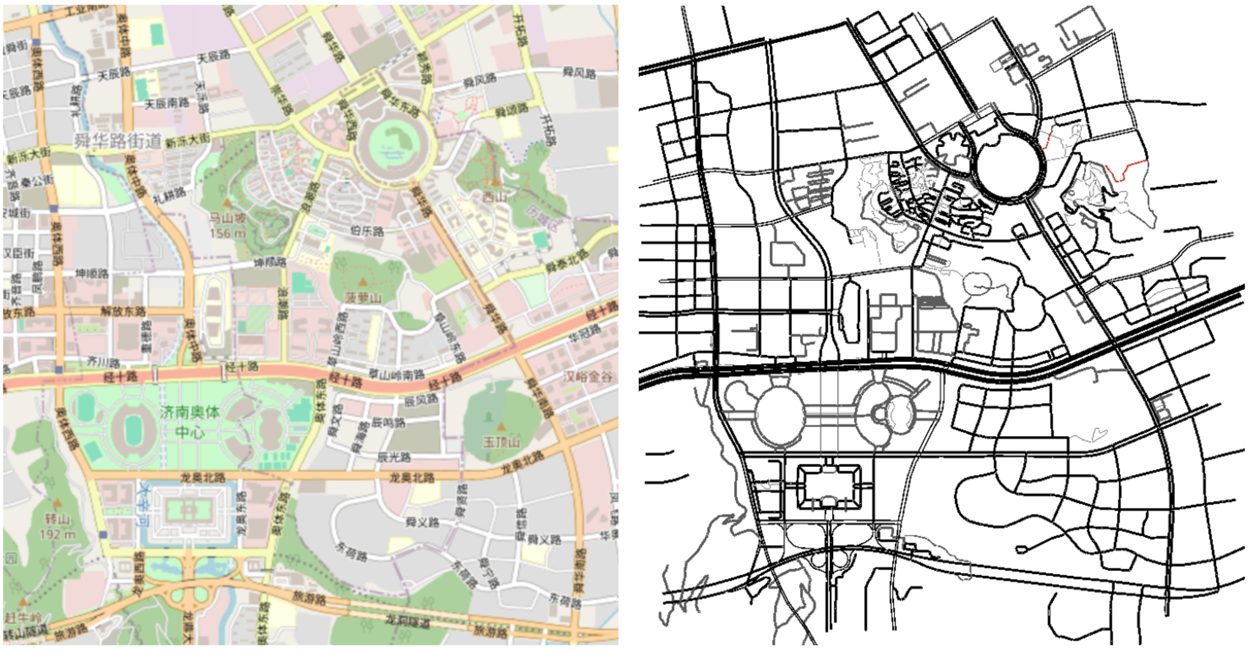

Figure 2. Depicting a realistic urban mobility scenario for Jinan (a city in the Shandong province of the People's Republic of China).

3. Methods

As discussed above, the trust-based IoV dataset proposed in this particular manuscript encompasses trustors, trustees, and 9 salient trust parameters. The same are delineated as follows:

3.1. Trustor

Trust in an IoV network involves multiple attributes (parameters), which can be quantified by considering it as a relational construct involving two entities, i.e., a trustor i and a trustee j. The trustor i assumes the role of an evaluator within an IoV network to assess and ascertain the trustworthiness of a trustee j. In our proposed dataset, there are 79 trustors listed in column 1 of the dataset.

3.2. Trustee

The trustee, also referred to as a target node, is an entity that is evaluated by a trustor as either trustworthy or untrustworthy. In our proposed dataset, there are 79 trustees (listed in column 2 of the dataset) that have encountered 96,707 interactions with the trustors.

3.3. Packet Delivery Ratio (PDR)

The packet delivery ratio ($0 \leq PDR \leq 1$) measures the degree of interaction between a trustor i and a trustee j at a time instance t within an IoV network, thereby providing a key understanding of their relationship. In order to ascertain PDR, we collect the total number of messages sent by a trustor i and successfully received by a trustee j at a time instance t in an IoV network. The PDR is, therefore, determined by taking into account the ratio between the aforementioned sent and successfully received messages between a trustor i and a trustee j. The same is listed in column 3 of the dataset, wherein 0 implies an unsuccessful interaction, whereas 1 suggests a successful interaction.

