A Hybrid Trust Management Heuristic for VANETs

Adnan Mahmood*[1,2], Bernard Butler[1], Wei Emma Zhang[2], Quan Z. Sheng[2], and Sarah Ali Siddiqui[2]
[1]Telecommunications Software & Systems Group, Waterford Institute of Technology, Ireland
[2]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

***Abstract*—State-of-the-art advances in vehicular communication have fostered the development of *smart mobility platforms*, where moving vehicles exchange safety-critical information with minimal latency, to improve passenger and pedestrian safety. It is, therefore, of paramount importance that the information that is exchanged is not only authentic, but its sender should be *trustworthy*. Consequently, incorrect information needs to be detected as such, and its source needs to be flagged as untrustworthy if it consistently sends incorrect information. In the case of highly dynamic vehicular networks, ignoring trustworthiness poses a serious threat to vehicular communications, especially if there is a chance that the malicious vehicle could be elected as the cluster head of other vehicles within a group. We propose a *hybrid trust management scheme* to identify such malicious vehicles and to inhibit them from being elected as the cluster head. The scheme encompasses a composite metric (i.e., trust values assigned to the vehicles coupled with their resource availability) for cluster head and proxy cluster head selection via intermittent elections. This approach helps to form trustworthy and resource efficient vehicular networks. Simulations of the proposed scheme have been conducted using MATLAB and are also presented in this manuscript.**

***Index Terms*—Vehicular Ad hoc Networks, Trust Management, Network Security, Intelligent Transportation Systems, etc.**

I. Introduction and Preamble

Over recent decades, researchers in both academia and industry have tried to improve the safety of road transportation for passengers and other road users, including pedestrians. Accordingly, the notion of Vehicular Ad hoc Networks (VANETs) has emerged to facilitate communication amongst the vehicles, between the vehicles and the supporting roadside infrastructure or network, and between the vehicles and other road users, especially vulnerable pedestrians. This has led to the emerging and promising paradigm of *Vehicle-to-Everything (V2X)* communication. Such communication is indispensable for both safety-critical and non-safety (e.g., infotainment) vehicular applications and services, and therefore requires both extremely high bandwidth (typically for infotainment purposes) and low-latency (typically for safety purposes) communication in order to ensure better Quality-of-Service and Quality-of-Experience for vehicular users. Furthermore, 5G networks fully support the usage of heterogeneous radio access technology links to guarantee a seamless ubiquitous communication in an *Always Best Connected* paradigm. However, whilst heterogeneity itself brings numerous advantages to the next-generation Intelligent Transportation System (ITS) frameworks, it also makes vehicular networks more vulnerable to a range of security attacks. This is because heterogeneity not only offers multi-path routes for the data transmission, but it also facilitates several devices to be connected simultaneously [1].

VANETs are now expected to play a critical role in smart cities and the Internet-of-Things (IoT) domain more generally. Indeed, it is anticipated that the Internet-of-Vehicles (IoV) will soon become a recognized subset of the IoT [2]. Also, since connected vehicles could disseminate safety-critical information, including (a) blind intersection warnings, (b) emergency vehicle warnings, (c) hazardous location alerts, (d) wrong-way drive warnings, (e) pre-crash safety alerts, etc., it is indispensable to have an extremely secure and trusted network so that such critical data information can be transmitted with high reliability and authenticity. Unlike traditional wired networks, vehicular networks are highly dynamic, distributed, and open to new hosts. They are, therefore, susceptible to numerous attacks, including *replay*, *collusion*, *jamming*, *flooding*, *spoofing*, *rushing*, *eavesdropping*, *man-in-the-middle*, *distributed denial of service*, *black hole*, *sybil*, and *jellyfish* [3].

