Social Networking and Big Data Analytics Assisted Reliable Recommendation System Model for Internet of Vehicles

Manish Kumar Pandey(✉) and Karthikeyan Subbiah

Department of Computer Science, Institute of Science,
Banaras Hindu University, Varanasi 221005, India
pandey.manish@live.com

Abstract. The devices are becoming ubiquitous and interconnected due to rapid advancements in computing and communication technology. The Internet of Vehicles (IoV) is one such example which consists of vehicles that converse with each other as well as with the public networks through V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian) and V2I (vehicle-to-infrastructure) communications. The social relationships amongst vehicles create a social network where the participants are intelligent objects rather than the human beings and this leads to emergence of Social Internet of Vehicles (SIoV). The big data generated from these networks of devices are needed to be processed intelligently for making these systems smart. The security and privacy issues such as authentication and recognition attacks, accessibility attacks, privacy attacks, routing attacks, data genuineness attacks etc. are to be addressed to make these cyber physical network systems very reliable. This paper presents a comprehensive survey on SIoV and proposes a novel social recommendation model that could establish links between social networking and SIoV for reliable exchange of information and intelligently analyze the information to draw authentic conclusions for making right assessment. The future Intelligent IoV system which should be capable to learn and explore the cyber physical system could be designed.

Keywords: Big data · IoV · SIoV · Social recommendation system · Cyber physical systems

1 Introduction

Technology has drastically transformed our lives by bringing in huge benefits that reflects the beginning of our associated future, such as vehicles associated with computers, onboard sensors, sensors in wearable devices that notify the movements of objects and its current state of affairs. So, the internet of Vehicles (IoV) is an inevitable juxtaposition of the mobility and the Internet of things, in other words it is the Internet of things in the area of transport. The IoV aims at achieving an integrated smart transport system by improving traffic flow, preventing accidents, ensuring the road safety, and creating a comfortable driving experience. Mobility in transportation systems generates a huge amount of real data and it is a great challenge to deal with this data surge. So a

© Springer International Publishing AG 2016
C.-H. Hsu et al. (Eds.): IOV 2016, LNCS 10036, pp. 149–163, 2016.
DOI: 10.1007/978-3-319-51969-2_13

multi-dimensional approach is required to handle and study the vast amount of generated data in structured as well as unstructured formats both from the independent and connected sensors of the Internet of Vehicle (IoV) to obtain optimal results with safety measures [2]. The big data [1] technology provides a solution to this challenging problem to evolve such intelligent and smart vehicular system.

1.1 The IoV Technology

Hardware Infrastructure: Convergence of technologies in the design of vehicles is quickly making them as key devices in the Internet of Things (IoT) [3–5] with the capabilities to accept data as well as send data to the cloud, to the traffic infrastructure and to other vehicles. As a result, the Internet of Vehicle (IoV) becomes an emerging technology in data communication with definite protocols that facilitates data transfer between cars, roadside equipment, wearable devices and traffic data management centers. So the IoV is the next technological revolution, which integrated with sensor networks, camera [5], mobile communication [7], real-time localization [8], ubiquitous computing and other technologies [9] to realize the essential requirements for Intelligent Transportation Systems (ITS) applications [6].

Processing Needs: Now, it is an era of smart objects with sensor inputs that are able to communicate via the Internet based on the protocols and/or prototype standards of ICT. Therefore, advanced techniques are necessary for effectively handling huge data generated from IoV and to perform efficient online analytical query processing [2]. Thereby, the big data analysis outcomes are pertinent to the transportation benefits in terms of cost efficiency, time utilization in ensuring road safety, for effective traffic management, in automated tolling and providing other ITS services. The following facts supports big data paradigm as a promising technology for intelligent IoV systems: (i) Massive data streams produced by IoV audio, video and sensors must be handled and integrated [10], (ii) Spatial data of IoV objects in the context of the environments is described as location based and in time series and (iii) Integration of federated IoV smart objects' data are tended to have its own implicit semantics that need to be recognized for the inferring justifications.

The scalability and capability of big data analytics and predictions for IoV data management, exploration and exploitations lies in dynamic and scalable technological facts, which includes:

It is vitally significant to identify and address IoV smart objects in order to interact or query with various objects to realize each other's identity and address effectively.
Effective methods of data abstraction and compression should be developed for filtering out the redundant data.
Data indexing, archiving, access control and scalability for IoV data.
Data warehouse and its query language for multi-dimensional analysis, semantic intelligibility and interoperability for diverse data of IoV,
Time-series and event level data aggregation,
It is essential for *privacy and protection of data management of IoV.*