3.4. Similarity (Sim)

The similarity ($0 \leq Sim \leq 1$) between a trustor i and a trustee j at a time instance t encompasses both external similarity (ES) and internal similarity (IS), and is a weighted amalgamation of the two. The same is listed in column 4 of the dataset.

3.4.1. External Similarity (ES)

The external similarity ($0 \leq ES \leq 1$) suggests the extent to which a trustor i and a trustee j access similar content at a time instance t, and is listed in column 5 of the dataset. ES is deemed to be 1 if the trustor i and a trustee j access similar content. Otherwise, it is regarded as 0.

3.4.2. Internal Similarity (IS)

The internal similarity ($0 \leq IS \leq 1$) manifests the degree of similarity in the positions (geographical locations), directions (travelling trajectories), speeds, and accelerations of a trustor i and trustee j. The same is depicted in column 6 of the dataset.

3.5. Familiarity (Fam)

The familiarity ($0 \leq Fam \leq 1$) between a trustor i and a trustee j at a time instance t is also segregated into external familiarity (EF) and internal familiarity (IF). The same is delineated in column 7 of the dataset.

3.5.1. External Familiarity (EF)

The external familiarity ($0 \leq EF \leq 1$) quantifies the level of the familiarity a trustor possesses towards a trustee, and is listed in column 8 of the dataset. The value of EF is obtained by calculating the ratio between the number of common vehicles that interact with both a trustor i and a trustee j, and the total number of vehicles that interact with a trustor over a given timestamp in an IoV network [30]. In other words, a higher number of shared interacting vehicles (i.e., $EF = 1$) indicates a stronger level of familiarity between a trustor and a trustee.

3.5.2. Internal Familiarity (IF)

The internal familiarity ($0 \leq IF \leq 1$) manifests the extent of interaction frequency between a trustor i and a trustee j, and is recorded in column 9 of the dataset. The value of IF is determined by quantifying the frequency of interactions between a trustor and a trustee over a given timestamp in an IoV network. In other words, a higher interaction frequency (i.e., $IF = 1$) indicates a stronger familiarity between the two parties (trustor and trustee).

3.6. Reward/Punishment (RP)

The reward/punishment ($0 \leq RP \leq 1$) is employed in order to ascertain the degree of a reward or a penalty allocated to a trustee j based on its conduct in an IoV network. Specifically, a trustee j is rewarded by a trustor i for exhibiting cooperation, honesty, and reporting critical events, whereas it is penalized for any sort of a misconduct [31]. The RP is determined by taking into consideration the PDR, and a metric that accounts for both positive and negative interactions between a trustor and a trustee. It is thus represented in column 10 of the dataset.

3.7. Context

Context plays an indispensable role for ascertaining the trust of a trustee in an IoV network since most of the other trust parameters are directly impacted owing to the same [32]. It provides specific information regarding the settings, wherein interactions take place between a trustor *i* and a trustee *j* in an IoV network, i.e., network stability, and temporal and spatial aspects. In the context of this particular dataset, the context ($0 \leq Context \leq 1$) implies the network communication quality segregated into four classes implying poor, medium, good, and excellent. The corresponding values pertinent to these four classes are depicted in column 11 of the dataset.

Figures 3–7 depict the packet delivery ratio, similarity, familiarity, reward/punishment, and context-related scores of each of the 79 vehicles in an IoV network at their most recent respective time instance. Additionally, Table 1 delineates the values of all of the 9 trust parameters introduced in this particular dataset so as to enable the readers to have a comprehensive understanding of the same.