A brief glimpse at the research literature reveals that a number of mechanisms have already been proposed for safeguarding VANETs against security attacks. These approaches have primarily relied on conventional cryptography-based solutions and have not fully accounted for the dynamic and distributed behavior of vehicular networks. Furthermore, it is worth noting here that reducing network management overhead, preserving privacy, achieving low-latency communication, and intelligent resource management can be extremely challenging within a VANET context. To overcome these challenges, in this paper, each VANET is assumed to support a vehicular cluster [4]. A suitable vehicle is elected as a *cluster head* for its respective cluster. We, therefore, developed a *Hybrid Trust Management Model* based on cluster formation that not only classifies the messages exchanged between the nodes (i.e., vehicles) within a cluster but also identifies and subsequently eradicates multiple malicious nodes from within the cluster in real-time.

The proposed model employs a composite metric for cluster head selection that encompasses both *trust values* and *resource availability*. The cluster head receives all the data requests from other nodes within the cluster, thereby reducing end-to-end latency and increasing resource efficiency. This is because each vehicle does not need to consult the infrastructure and/or network individually for a particular request, and the cluster resources can be allocated intelligently by the cluster head in order of service priority. Furthermore, it preserves privacy as the nodes are incognito to each other, apart from the cluster head. The main contributions of our paper are: (a) selection of

*The corresponding author acknowledges the support of the 'Science Foundation Ireland's Research Centre for Future Networks and Communications (CONNECT)' for the research-at-hand.

978-1-5386-9151-9/19/$31.00 ©2019 IEEE

Table I: Current State-of-the-Art viz. Trust Management in VANETs

No.	Proposed Scheme	Data Trust Model	Node Trust Model	Evaluation	Salient Contribution
[5]	ART: An Attack-resistant Trust Management Scheme for Securing Vehicular Ad hoc Networks	✓	✓	GloMoSim 2.03 Simulation Platform	Data trust evaluation, Node trust evaluation in two dimensions (i.e., functional and recommendation trust)
[6]	Trust Management System for SDN-based VANETs	✓	✓	MATLAB-based MoSim Simulation Tool	Decay method design, Trust factor collection approach design, Optimized Link State Routing (OLSR) and proposed Trust Management System integration
[7]	A Job Market Signaling Scheme for Trust Management	✓	✓	NS2-34, VanetMobisim, SUMO	Markov chain of Distributed Trust Model (DTM^2)
[8]	DREAMS: Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks	✗	✓	Actual Urban Area of San Francisco	Introduction of Vehicular Edge Computing, Improved reputation update, Resource allocation algorithm design
[9]	TEAM: A Trust Evaluation and Management Framework in Context-enabled Vehicular Ad hoc Networks	✓	✓	VEINS Simulation Environment	Trust evaluation framework, Context establishment (4 contexts), Asset-based threat modeling, Realistic evaluation focused on Quality-of-Service
[10]	Blockchain-based Trust Management	✓	✗	MATLAB-based Simulation Environment	Decentralized trust management scheme, Joint Proof-of-Work and Proof-of-Stake consensus mechanism
[11]	Adaptive Trust and Privacy Management Framework	✓	✓	ONE Simulator	Adaptive Linkability and Recognition Scheme (ALRS), and Adaptive Trust Management Scheme (ATMS)
[12]	Clustering Algorithm based on Hybrid Mobility Similarities and Trust Management Scheme	✓	✓	VEINS Simulation Environment	Stable and trustworthy cluster head selection, Event specific trust scheme, Introduction of a timer to reduce the number of exchanged control messages
[13]	Trust Model for Secure Group Leader-based Communications	✓	✓	GrooveNet (v2.0.1)	Designed a group-based Hybrid Trust Model (HTM), Trust value evaluation mechanism, and developed a Misbehavior Detection System (MDS)
[14]	Trust Model for Group Leader Selection in VANET	✓	✗	GrooveNet (v2.0.1)	Self-organization ability evaluation, Node trust evaluation

the cluster head depending on a composite metric that includes both trust values and resource availability, (b) discovery and eradication of malicious nodes within a cluster in real-time, (c) prohibiting the malicious node from becoming the cluster head before it is evicted, and (d) improving resource utilization by random and intermittent elections.