Communication Network's Needs: Wireless networks can be organized into three major categories. An infrastructure wireless network is the first one that mainly relies on a central station that coordinates all communications [11]. Second are ad hoc networks or non-structured networks that give equal roles to all stations in the network [12, 13]. Third, hybrid networks which combines the first two categories [14]. A case of hybrid networks is hybrid vehicular ad hoc networks (hybrid-VANETs) [15], which employ ad hoc networks for communication among vehicles and infrastructure networks, for example cellular systems for communication and wireless local area networks (WLANs) with a core network [16, 17]. Smart vehicles, through their finer communication potentiality, will be capable to work jointly not only with navigation and broadcast satellites, but also through passenger smart vehicles, smart phones and roadside units, making them an important component of IoT and the development of smart cities [18]. VANETs combine these with new applications and procedures to facilitate the intelligent communication among the connection to the Internet and the vehicles. VANETs rely on on-board units (OBU) and roadside units (RSU) and to facilitate the connectivity. The RSUs are communication infrastructure units that are positioned next to roads to communicate with vehicles and to a larger infrastructure or to a core network, depending upon metropolitan traffic topography. The OBU is a network device integrated with different sensors attached in vehicles that supports communication with different wireless networks, for example dedicated short-range communication (DSRC) and WLAN. A VANET has a varied range of applications, from road safety, through traffic management by the detection and avoidance of traffic accidents [19], traffic flow, reduction of traffic congestion [20], and infotainment to provide of driving comfort [21].

SIoV: The Fig. 1 shows different components of SIoV and the communication between them. The Social Internet of Things (SIoT) introduces social relationships between things, creating a social network where the participant entities are not humans, but intelligent things. In such networks, information about the traffic and road conditions is obtained from both humans as well as machines. As humans can be biased or may be forced to propagate false information for personal gains, the network should integrate mechanisms to assert the trust and reputation of the information sources.

The Social Internet of Things (SIoT) [22] is a network of intelligent things that have social interactions. The Social Internet of Vehicles (SIoV) [23, 24] is an example of a SIoT where the things are smart vehicles. Alam et al. [24] designed logical models of the subsystems occupied in the SIoV communication process and propose models that could be useful in order to set up safety, efficiency or comfort applications based Social Internet of Vehicles (SIoV).

Even though the basic rules are the same for both social networks of vehicles and social networks of humans, there are important differences in terms of the active character of the entities, the topology of the network, privacy concerns, their social interactions and security issues that arise.

Social Internet of Vehicles (SIoV) describes both the social interactions among vehicles [25] and among drivers [26]. As described in [26], a vehicular social network is produced when a driver goes to an area where additional public with familiar interests

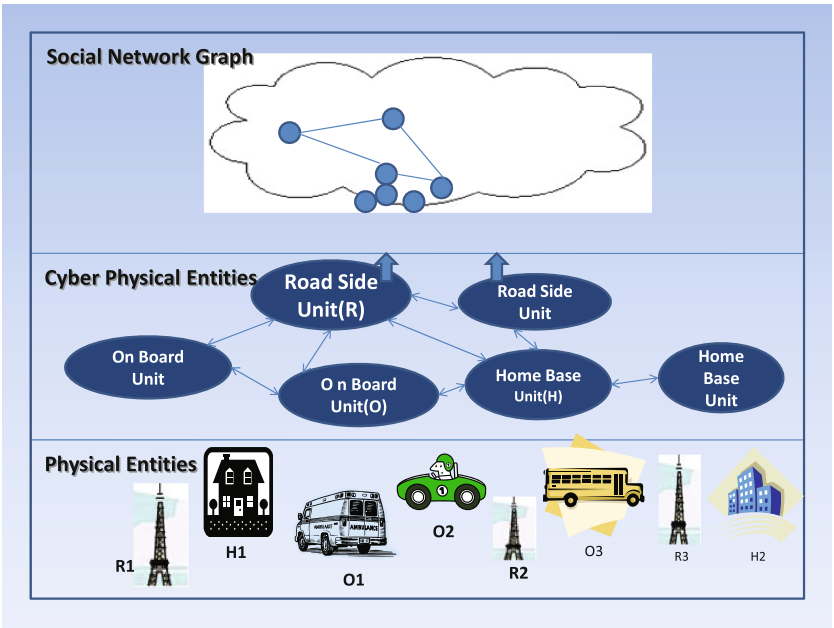

Fig. 1. Social Internet of Vehicles

or related content exist. Contrary to this, Nitti et al. [25] describe a vehicular social network as social interactions among cars, which converse alone to glance for update services and exchange messages relevant to traffic. As vehicles are autonomous and becoming more autonomous [27] and applications are already developed to support social interactions among drivers and passengers [28, 29].

1.2 The Next Generation Vehicles and SIoV

Recent advancements in technology that are context-aware and wireless vehicular communication techniques, such as Long-Term Evolution (LTE), Dedicated Short-Range Communications (DSRC), Worldwide Interoperability for Microwave Access (WiMax) and IEEE 802.11p [30] has boosted the design, development and deployment of vehicular networks. An increasing number of social network applications are being proposed for vehicular networks, which leads to a shift from traditional vehicular networks toward SIoV. The key aspects that enable SIoV in current vehicular networks are briefly discussed as follows.

Similar to [31], we focus on three main components, namely: next-generation vehicles; vehicle context-awareness; and SIoV context-aware applications.