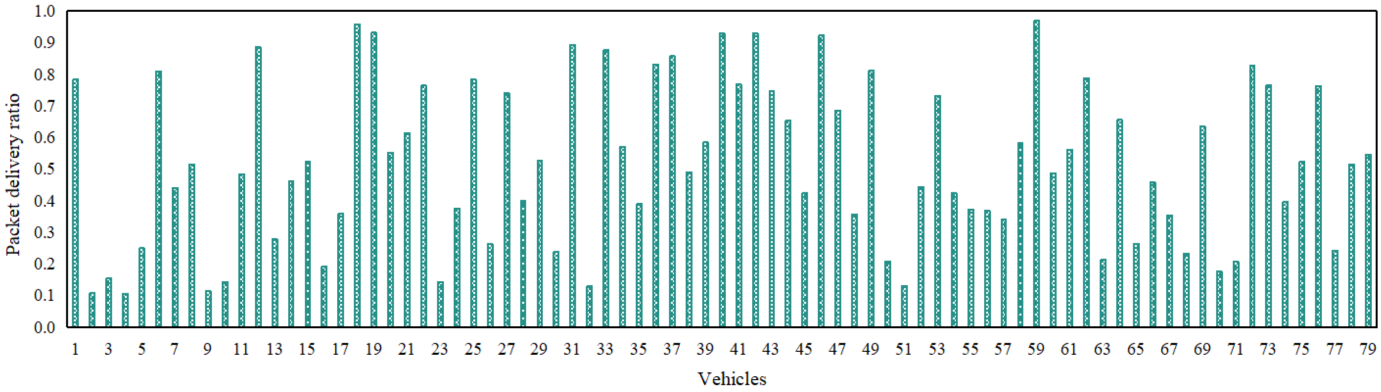

Figure 3. Packet delivery ratios of 79 vehicles in an IoV network.

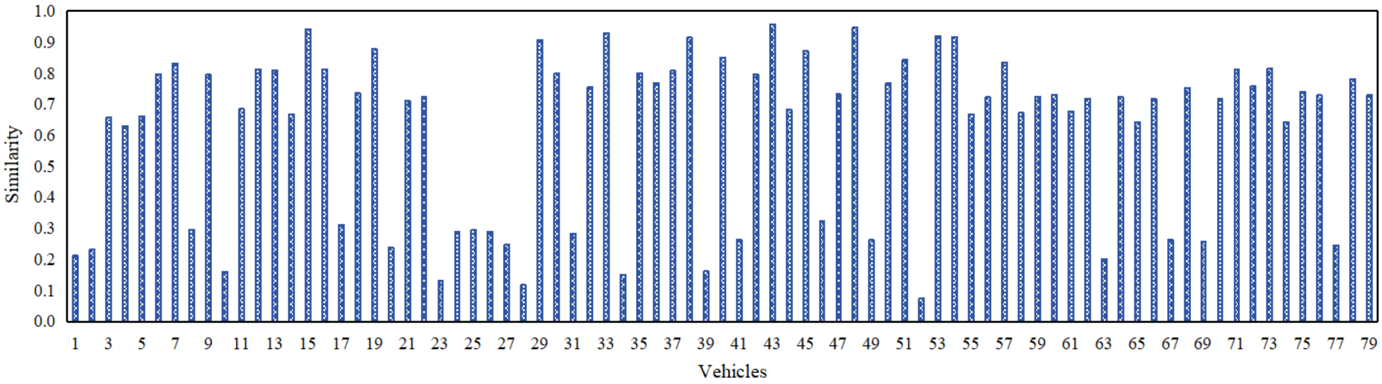

Figure 4. Similarity-related values of 79 vehicles in an IoV network.