II. An Overview of Existing State-of-the-Art

The dynamic networking topologies, vulnerable communication channels, and limited resources of VANETs have made them more susceptible to various sorts of malicious attacks as compared to traditional fixed networks. Trustworthiness, which could be defined as the confidence of one node in another for a particular action (or set of actions), encompasses both *data trust* and *node trust*, and its assurance is currently one of the biggest challenge encountered by VANETs [5], [6]. Amongst several nodes within a VANET, there could be *malicious nodes* as well as *selfish nodes*. Malicious nodes generally disperse fake and malicious information to other nodes, whereas, selfish nodes look after their own personal interests and collaborate with other nodes only when it serves their benefit [7]. In order to address such problematic nodes, *Trust Model Schemes* are designed to protect the network by identifying and eliminating malicious nodes, as well as by encouraging the selfish nodes to cooperate more with the other nodes [5]–[14]. A comparison of current state-of-the-art viz. trust management in VANETs is presented in Table I.

Over the past few years, schemes have been proposed for ensuring security in VANETs. Most of these schemes utilize traditional cryptography-based approaches, where vehicles use *certificates* and *public key infrastructures* for managing node identities, hence improving the overall security of the network. Unfortunately, such schemes are not effective in the context of vehicular networks because of (a) the dynamic behavior of

vehicles (so identities need to be checked more frequently), (b) the lack of a pervasive and reliable networking infrastructure (so the identity control messages can't be shared reliably), and (c) the greater vulnerability of VANETs to insider threats [9]. It is pertinent to mention that insider attacks are particularly insidious and have the potential to cause catastrophic damage. Thus, in order to overcome these shortcomings, a more general interpretation of *trust* (i.e., one not limited to public key infrastructure) has been recommended for guaranteeing security in VANETs [15].

In *reputation-based trust system*, a credit amount is assigned to each node that is primarily dependent on the node's behavior [6]. Therefore, when choosing between two otherwise equivalent candidate nodes, the node with the higher credit is more likely to be chosen. A node is thus removed from the network (i.e., repudiated) if its credits are depleted. Each node's trust score is assessed on various aspects, including its neighbor's recommendation, its overall reputation in the network, and its previous dealings and interactions with other nodes.

Trust Models also comprise three categories. *Entity-oriented trust models* evict malicious nodes. *Data-oriented trust models* assess both the accuracy and authenticity of the information transmitted by a particular node. *Hybrid trust models* ascertain both the node's trustworthiness and the reliability of the data transmitted by a node. Frameworks, such as *TEAMS* [9], have been proposed to assess trust models depending on both node trust and data trust.

SDN, fog computing, and edge computing are being applied to vehicular networks. In SDN-based VANETs, trust models have been designed to help protect the data plane from diverse sort of malicious attacks. Some trust models use fuzzy logic and graph theory to make decisions regarding the trustworthiness of a node, while others rely on multi-weighted subjective logic, Bayesian interference techniques, or the job marketing signaling model, etc. [6]–[8], [10].

As mentioned earlier, VANETs may operate as vehicular clusters or vehicular clouds [13], [14]. In this context, a cluster head is the vehicle with the highest total trust value among all the vehicles in the cluster. The total trust value encompasses a *direct trust value* which is assigned by a neighboring vehicle depending on its past interactions with the target vehicle, and an *indirect trust value* which is a recommendation by its peers (nearest neighbors) [16].