Vehicular ad hoc networks (VANETs) are a class of mobile ad hoc network that has been anticipated to improve traffic protection and applications to provide comfort to drivers. The unique features of VANETs comprise of quick vehicles that follow predestined paths (i.e., roads) and message exchange having different priority levels. For example, messages for traffic safety applications require timely delivery of reliable

message making it of high priority while messages for comfort and infotainment applications have low priority [32]. Vehicles can communicate among themselves (vehicle-to-vehicle, V2V) as well as with roadside units (vehicle-to-infrastructure, V2I) by using the on-board unit. The other forms of communication, such as vehicle-to-cloud broadband (V2B), where the vehicle communicate with a monitoring data centre, vehicle-to-human (V2H) to communicate with susceptible road users, and vehicle-to-sensor (V2S), where the vehicles converse with sensors embedded in the location [32] are enabled.

1.3 Interaction of SIoV with Social Network

Social network analysis (SNA) refers to the use of network theory to analyses social networks to discover important players in a network. Individual actors (either be vehicles or drivers or even passengers) within the network are represented as nodes, and the interactions or relationships among them are represented by the corresponding edges [33]. Based on the nature of interaction (either static or dynamic, metrics, like centrality, cohesion, degree and clustering coefficient among entities of the network) can reveal specific relations among nodes, as well as groups of entities that share common habits.

Cunha et al. [34] showed that vehicles tend to demonstrate a similar behavior and routines in terms of mobility. The vehicles mobility could be mapped in terms of social network, following the same basic laws of degree distribution and distance among nodes. Applying Social network analysis on vehicular networks can consequently improve the performance of communication protocols and services. Graph theory concepts, like centrality and clustering, can be applied in vehicular networks, as long as they integrate their specific features, such as mobility of nodes, channel conditions and drivers' behavior.

For information spreading in a network, the centrality of nodes has most important role to play [35, 36]. In a similar way, central nodes can serve as good spreaders of infections [37] or as good points for building defense mechanisms [38]. Furthermore, central nodes can be elected as the cluster head of groups that are created on the fly. A cluster head may act as a relay node for inter clusters traffic or as a relay node for intra-cluster communication [39].

1.4 Types of Attack in IoV

In information security, STRIDE Threat Model classifies attacks and threats into six main categories [40], specifically: tampering with data, spoofing identity, repudiation, disclosure of information, denial of service and elevation of privilege. Especially, Internet of Vehicles system is prone to different attacks like jamming, interference, eavesdropping and so on, These attacks and threats decease the stability, robustness, real-time, security and privacy of IoV, and make it lose the ability to provide effective services, even cause serious accidents [41–45], due to following constraints such as dynamic topology characteristics, bandwidth limitations, transmission power limitations, abundant sources, mobile limitation, non-uniform distribution of nodes, perception of vehicle dependent data on the trajectory, large scale network etc.

Following are various types of attacks in IoV.

Attacks on Authentication: This attack is categorized in to following sub-classes:

Sybil attack: In wireless networks, a single node with multiple identifications can damage the system by controlling most nodes in the system.
GPS deception: GPS deception can provide a node with fake information about its location, speed and some other GPS information.
Masquerading attack: In a network environment, this attack uses fake identity to gain the network access.
Wormhole attack: This kind of attack always have fatal influences on IoV system due to its characteristics of change and high dependence on efficient routing algorithm.

Availability Attacks: Denial of service and channel interference are common types of attacks on availability.

Secrecy Attacks: This steals data by eavesdropping or interception.

Routing Attacks: There are four different attack types in routing process [46, 47], which includes Eavesdropping [48], Denial of service [49], Masquerading [50], Route modification [51].

Data Authenticity Attacks: It is necessary to ensure that the source data has not been modified when data packets are transmitted through the network. Data authenticity attacks can be categorized into four subtypes namely: Replay attack, Camouflage attack, Fabricating and tampering with messages and Illusion attack [51–53].

1.5 Threats in SIoV

The security in vehicular network is a vital aspect of SIoV, because any negotiation in security could lead to life-threatening situations along with damage of other components that use the SIoV. Social vehicular network security contemplates social characteristics and human behavior in a similar manner [32]. This section reviews issues of security, trust along with reputation in vehicular networks with a specific focus on the social aspects.

SIoV Threats. Raya has reviewed the threats available in vehicular networks and categorized them into insider/outsider, malicious/rationale and active/passive categories [54]. Zeadally [55] has differently classified them into threats to availability, authenticity and to confidentiality.

Denial of Service (DoS) Attack aims to prevent legal users from accessing data or services in computer networks. In vehicular networks, large volumes of irrelevant messages will be flooded that result in jamming of the traffic that negatively impacts the communication between the network's nodes, on-board units and roadside units.

False Message Injection. An attacker from inside can mark a false message and broadcast it to the network. In this manner the attacker can falsify the traffic flow and could affect the decisions of other drivers, causing damage either through traffic jams or accidents.

Malware, such as viruses or worms, is typically introduced through outside unit software and firmware updates. Malware can contaminate vehicles and even permit remote adversaries to acquire control of individual vehicles.