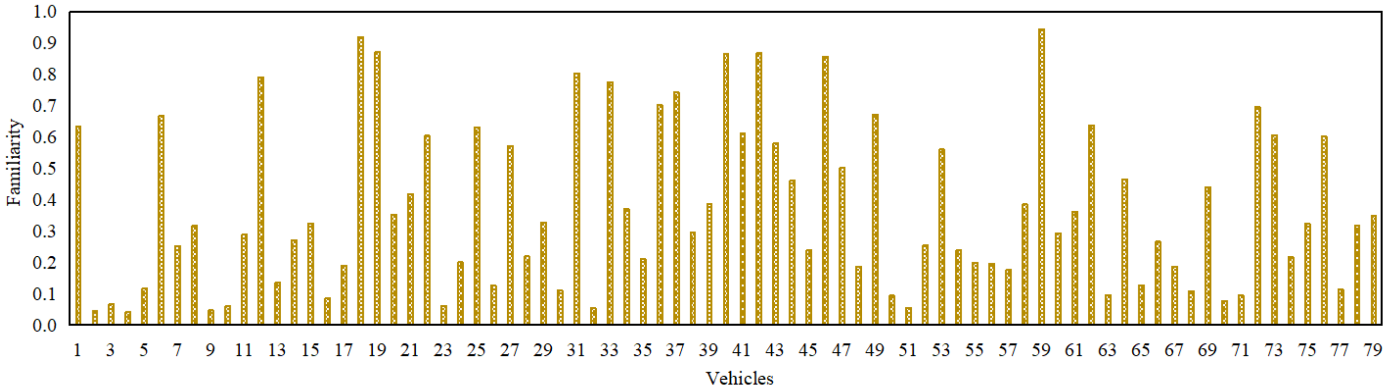

Figure 5. Familiarity-related values of 79 vehicles in an IoV network.

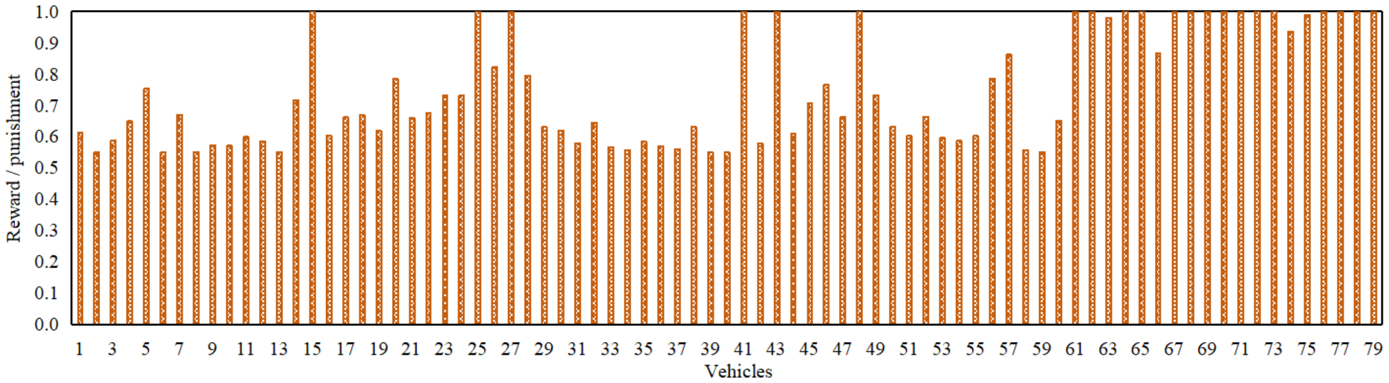

Figure 6. Reward/punishment-related values of 79 vehicles in an IoV network.

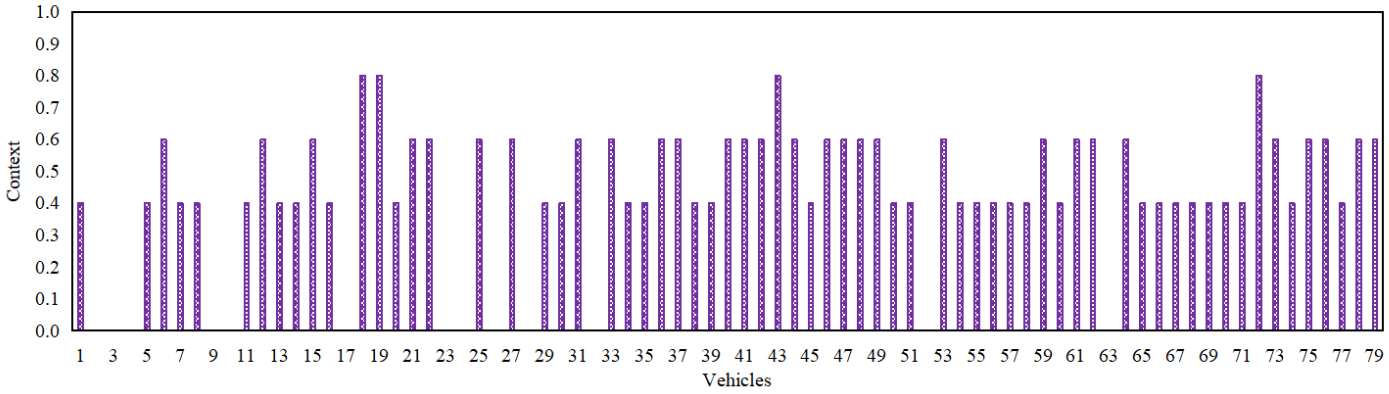

Figure 7. Context-related values of 79 vehicles in an IoV network.