The trust values assigned by the neighboring vehicles could be computed through various mechanisms. In [17], each vehicle ascertains the trust values for the other vehicles within the cluster by utilizing fuzzy sets and by taking into consideration the recommendations from the neighboring vehicles, the node's previous reputation, and the recommendations from the roadside infrastructure. A message is thus sent by each vehicle to its one-hop neighbors for testing purposes. Subsequently, the neighbor sends the message(s) to the intended destination post-authentication. The neighbor is considered trustworthy if the acknowledgement of the said message is received from the intended recipient node. Otherwise, a trust value equal to '0' is assigned to that neighbor [18]. To derive the trust value of a neighboring vehicle, direct trust scores can be combined with indirect trust scores.

Vehicular behavior analysis helps to guarantee trusted communication between nodes. Of course, such trustworthy message exchange is essential for safety-critical applications and services in VANETs. The key intent is to provide traffic safety with a lowest possible network overhead, end-to-end response time, and resource consumption. Thus, discovery and eviction of malicious or selfish nodes is needed to restrict any forged and obsolete information from being circulated in the network. Effective methods to elect a reliable cluster head and to remove malicious nodes require ongoing research.

III. System Model and Simulation Results

We have developed a vehicular cluster model that comprises both trusted and malicious vehicles (nodes) $V_i, i = 1, \ldots, I$. The hop distance between each of the I nodes is 1. Trust values $T_{i,j,k}, j = 1, \ldots, I-1; j \neq i; k = 1, \ldots, K$ are assigned to each node i by its neighbors j at every time instance indexed by k. The trust values are based on a node's behavior, i.e., if the information shared by a node is legitimate (hence not malicious), it is considered as a trusted node and has a higher trust value. The trust scores vary between 0 and 1, wherein, 0 represents an untrusted node at (any) time instance while 1 signifies the highest level of trust. The trust value assigned to node i by its one-hop neighbors j at time instance k is derived using Equation 1 as follows:

$$T_{i,k} = \frac{\sum_{l=1}^{k-1} w_l T_{i,l} + (\sum_{j=1}^{I-2} T_{i,j,k})/(I-2)}{2} \tag{1}$$

where, weights w_l sum to 1. $A_{i,k} = \sum_{l=1}^{k-1} w_l T_{i,l}$ represents the weighted sum of *past* trust scores for node i and $B_{i,k} = \sum_{j=1}^{I-2} T_{i,j,k}/(I-2)$ represents the average trust score assigned by the remaining $I-2$ nodes, indexed by j, to node i in the current time indexed by k. The updated score $T_{i,k}$ for node i at instant k is just the arithmetic mean of $A_{i,k}$ and $B_{i,k}$.

A threshold value has also been set in order to identify the trusted nodes at every time instance k, i.e., node i having $T_{i,k} \geq T_0$, where T_0 is a threshold, is considered a trusted node at that time instance. Furthermore, the available resources $(R_{i,k}, i = 1, \ldots, I)$ possessed by each node i at instant k is computed using Equation 2 for determining if a particular node has sufficient resources and fulfills the minimal requirements ($R_{i,k} \geq R_0$, where R_0 is the minimum acceptable requirement of composite network resources for node i) to be a candidate cluster head.