Masquerading and Sybil. In a masquerading attack, a vehicle fakes its identity and pretends to be legal in the networks of the vehicle. Outsiders can carry out attacks, e.g. injecting false messages. In a Sybil attack, the attacker creates multiple identities and pretends to be multiple legitimate vehicles concurrently.

Impersonation Attack. In this, the attacker loots the identity of a legitimate vehicle to broadcast security messages on that vehicle's behalf. This could affect other drivers' decision making and create chaos in traffic.

1.6 Trust Issues in SIoV

There has been a detailed study of establishment of Trust in social networks. Original the concept of social trust was based on sociology. According to Golbeck, trust is defined as "a commitment to an action based on a belief that the future actions of that individual will lead to a good outcome" [56]. The social network as platforms to build mutual trust among entities was foreseen by Golbeck [57]. Wang et al. [58] has proposed a trustworthy Web service selection approach based on collaboration reputation by constructing a Web service collaboration network based on social networks. Zhang et al. [59] has proposed a newly-fashioned scheme BiFu, enabling the social media sites to alleviate the influence of the cold-start problem. Huang et al. [60] has proposed an approach that is capable of measuring the reputation of a single node effectively when the node suffers from malicious feedback ratings. Following are the trust issues in SIoV.

SIoV Trust Characteristics: There are five characteristics of Trust in the SIoV that makes them different from trust in customary social settings.

Uncertainty: Being dynamic trust is uncertain in SIoV.
Subjectivity: Trust in the SIoV depends on our actions consequences that is affected by the context [61] and that is what make it subjective.
Intransitivity: Trust in the SIoV is not always transitive
Context Dependence: Trust in the SIoV is context-dependent
Non-cooperativeness: Trust in the SIoV is need not be always cooperative

Reputation: Reputation management is component of trust management. Trust is dynamic and indicates whether an individual is to be believed on the basis of the trust value. Reputation is submissive and represents estimation about an individual. A reputation system could be classified into positive and negative reputation.

Overall trust is a multifaceted concept. SIoV faces two big challenges in form of trust-based management and decision making. For establishment of trust one needs to address the trust characteristics of the SIoV.

Security and privacy of IoV are serious issues because it will affect the lives of people on the roads. If network intrusion happens in IoV, the vehicles may be controlled by

hackers, and this will lead to traffic havoc. So the security of IoV is a very serious issue. At the same time, driving tracks are the privacy of people. People may not want to let others know where and when they have been. However, the IoV could capture and driving track of vehicles, which will reveal the privacy. Some information in IoV could be public, while some information must be protected as privacy. Ensuring security could assure the safety of vehicle driving and also protect the privacy of people.

Thus we could see following queries for which we will try to find out answers in the context of SIoV:-

How trust recognition can be made in SIoV?
How to store, transform and analyze such a data surge?
Which are the technologies that should be capable of and scalable to in the era of ever increasing vehicular data?

This paper proposes an architecture wherein inter-vehicle recommendation system could be established with the assistance based on social networks by enabling reliable exchange of information.

The current paper is structured into four sections. The first section briefly introduces the concept of Internet of Vehicles, Social Internet of Vehicles, Security and Threats concerns in IoV as well as in SIoV and describes how the big data paradigm will be useful in analyzing the data generated in IoV. This Section also presents a comprehensive survey of previous research works in the area of IoV, SIoV as well as Big Data in IoV. Second section elucidates the proposed recommendation model and followed by discussion. Third section concluded with the essential features of the proposed model and future direction and followed by list of relevant references.

2 Proposed Architecture and Discussion

The current work proposes a recommender system model for IoV assisted by social networking recommendation system that uses reputation received in daily relationships, such as acquaintances meeting or helping other users. An acquaintance is a reliable person, previously known, who can provide the recommendation of others. A reputation acquaintance is a user having an indirect relationship with another user sent to the social network via reputations, so it is considered reliable by reputation.

Let's suppose that two previously known users Ride 1 and Ride 2 do not have any acquaintances in the social network. Their interaction through the social network makes them reliable users with HIGH trust level. They also trade their list of acquaintances. Upon having acquaintance with each other, the Ride 1 can exchange reliable messages with every acquaintance of Ride 2. Similarly, Ride 2 can exchange messages with acquaintances of Ride 1 as he has a path on the certification graph to the acquaintances of Ride 1. Figure 2 illustrates this situation. It can be depicted from the figure that Ride 2 has the users Ride 3 and Ride 4 as acquaintances, these users will be notified of the new relationship of Ride 1 and Ride 2.