Table 1. A snapshot of values pertinent to the trust parameters, i.e., packet delivery ratio (PDR), similarity (Sim), external similarity (ES), internal similarity (IS), familiarity (Fam), external familiarity (EF), nternal familiarity (IF), reward/punishment (RP), and context, in the trust-based IoV dataset.

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
0	1	0.7113	0.6833	1	0.3666	0.6801	1.0000	0.3602	0.5329	0.6
0	10	0.9625	0.9047	1	0.8094	0.6083	1.0000	0.2166	0.9271	0.8
0	78	0.7849	0.2117	0	0.4235	0.6138	1.0000	0.2276	0.6330	0.4
.	.	.	.	.	.	.	.	.	.	.
5	9	0.7617	0.7646	1	0.5292	0.7765	1.0000	0.5529	0.6002	0.6
5	25	0.1275	0.7946	1	0.5892	0.6257	1.0000	0.2513	0.0533	0.4
5	65	0.9199	0.7658	1	0.5315	0.5569	1.0000	0.1138	0.8491	0.6
.	.	.	.	.	.	.	.	.	.	.
9	10	0.7832	0.4056	0	0.8112	1.0000	1.0000	1.0000	0.6305	0.6
9	37	0.1610	0.9599	1	0.9199	0.5500	1.0000	0.1000	0.0696	0.4
9	70	0.4428	0.8090	1	0.6581	0.6116	1.0000	0.2232	0.2536	0.4
.	.	.	.	.	.	.	.	.	.	.
17	21	0.2089	0.4289	0	0.8578	0.9807	1.0000	0.9614	0.0947	0.4
17	53	0.8233	0.7468	1	0.4935	0.6421	1.0000	0.2841	0.6900	0.6
17	59	0.6767	0.6915	1	0.3830	0.6421	1.0000	0.2841	0.4898	0.6
.	.	.	.	.	.	.	.	.	.	.
23	24	0.9312	0.8760	1	0.7519	1.0000	1.0000	1.0000	0.8693	0.8
23	67	0.3746	0.2880	0	0.5760	0.7328	1.0000	0.4656	0.2004	0.0
23	70	0.8733	0.7228	1	0.4456	0.6758	1.0000	0.3516	0.7694	0.6
.	.	.	.	.	.	.	.	.	.	.
27	40	0.9835	0.8466	1	0.6933	0.8098	1.0000	0.6196	0.9674	0.8