$$R_{i,k}^{\mathrm{BW}} = \frac{\min_j(e(i,j,k))}{\sum_j e(i,j,k)}$$

$$R_{i,k}^{\mathrm{Pr}} = \frac{p_{i,k}}{\sum_i p_{i,k}}$$

$$R_{i,k} = w_B R_{i,k}^{\mathrm{BW}} + w_P R_{i,k}^{\mathrm{Pr}}$$

$$w_B + w_P = 1 \tag{2}$$

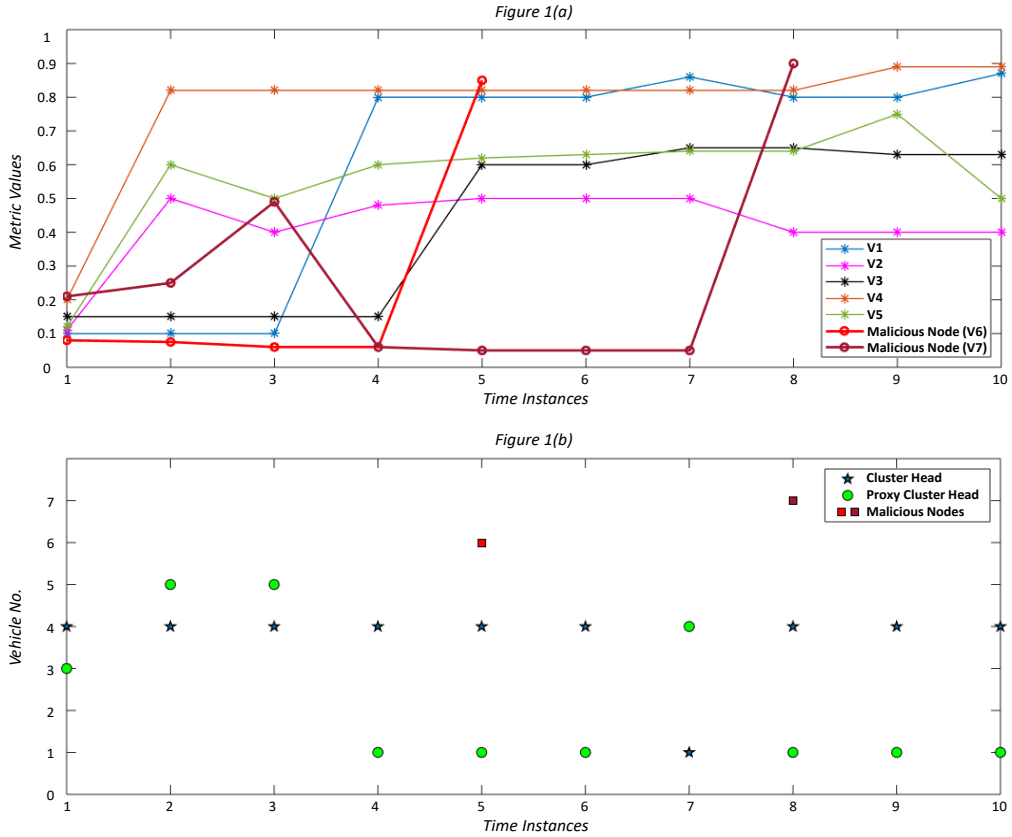

Figure 1: (a) Metric Values at each time instance with Malicious Node Identification and Eviction, and b) Depiction of Cluster Head, Proxy Cluster Head at each time instance and the Malicious Node

where, $e(i,j,k)$ refers to the *link capacity* between nodes i and j at instant k, and $p_{i,k}$ is the *remaining power* (at time k) for node i. The corresponding resource types are normalised as nondimensional ratios $R_{i,k}^{\mathrm{BW}}$ and $R_{i,k}^{\mathrm{Pr}}$ respectively. Note that R^{BW} is based on the capacity of the weakest link, rather than a simple weighted average. The composite resource availability $R_{i,k}$ for node i at instant k is the weighted sum of the two.

The cluster heads are then selected depending on a composite metric $U_{i,k}$ (defined in Equation 3) for node i at instant k, as the weighted sum of (normalised) resource availability $R_{i,k}$ and computed trust score $T_{i,k}$. The node with the highest value of $U_{i,k}$ becomes the cluster head V_k^{CH}, whereas, the node having the second highest metric value becomes the proxy cluster head V_k^{PCH}. Weights for trust and available resources are introduced to incorporate preferences based on application requirements, i.e., applications demanding more security could assign higher weights to the trust values, with more risk that the resulting cluster head may not be able to meet its functional requirements, and vice versa.