The user receives messages and validates those messages using his likes and the followers-list stored in the user's equipment. The message will be considered as reliable

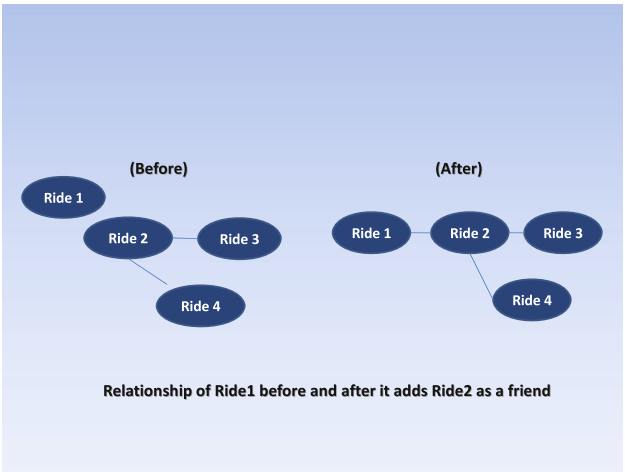

Fig. 2. Relationship of Ride 1 before and after adding Ride 2 as its friend

if the users on the receiver's social network has garnered a positive reputation for the sender or if its sender belongs to the social network of the receiver. Otherwise, the message is considered not reliable and ignored.

The operation of social networking recommendation as shown in Fig. 3 is based on PGP (Pretty Good Privacy) [62], and works as follows:

Step 1: The user generates a self-liked page.
Step 2: The page can be liked and followed by acquaintances in direct contact.
Step 3: The device of each user stores the likes and follower list of the added acquaintance and its acquaintances of acquaintances.
Step 4: The page of the new acquaintance is shared with the user's acquaintances to update their lists of acquaintances of acquaintances. Acquaintances of acquaintances recognize the page and thus receive reliable messages, giving out the conviction of the acquaintance that is a reliable user.
Step 5: After meeting a user, communication starts by searching a valid page address. Identification of a common acquaintance permits the users to verify their identities.

A Ride who does not trust a sender because he is not in his acquaintance, or even acquaintance of acquaintances, examines the page to determine if the sender is reliable. When receiving a message from a node that is neither an acquaintance nor a friend of his acquaintance then the receiving node considers the sender is reliable only when the number of its positive reputations is more than to the negative ones. The receiver takes into account the valuations of reliable users only when the users who are acquaintances or acquaintances of acquaintances of the receiver.

Linking reputation to the social network of the user restricts collusion attacks. Collusion can be produced when malicious users make a positive bonus for each other.

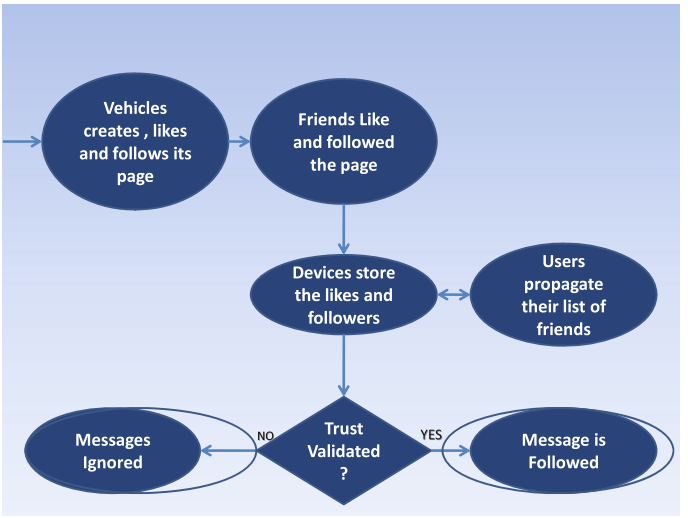

Fig. 3. Flow graph of the proposed model.

Thus, reputation is an additional prospect of trust acknowledgment, which permits users who are acquaintances or acquaintances of acquaintances to be measured trustworthy. Reputation can also have special feature to rate acquaintances or acquaintances of acquaintances.

Besides SIoV, the social networking also generates huge amount of data that needs to be analyzed to provide more reliable recommendation system. Thus we can see that sensor data along with data generated from social networking data is required to be processed for making vehicular system intelligent. This guides us to tap the potential of Big Data Analysis. It is clear that the IoT, IoV and SIoV applications can generate unprecedented amount of data for which big data provides promising tool [63, 64] to store and process these data.

The data sets generated from IoV have similar characteristics as that of big data i.e. volume, velocity, variability, variety, veracity, values, even visualization (i.e. Vi –where i = 1, 2, …, n) as shown in Fig. 4.

The algorithms for IoV big data set analysis can be grouped in many forms, which include heterogeneous, nonlinear, high-dimensional and distributed data processing [65].

As shown in Fig. 5, we could use this big data framework to analyze massive IoV and SIoV data for predicting congestion and free movements of traffic in making well-organized runtime traffic management. It is quite clear from proposed model that First Step is the pre-processing of raw data to ETL (Extract, Transform, Load), the second step is to analyze the pre-processed data using various Big Data Analytics tools to meet the defined objectives/goals and in the last and third step the outcomes of the analysis are to be used to generate desired results in form of reports, queries or future predictions. In future this model could be used with SIoV data for sentiment analysis for establishing the trust recognition.