Table 1. *Cont.*

Trustor	Trustee	PDR	Sim	ES	IS	Fam	EF	IF	RP	Context
27	53	0.3995	0.1174	0	0.2348	0.7963	1.0000	0.5926	0.2191	0.0
27	74	0.7684	0.7259	1	0.4519	0.7694	1.0000	0.5388	0.6095	0.6
.	.	.	.	.	.	.	.	.	.	.
35	36	0.7692	0.1149	0	0.2298	0.6487	1.0000	0.2973	0.6107	0.4
35	37	0.5302	0.8996	1	0.7993	0.8904	1.0000	0.7807	0.3314	0.6
35	54	0.1979	0.7465	1	0.4929	0.6607	1.0000	0.3213	0.0887	0.4
.	.	.	.	.	.	.	.	.	.	.
40	41	0.5738	0.7033	1	0.4067	0.5661	1.0000	0.1321	0.3747	0.6
40	45	0.3765	0.6316	1	0.2632	0.6867	1.0000	0.3733	0.2018	0.4
40	59	0.7693	0.2638	0	0.5276	1.0000	1.0000	1.0000	0.6108	0.6
.	.	.	.	.	.	.	.	.	.	.
43	45	0.4167	0.8005	1	0.6009	0.5899	1.0000	0.1797	0.2325	0.4
43	52	0.2337	0.7170	1	0.4339	0.6113	1.0000	0.2225	0.1086	0.4
43	58	0.9459	0.6806	1	0.3611	0.8295	1.0000	0.6590	0.8961	0.8
.	.	.	.	.	.	.	.	.	.	.
50	52	0.4822	0.7346	1	0.4692	1.0000	1.0000	1.0000	0.2873	0.6
50	55	0.5339	0.8764	1	0.7527	1.0000	1.0000	1.0000	0.3350	0.6
50	62	0.7857	0.8393	1	0.6785	0.6659	1.0000	0.3317	0.6341	0.6
.	.	.	.	.	.	.	.	.	.	.
54	57	0.6790	0.8617	1	0.7234	1.0000	1.0000	1.0000	0.4926	0.6
54	61	0.5491	0.8709	1	0.7417	0.7000	1.0000	0.4000	0.3498	0.6
54	75	0.3732	0.6680	1	0.3360	0.6025	1.0000	0.2049	0.1944	0.4
.	.	.	.	.	.	.	.	.	.	.
60	61	0.6867	0.9094	1	0.8187	1.0000	1.0000	1.0000	0.5020	0.6
60	63	0.4465	0.8510	1	0.7020	0.6292	1.0000	0.2583	0.2567	0.4
60	75	0.3603	0.9066	1	0.8131	0.6722	1.0000	0.3444	0.1900	0.4
.	.	.	.	.	.	.	.	.	.	.
63	65	0.8792	0.7572	1	0.5145	1.0000	1.0000	1.0000	0.7792	0.8
63	67	0.6562	0.7231	1	0.4462	1.0000	1.0000	1.0000	0.4653	0.6
63	74	0.4972	0.9154	1	0.8307	0.6249	1.0000	0.2497	0.3007	0.4
.	.	.	.	.	.	.	.	.	.	.
70	71	0.5665	0.7666	1	0.5332	0.5753	1.0000	0.1505	0.3672	0.4
70	73	0.5879	0.7530	1	0.5059	0.6969	1.0000	0.3937	0.3893	0.6
70	76	0.9644	0.1530	0	0.3060	0.9343	1.0000	0.8685	0.9307	0.6
.	.	.	.	.	.	.	.	.	.	.
74	75	0.1220	0.7480	1	0.4960	0.5500	1.0000	0.1000	0.0507	0.0
74	77	0.5229	0.7413	1	0.4826	0.9888	1.0000	0.9775	0.3245	0.6
74	78	0.2091	0.7263	1	0.4526	1.0000	1.0000	1.0000	0.0948	0.4

4. Conclusions and Future Directions

The manuscript-at-hand employs Java to design a trust-based IoV simulator which ascertains the trust values of vehicles in an IoV network and further facilitates in segregating the trustworthy vehicles from the untrustworthy ones via an optimal decision boundary. The trust-based IoV dataset obtained via this simulator is the first of its kind and encompasses nine salient trust parameters, i.e., packet delivery ratio, similarity, external similarity, internal similarity, familiarity, external familiarity, internal familiarity, reward/punishment, and context. The underlying rationale of the said trust parameters lies in their effectiveness to investigate dynamic interactions between trustors and trustees in an IoV network, thereby offering valuable insights into the behavior of the same and a foundation for researchers from both academia and industry to utilize and expand upon. In the near future, the authors intend to employ a trust-based IoV testbed to (a) ascertain the parameters introduced in this dataset via realistic interactions and (b) simulate various intricate IoV-based trust attacks, i.e., self-promoting attacks, on–off attacks, opportunistic service attacks, selective behavior attacks, bad mouthing attacks, and good mouthing attacks.

Author Contributions: The following are the contributions made by the authors: conceptualization, Y.W. and A.M.; methodology, Y.W. and A.M.; software, Y.W.; validation, Y.W. and A.M.; formal analysis, Y.W. and A.M.; investigation, Y.W. and A.M.; resources, Y.W.; data curation, Y.W. and A.M.; writing—original draft preparation, Y.W. and A.M.; writing—review and editing, A.M.; visualization, Y.W. and A.M.; supervision, A.M., M.F.M.S., and H.Z.; funding acquisition, Y.W. All authors have read and agreed to the published version of the manuscript.