$$U_{i,k} = w_R R_{i,k} + w_T T_{i,k}$$
$$w_R + w_T = 1 \tag{3}$$

Algorithm Hybrid Trust Management Scheme

for $k = 1\ to\ K$ **do**
  for $i = 1\ to\ I$ **do**
    $T_i \leftarrow CompTrust$
    $R_i \leftarrow AvailableResources$
    $U_i \leftarrow CompMetric(T_i, R_i, w_T, w_R)$
  end for
  if $U_i < Threshold$ **then**
    $V^{\mathrm{mal}} \leftarrow v_i$
  end if
  for $l = 1\ to\ n$ **do**
    $BestMetric \leftarrow sort(U_i)$
  end for
  $V^{\mathrm{CH}} \leftarrow BestMetric(l)$
  $V^{\mathrm{PCH}} \leftarrow BestMetric(l+1)$
  if $V^{\mathrm{CH}}\ is\ V^{\mathrm{mal}}$ **then**
    $V^{\mathrm{CH}} \leftarrow V^{\mathrm{PCH}}$
    $V^{\mathrm{PCH}} \leftarrow BestMetric(l+2)$
  else
    if $V^{\mathrm{PCH}}\ is\ V^{\mathrm{mal}}$ **then**
      $V^{\mathrm{PCH}} \leftarrow BestMetric(l+2)$
    end if
  end if
  update $V^{\mathrm{CH}}, V^{\mathrm{PCH}}$
end for

Elections for V_k^{CH} are held at random instant k, i.e., when an existing $V_{<k}^{\mathrm{CH}}$ no longer has resources to act as the cluster head at time instant k, or its trust values start to fall, or a new node with better resources and a higher trust value is added to the cluster. Also, if a node suddenly starts getting higher composite metric values assigned to it, then the historic precedence of its metric values is investigated over the past time instances. Therefore, if the preceding metric values are below the minimum acceptable threshold on multiple occasions at the previous time instances, it is considered as a malicious node V^{mal} and is prohibited from becoming a cluster head (V^{CH}) or V^{PCH} at this time instance, and is evicted from the cluster. In cases where the malicious node has the highest composite metric value at a time instance, the node with the second (respectively, third) highest metric value becomes the cluster head V^{CH} (respectively, V^{PCH}).

Simulation results in Figure 1(a) illustrate the metric value of every node for the 10 time instances and identifies the node with a composite metric value below the minimum acceptable threshold (i.e., *malicious node*). For simulation purposes, the minimum acceptable threshold value is set as 0.1. It could be observed that *Vehicle 6* has metric values below 0.1 for the first 4 time instances and its metric value instantaneously peaks at around 0.85 which is the highest metric value amongst all the vehicles at that particular time instance. Also, metric values for *Vehicle 7* decreases below 0.1 at the fourth time instance for three consecutive time instances but then instantly peaks up to 0.9 at the seventh time instance. Our trust management system checks the prior reputation of these nodes and categorizes them as malicious nodes before removing them from the cluster.

Furthermore, Figure 1(b) depicts the cluster heads, proxy cluster heads, and malicious nodes for the 10 time instances. It can be observed that elections for V^{CH} are held at instances $k = 1, 7, 8$, but for V^{PCH}, are held at $k = 1, 2, 4, 7, 8$ owing to either change in the trust values or as a consequence of reduction in available resources of $V_{<k}^{\mathrm{CH}}$ and $V_{<k}^{\mathrm{PCH}}$ respectively. Also, at $k = 5, 8$, *Vehicle 6* and *7* are identified as malicious nodes respectively, and are hence plotted as being malicious. In this case, the node with the second highest metric value, i.e., *Vehicle 4*, and the node with the third highest metric value, i.e., *Vehicle 1*, becomes V^{CH} and V^{PCH} respectively.

IV. Conclusion

In this paper, we have proposed a hybrid trust management scheme for cluster-based VANETs. The scheme elects a cluster head amongst a group of vehicles, i.e., by choosing the node with the maximum composite metric comprising average trust values assigned to the vehicles (i.e., nodes) and their available resources at any particular time instance. It ensures the eviction of multiple malicious nodes in real-time, and further prohibits them from becoming the cluster head. Our proposed scheme also scales considerably well with the cluster size. Simulation results illustrate identification and removal of malicious nodes along with ensuring an optimal cluster head and proxy cluster head at every time instance.