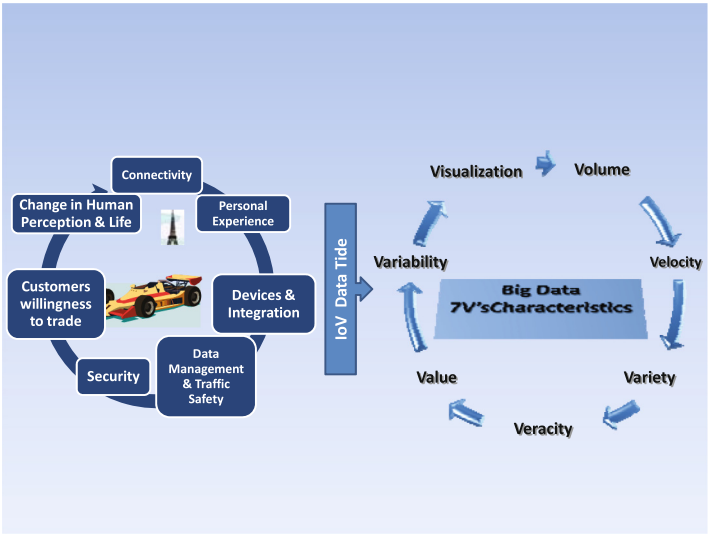

Fig. 4. Big data generation in IoV and its characteristics

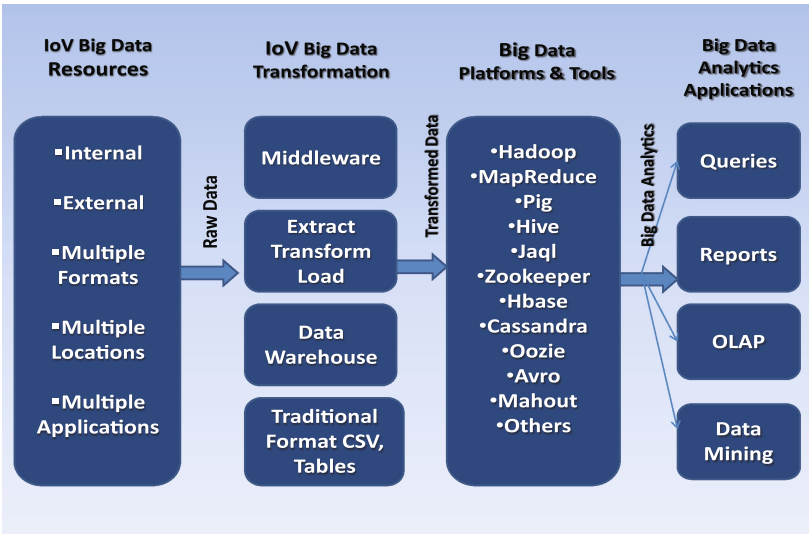

Fig. 5. The model of IoV massive data analytics framework

3 Conclusion

This current work has proposed a novel approach for processing an unprecedented amount of data from completely unrelated networks to create a reliable and trust worthy recommendation system. This social networking recommendation system incorporates

mechanisms for assessment of the trust and reputation of the information sources and thereby permitting the cyber-physical system to trade messages in a reliable way. One can view through direct contacts between two acquaintances that call for their identity, so they rely on the recommendations and thus, establish trust in the cyber-physical systems like that in IoV. Apart from this we have augmented a paradigm of big data Analytics technique for making IoV in to intelligent IoV by processing both the unstructured as well as the structured data sets generated from Social IoV and Social networks. In future we would like to develop an application to analyze social data by big data analytics techniques for sentiment analysis in order to have a better insight of trust recognition.

References

1. Fan, W., Bifet, A.: Mining big data: current status, and forecast to the future. SIGKDD Explor. **14**(2), 1–5 (2013)
2. Bifet, A.: Mining big data in real time. Informatica **37**, 15–20 (2013)
3. Wu, B.: Internet-of-vehicles based on technologies of internet-of-things. In: ICLEM, pp. 348–356 (2012)
4. Vermesan, O., Friess, P.: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, Aalborg (2013). ISBN 978-87-92982-96-4
5. Bin, S., Yuan, L., Xiaoyi, W.: Research on data mining models for the internet of things. In: Proceedings International Conference on Image Analysis and Signal Processing, pp. 127–132 (2010)
6. Leng, Y., Zhao, L.: Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things. In: Proceedings International Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, Heilongjiang, China, vol. 6, pp. 3190–3193 (2011)
7. Goggin, G.: Driving the internet: mobile internets, cars, and the social. Future Internet **4**, 306–321 (2012). doi:10.3390/fi4010306
8. Guo, D., Mennis, J.: Spatial data mining and geographic knowledge discovery: an introduction. Comput. Environ. Urban Syst. **33**, 403–408 (2009). Elsevier
9. Crawford, K., Schultz, J.: Big data and due process: toward a framework to redress predictive privacy harms. B. C.L. Rev. **55**, 93 (2014). http://lawdigitalcommons.bc.edu/bclr
10. Dlodlo, N., et al.: The state of affairs in internet of things research. Electron. J. Inf. Syst. Eval. **15**(3), 244–258 (2012)
11. El-Hoiydi, A., Decotignie, J.D.: WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In: Proceedings of the Ninth International Symposium on Computers and Communications (ISCC 2004), Alexandria, Egypt, vol. 1, pp. 244–251, 28 June–1 July 2004
12. Perkins, C.E.: Ad Hoc Networking. Addison-Wesley Professional, Boston (2008)
13. Caballero-Gil, P., Caballero-Gil, C., Molina-Gil, J.: How to build vehicular ad-hoc networks on smartphones. J. Syst. Architect. **59**, 996–1004 (2013)
14. Liu, B., Liu, Z., Towsley, D.: On the capacity of hybrid wireless networks. In: Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications on IEEE Societies (INFOCOM 2003), San Francisco, CA, USA, vol. 2, pp. 1543–1552, 30 March–3 April 2003