Funding: The corresponding author's PhD research at Universiti Malaysia Sarawak, Malaysia, has been funded by the Qilu Institute of Technology, Jinan, Shandong, China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented within this manuscript-at-hand are available at https://github.com/wangyingxun/IoV, accessed on 1 August 2024. A comprehensive dataset is also available to the readers on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cao, T.; Yi, J.; Wang, X.; Xiao, H.; Xu, C. Interaction Trust-Driven Data Distribution for Vehicle Social Networks: A Matching Theory Approach. *IEEE Trans. Comput. Soc. Syst.* **2024**, *11*, 4071–4086. [CrossRef]
2. Yang, Z.; Wang, R.; Wu, D.; Yang, B.; Zhang, P. Blockchain-Enabled Trust Management Model for the Internet of Vehicles. *IEEE Internet Things J.* **2023**, *10*, 12044–12054. [CrossRef]
3. Adhikari, M.; Munusamy, A.; Hazra, A.; Menon, V.G.; Anavangot, V.; Puthal, D. Security in Edge-Centric Intelligent Internet of Vehicles: Issues and Remedies. *IEEE Consum. Electron. Mag.* **2022**, *11*, 24–31. [CrossRef]
4. Yang, X.; Zhu, F.; Yang, X.; Luo, J.; Yi, X.; Ning, J.; Huang, X. Secure Reputation-Based Authentication With Malicious Detection in VANETs. *IEEE Trans. Dependable Secur. Comput.* **2024**, 1–15. [CrossRef]
5. Zhang, Y.; Zhao, Y.; Zhou, Y. User-Centered Cooperative-Communication Strategy for 5G Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 13486–13497. [CrossRef]
6. Shokrollahi, S.; Dehghan, M. TGRV: A Trust-Based Geographic Routing Protocol for VANETs. *Ad Hoc Netw.* **2023**, *140*, 103062. [CrossRef]
7. Rathee, G.; Kumar, A.; Kerrache, C.A.; Calafate, C. A Trust Management Solution for 5G-based Future Generation Internet of Vehicles. *Comput. Netw.* **2024**, *248*, 110501. [CrossRef]
8. Abbas, G.; Ullah, S.; Waqas, M.; Abbas, Z.H.; Bilal, M. A Position-based Reliable Emergency Message Routing Scheme for Road Safety in VANETs. *Comput. Netw.* **2022**, *213*, 109097. [CrossRef]
9. Ullah, S.; Abbas, G.; Waqas, M.; Abbas, Z.H.; Khan, A.U. RSU Assisted Reliable Relay Selection for Emergency Eessage Routing in Intermittently Connected VANETs. *Wirel. Netw.* **2023**, *29*, 1311–1332. [CrossRef]
10. Monfared, S.K.; Shokrollahi, S. DARVAN: A Fully Decentralized Anonymous and Reliable Routing for VANets. *Comput. Netw.* **2023**, *223*, 109561. [CrossRef]
11. Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning. *IEEE Internet Things J.* **2020**, *7*, 6647–6662. [CrossRef]
12. Tripathi, K.N.; Sharma, S.C. A Trust Based Model (TBM) to Detect Rogue Nodes in Vehicular Ad-hoc Networks (VANETS). *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 426–440. [CrossRef]
13. Kuang, Y.; Xu, H.; Jiang, R.; Liu, Z. GTMS: A Gated Linear Unit Based Trust Management System for Internet of Vehicles Using Blockchain Technology. In Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 9–11 December 2022; pp. 28–35.
14. Li, W.; Meng, W.; Kwok, L.F. Surveying Trust-Based Collaborative Intrusion Detection: State-of-the-Art, Challenges and Future Directions. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 280–305. [CrossRef]
15. Kaur, G.; Kakkar, D. Hybrid Optimization Enabled Trust-based Secure Routing with Deep Learning-based Attack Detection in VANET. *Ad Hoc Netw.* **2022**, *136*, 102961. [CrossRef]
16. Li, W.; Meng, W.; Yang, L.T. Enhancing Trust-based Medical Smartphone Networks via Blockchain-based Traffic Sampling. In Proceedings of the IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021; pp. 122–129.
17. Wazid, M.; Das, A.K.; Shetty, S. TACAS-IoT: Trust Aggregation Certificate-Based Authentication Scheme for Edge-Enabled IoT Systems. *IEEE Internet Things J.* **2022**, *9*, 22643–22656. [CrossRef]
18. Fernandes, C.P.; Montez, C.; Adriano, D.D.; Boukerche, A.; Wangham, M.S. A Blockchain-based Reputation System for Trusted VANET Nodes. *Ad Hoc Netw.* **2023**, *140*, 103071. [CrossRef]
19. Aslan, M.; Sen, S. A Dynamic Trust Management Model for Vehicular Ad Hoc Networks. *Veh. Commun.* **2023**, *2*, 11304. [CrossRef]