References

[1] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, and M. Qiu, "A Scalable and Quick-Response Software Defined Vehicular Network Assisted by Mobile Edge Computing," in IEEE Communications Magazine, vol. 55, no. 7, pp. 94-100, July 2017. doi: 10.1109/MCOM.2017.1601150

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," in IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3701-3709, April 2017.

[3] A. D. Maio, M. R. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, and T. Engel, "Enabling SDN in VANETs: What is the Impact on Security?," in Sensors, vol. 16, no. 12, pp. 1-24, December 2016. doi: 10.3390/s16122077

[4] L. A. Maglaras, A. H. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, "Social Internet of Vehicles for Smart Cities," in Journal of Sensor and Actuator Networks, vol. 5, no. 3, February 2016. doi:10.3390/jsan5010003

[5] W. Li, and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960-969, April 2016. doi: 10.1109/TITS.2015.2494017

[6] S. Tan, X. Li, and Q. Dong, "A Trust Management System for Securing Data Plane of Ad hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7579-7592, September 2016. doi: 10.1109/TVT.2015.2495325

[7] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3657-3674, August 2015. doi: 10.1109/TVT.2014.2360883

[8] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks," in IEEE Access, vol. 5, pp. 25408-25420, November 2017. doi: 10.1109/ACCESS.2017.2769878

[9] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad hoc Networks," in IEEE Access, vol. 6, pp. 28643-28660, May 2018. doi: 10.1109/ACCESS.2018.2837887

[10] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks," in IEEE Internet of Things Journal, May 2018. doi: 10.1109/JIOT.2018.2836144

[11] T. N. D. Pham, and C. K. Yeo, "Adaptive Trust and Privacy Management Framework for Vehicular Networks", in Vehicular Communications, vol. 13, pp. 1-12, July 2018. doi: 10.1016/j.vehcom.2018.04.006

[12] S. Oubabas, R. Aoudjit, J. J. P. C. Rodrigues, and S. Talbi, "Secure and Stable Vehicular Ad hoc Network Clustering Algorithm based on Hybrid Mobility Similarities and Trust Management Scheme", in Vehicular Communications, vol. 13, pp. 128-138, July 2018. doi: 10.1016/j.vehcom.2018.08.001

[13] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust Model for Secure Group Leader-based Communications in VANET", in Wireless Networks, pp. 1-23, May 2018. doi: 10.1007/s11276-018-1756-6

[14] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust Model for Group Leader Selection in VANET", in International Journal of Digital Information and Wireless Communications, vol. 8, no. 2 pp. 139-143, June 2018. doi: 10.17781/P002421

[15] X. Yao, X. Zhang, H. Ning, and P. Li, "Using Trust Model to Ensure Reliable Data Acquisition in VANETs", in Ad hoc Networks, vol. 55, pp. 107-118, February 2017. doi: 10.1016/j.adhoc.2016.10.011

[16] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based Authentication Technique for Cluster based Vehicular Ad hoc Networks (VANET)", in Wireless Networks, vol. 24, no. 2, pp. 373-382, February 2018. doi: 10.1007/s11276-016-1336-6

[17] F. G. Mármol, and G. Pérez, "TRIP, A Trust & Reputation Infrastructure-based Proposal for Vehicular Ad hoc Networks", in Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941, May 2012. doi: 10.1016/j.jnca.2011.03.028

[18] S. Tangade, and S. S. Manvi, "Trust Management Scheme in VANET: Neighbour Communication based Approach," in International Conference on Smart Technologies for Smart Nation (SmartTechCon), pp. 741-744, May 2017. doi: 10.1109/SmartTechCon.2017.8358469