15. Wang, M., Shan, H., Lu, R., Zhang, R., Shen, X., Bai, F.: Real-time path planning based on hybrid-VANET-enhanced transportation system. IEEE Trans. Veh. Technol. **64**, 1664–1678 (2014)
16. Tornell, S.M., Patra, S., Calafate, C.T., Cano, J.C., Manzoni, P.: GRCBox: extending smartphone connectivity in vehicular networks. Int. J. Distrib. Sens. Netw. **2015**, 478064 (2015)
17. Marquez-Barja, J.M., Ahmadi, H., Tornell, S.M., Calafate, C., Cano, J., Manzoni, P., Da Silva, L.: Breaking the vehicular wireless communications barriers: vertical handover techniques for heterogeneous networks. IEEE Trans. Veh. Technol. **64**, 5878–5890 (2014)
18. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**, 1645–1660 (2013)
19. Joerer, S., Bloessl, B., Huber, M., Jamalipour, A., Dressler, F.: Demo: simulating the impact of communication performance on road traffic safety at intersections. In: Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, Maui, HI, USA, pp. 287–290, 7–11 September 2014
20. Maglaras, L.A., Basaras, P., Katsaros, D.: Exploiting vehicular communications for reducing CO_2 emissions in urban environments. In: Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, pp. 32–37, 2–6 December 2013
21. Cheng, H.T., Shan, H., Zhuang, W.: Infotainment and road safety service support in vehicular networking: from a communication perspective. Mech. Syst. Signal Process. **25**, 2020–2038 (2011)
22. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The Social Internet of Things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**, 3594–3608 (2012)
23. Alam, K., Saini, M., El Saddik, A.: Toward social internet of vehicles: concept, architecture, and applications. IEEE Access **3**, 343–357 (2015)
24. Alam, K.M., Saini, M., Saddik, A.E.: Workload model based dynamic adaptation of social internet of vehicles. Sensors **15**, 23262–23285 (2015)
25. Nitti, M., Girau, R., Floris, A., Atzori, L.: On adding the social dimension to the internet of vehicles: friendship and middleware. In: Proceedings of the 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, pp. 134–138, 27–30 May 2014
26. Luan, T., Lu, R., Shen, X., Bai, F.: Social on the road: enabling secure and efficient social networking on highways. IEEE Wirel. Commun. **22**, 44–51 (2015)
27. Schwarz, C., Thomas, G., Nelson, K., McCrary, M., Sclarmann, N., Powell, M.: Towards autonomous vehicles. Technical report 25-1121-0003-117, Mid-America Transportation Center, Lincoln, NE, USA (2013)
28. Squatriglia, C.: Ford's Tweeting Car Embarks on American Journey 2.0. Wired (2010). http://www.wired.com/2010/05/ford-american-journey/. Accessed 15 Jan 2016
29. Sha, W., Kwak, D., Nath, B., Iftode, L.: Social vehicle navigation: integrating shared driving experience into vehicle navigation. In: Proceedings of the 14th Workshop on Mobile Computing Systems and Applications, Jekyll Island, GA, USA, 26–27 February 2013
30. Wan, J., Zhang, D., Zhao, S., Yang, L., Lloret, J.: Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. IEEE Commun. Mag. **52**, 106–113 (2014)
31. Vegni, A., Loscri, V.: A Survey on Vehicular Social Networks. IEEE Commun. Surv. Tutor. **17**, 2397–2419 (2015)

32. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. Appl. **37**, 380–392 (2014)
33. Scott, J.: Social Network Analysis. Sage Publications Ltd., Thousand Oaks (2012)
34. Cunha, F., Carneiro Vianna, A., Mini, R., Loureiro, A.: How effective is to look at a vehicular network under a social perception? In: Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, pp. 154–159, 7–9 October 2013
35. Basaras, P., Katsaros, D., Tassiulas, L.: Detecting influential spreaders in complex, dynamic networks. Computer **46**, 24–29 (2013)
36. Borge-Holthoefer, J., Rivero, A., Moreno, Y.: Locating privileged spreaders on an online social network. Phys. Rev. E **85** (2011). doi:10.1103/PhysRevE.85.066123
37. Canright, G.S., Engø-Monsen, K.: Spreading on networks: a topographic view. Complexus **3**, 131–146 (2006)
38. Noel, S., Jajodia, S.: Optimal IDS sensor placement and alert prioritization using attack graphs. J. Netw. Syst. Manag. **16**, 259–275 (2008)
39. Souza, E., Nikolaidis, I., Gburzynski, P.: A new aggregate local mobility (ALM) clustering algorithm for VANETs. In: Proceedings of the 2010 IEEE International Conference on Communications (ICC), Cape Town, South Africa, pp. 1–5, 23–27 May 2010
40. Lazarevic, A., Srivastava, J., Kumar, V.: Cyber threat analysis–a key enabling technology for the objective force (a case study in network intrusion detection). In: Proceedings of the IT/C4ISR, 23rd Army Science Conference (2002)
41. Yu, L., Deng, J., Brooks, R.R., Yun, S.B: Automobile ECU design to avoid data tampering. In: Proceedings of the 10th Annual Cyber and Information Security Research Conference, p. 10. ACM (2015)
42. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
43. Singh, R., Singh, P., Duhan, M.: An effective implementation of security based algorithmic approach in mobile adhoc networks. Hum. Centric Comput. Inf. Sci. **4**(1), 1–14 (2014)
44. Othmane, L.B., Weffers, H., Mohamad, M.M., Wolf, M.: A survey of security and privacy in connected vehicles. In: Benhaddou, D., Al-Fuqaha, A. (eds.) Wireless Sensor and Mobile Ad-Hoc Networks, pp. 217–247. Springer, New York (2015)
45. Yan, G., Wen, D., Olariu, S., Weigle, M.C.: Security challenges in vehicular cloud computing. IEEE Trans. Intell. Transp. Syst. **14**(1), 284–294 (2013)
46. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., Jamalipour, A.: A survey of routing attacks in mobile ad hoc networks. IEEE Wirel. Commun. **14**(5), 85–91 (2007)
47. Cheng, J., Cheng, J., Zhou, M., Liu, F., Gao, S., Liu, C.: Routing in internet of vehicles: a review. IEEE Trans. Intell. Transp. Syst. **16**(5), 2339–2352 (2015)
48. Shah, N., Valiveti, S.: Intrusion detection systems for the availability attacks in ad-hoc networks. Int. J. Electron. Comput. Sci. Eng. (IJECSE) **1**(3), 1850–1857 (2012). ISSN 2277-1956
49. Ji, S., Chen, T., Zhong, S.: Wormhole attack detection algorithms in wireless network coding systems. IEEE Trans. Mob. Comput. **14**(3), 660–674 (2015)
50. Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the RPL-based internet of things. Int. J. Distrib. Sens. Netw. 13(794326) (2013)
51. Xia, H., Jia, Z., Li, X., Ju, L., Sha, E.H.-M.: Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw. **11**(7), 2096–2114 (2013)
52. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on vanet security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)

53. Rawat, D.B., Yan, G., Bista, B., Weigle, M.C.: Trust on the security of wireless vehicular ad-hoc networking. Ad Hoc Sens. Wirel. Netw. (AHSWN) J. **24**, 283–305 (2014)
54. Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, pp. 11–21, 7 November 2005
55. Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. **50**, 217–241 (2012)
56. Golbeck, J.: Computing with trust: definition, properties, and algorithms. In: Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, pp. 1–7, 28 August–1 September 2006
57. Golbeck, J.: Computing with Social Trust. HCI. Springer, London (2008)
58. Wang, S., Huang, L., Hsu, C.-H., Yang, F.: Collaboration reputation for trustworthy Web service selection in social networks. J. Comput. Syst. Sci. **82**(1), 130–143 (2016)
59. Zhang, D., Hsu, C.H., Chen, M., Chen, Q., Xiong, N., Lloret, J.: Cold-start recommendation using bi-clustering and fusion for large-scale social recommender systems. IEEE Trans. Emerg. Top. Comput. **2**(2), 239–250 (2014)
60. Huang, L., Wang, S., Hsu, C.H., et al.: J. Supercomput. **71**, 2190 (2015). doi:10.1007/s11227-015-1432-x
61. Gupta, S.: A general context-dependent trust model for controlling access to resources. Ph.D. thesis, Jadavpur University, Kolkata, India (2012)
62. Djamaludin, C., Foo, E., Corke, P.: Establishing initial trust in autonomous delay tolerant networks without centralised PKI. Comput. Secur. **39**(Part B), 299–314 (2013). Elsevier
63. Crawford, K., Schultz, J.: Big data and due process: toward a framework to redress predictive privacy harms. BCL Rev. **55**, 93 (2014). http://lawdigitalcommons.bc.edu/bclr
64. Tene, O., Polonetsky, J.: Big data for all: privacy and user control in the age of analytics. Nw. J. Tech. Intell. Prop. **11**, 239 (2013). http://scholarlycommons.law.northwestern.edu
65. Diebold, F.X.: Big Data Dynamic Factor Models for Macroeconomic Measurement and Forecasting, pp. 115–122. Cambridge University Press, Cambridge (2003)