20. Alalwany, E.; Mahgoub, I. Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. *Sensors* **2024**, *24*, 368. [CrossRef]
21. Zhang, S.; He, R.; Xiao, Y.; Liu, Y. A Three-Factor Based Trust Model for Anonymous Bacon Message in VANETs. *IEEE Trans. Veh. Technol.* **2023**, *72*, 11304–11317. [CrossRef]
22. Nazih, O.; Benamar, N.; Lamaazi, H.; Choaui, H. Towards Secure and Trustworthy Vehicular Fog Computing: A Survey. *IEEE Access* **2024**, *12*, 35154–35171. [CrossRef]
23. Mahmood, A.; Sheng, Q.Z.; Zhang, W.E.; Wang, Y.; Sagar, S. Towards a Distributed Trust Management System for Misbehavior Detection in the Internet of Vehicles. *ACM Trans. Cyber-Phys. Syst.* **2023**, *7*, 1–25. [CrossRef]
24. Sagar, S.; Mahmood, A.; Sheng, Q.Z.; Munazza, Z.; Farhan, S. Can We Quantify Trust? Towards a Trust-based Resilient SIoT Network. *Computing* **2024**, *106*, 557–577. [CrossRef]
25. Zhang, S.; Zhang, D.; Wu, Y.; Zhong, H. Service Recommendation Model Based on Trust and QoS for Social Internet of Things. *IEEE Trans. Serv. Comput.* **2023**, *16*, 3736–3750. [CrossRef]
26. Wang, Y.X.; Mahmood, A.; Sabri, M.F.M.; Zen, H.; Kho, L.C. MESMERIC: Machine Learning-based Trust Management Mechanism for the Internet of Vehicles. *Sensors* **2024**, *24*, 863. [CrossRef]
27. Mahmood, A.; Siddiqui, S.A.; Sheng, Q.Z.; Zhang, W.E.; Suzuki, H.; Ni, W. Trust on Wheels: Towards Secure and Resource Efficient IoV Networks. *Computing* **2022**, *104*, 1337–1358. [CrossRef]
28. Qi, J.X.; Zheng, N.; Xu, M.; Chen, P.; Li, W.Q. A Hybrid-Trust-based Emergency Message Dissemination Model for Vehicular Ad Hoc Networks. *J. Inf. Secur. Appl.* **2024**, *81*, 103699. [CrossRef]
29. Azizi, M.; Shokrollahi, S. RTRV: An RSU-assisted Trust-based Routing Protocol for VANETs. *Ad Hoc Netw.* **2024**, *154*, 103387. [CrossRef]
30. Lam, C.C.; Song, Y.; Cao, Y.; Zhang, Y.; Cai, B.; Ni, Q. Multidimensional Trust Evidence Fusion and Path-Backtracking Mechanism for Trust Management in VANETs. *IEEE Internet Things J.* **2024**, *11*, 18619–18634.
31. Sagar, S.; Mahmood, A.; Sheng, Q.Z.; Zhang, W.E. Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach. In Proceedings of the IEEE International Conference on Communications (ICC), Virtual, 7–11 June 2020; pp. 1–6.
32. Mao, W.; Hu, T.; Zhao, W. Reliable Task Offloading Mechanism based on Trusted Roadside Unit Service for Internet of Vehicles. *Ad Hoc Netw.* **2023**, *139*, 103045. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.