VANET Blockchain: A General Framework for Detecting Malicious Vehicles

Ahmad Mostafa
Computer Networks Department
Faculty of Informatics and Computer Science
The British University in Egypt
Email: ahmad.mostafa@bue.edu.eg

Abstract —Malicious nodes are affecting many of the current networks, specially, the decentralized networks such as VANETs. VANETs are highly decentralized networks that are highly dynamic and include many nodes or vehicles that are introduced and leave the network abruptly. In order to overcome this challenge, we propose using the blockchain technology. Blockchain is an emerging technology that is changing how modern system and technologies operate. Many systems nowadays are based on this technology including the Bitcoin system. However, many other technologies are realizing the potential benefits of the blockchain technology. In this paper, we propose the use of mini blockchain in the detection of malicious vehicles in VANET. We propose a general framework in which malicious vehicles will not be able to gain the trust of other vehicles and be part of the network. This is achieved through the utilization of environmental sensory data and validating the authenticity of the packets, and allowing a vehicle to add different blocks to the blockchain. We show that our framework is able to deal with malicious nodes and with Sybil attacks.

Index Terms—VANET, blockchain, sybil attacks, authentication, data validation, mini blockchain, fingerprint, malicious nodes.

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANET) is becoming more relevant in todays networks and is becoming an essential part of the roads. This is mainly due to the fact of the advances in connectivity and capabilities of vehicles which have led to the introduction of autonomous vehicles. Autonomous vehicles are highly capable due to being equipped with different types of sensors in order to understand the environment and react according to the best interest of the driver. The control of the autonomous vehicle is based on machine learning techniques without any intervention from the driver or passengers of the vehicle. This introduces a main security concern, since if the vehicle is attacked or is malicious, it can cause major accidents or damage.

Moreover, the VANET is based on connectivity between the vehicles, which is achieved either through vehicle-to-vehicle (V2V) connectivity or through vehicle-to-infrastructure (V2I) connectivity. This can be demonstrated in Fig. 1. In V2V, vehicles are highly dependent on information that they receive from other vehicles. The information can be for convenience applications such as infotainment, or it can crucial information such as the occurence of accidents or road conditions. In this scenario, a malicious node can cause an extensive amount of harm if it conveys false or misleading information to other vehicles.

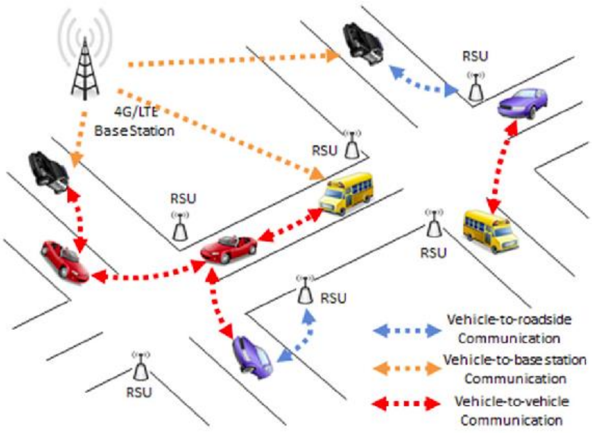
4G/LTE
Base Station
RSU
RSU
RSU
RSU
RSU
RSU
Vehicle-to-roadside Communication
Vehicle-to-base station Communication
Vehicle-to-vehicle Communication

Fig. 1. VANET general architecture [1].

One of the concepts that has been introduced in recent years that verifies identity along with the proof that specific work has been done is the blockchain technology [2]. Blockchain is the backbone of different technologies including cryptocurrency (BitCoin). The technology of blockchain is based on unifying a ledger between all nodes in the network in a distributed fashion and insure that no external node can join the network without authorization. In this aspect, in order for a node to participate in the system or to perform any mining, the node has to prove that it has utilized some amount of actual resources such as computing power in order to be able to mine. However, some research has been done in order to overcome the limitation of proof of work and replacing it by the proof of stake [3]. In proof of stake, the nodes that are allowed to participate in mining are the nodes that are stakeholders in the system.

In order to overcome this issue of malicious vehicles, we introduce a general framework that utilizes blockchain in order to detect such vehicles within the

Manuscript received September 18, 2018; revised April 9, 2019.
doi:10.12720/jcm.14.5.356-362

network. The framework relies on using a fingerprint from the vehicles in order to ensure that the vehicle has been part of the existing network. This idea has been presented earlier in literature [4]. However, it was used for static Internet-of-Things (IoT).

Once the fingerprint is verified, the blockchain provided by the vehicles is examined to verify its authenticity. If it is authentic, then the vehicles will be able to reach consensus on one blockchain, and hence, this blockchain will propagate through the whole network through vehicle communication. However, one issue is that the size of the blockchain increases as the number of nodes in the network increases. In order to overcome this limitation, we proposed the use of mini blockchain.

This paper is organized as follows: in the next section we introduce the related work to detect malicious nodes within VANETs. Following that, we introduce the general concept of blockchain, mini blockchain, importance of environmental data and introduce our framework. Finally, we discuss the validity of framework followed by a conclusion.

II. Related Work

Detection of malicious vehicles have been studied in literature. Some authors have proposed the detection of malicious vehicles through searching for possible explanations for the data with the assumption of the existence of malicious nodes [5]. Following that, the data is scored and is ranked according to the score and that score is used to detect the malicious vehicle.

In [6], the authors have proposed the modification of the existing Ad-Hoc On Demand Distance Vector (AODV) routing protocol in order to be able to isolate malicious vehicles and to avoid collisions between the different vehicles in the vehicular network.

On the other hand, some authors proposed a new system called TrustLevel [7]. In this system, each vehicle is ranked according to the accuracy of its information. TrustLevel utilizes data from other surrounding vehicles in order to verify the validity of the transmission. Following that, TrustLevel uses a reward level system in order to enhance communication within the VANET. In [8], the authors proposed the utilization of data mining techniques and proposed a VANETs Association Rules Mining (VARM). VARM is a mining technique that takes place apriori to the communication taking place, and will be used in order to detect any malicious communication.

Since the introduction of the blockchain technology and the increased interest that it witnessed due to Bitcoin [9], it has been used in many security applications in order to ensure the validity and authentication of data and entities. Some approaches have been introduced to utilize blockchain in the security of Internet-of-Things (IoT) devices. For example, in [10], the authors proposed the use of blockchain in smart home in which they eliminate the proof of work and coins technology and concepts. In their approach, the system is composed of three main layers: a cloud storage, overlay and a smart home. However, the system also requires a highly capable devices within the smart home to act as a miner. This approach might be applicable in static networks, however, it is not possible to use in highly dynamic networks such as VANETs or in a distributed architecture.

Others have also introduced the use of blockchain in distributed environment. The authors in [11] have proposed blockchain for vehicular networks. They integrated the VANET technology with the Ethereum technology and used the Ethereum smart contract technology in order to authenticate and validate the vehicles within the VANET. Their proposed approach was for both essential and infomercial applications. In [12], the authors proposed the use of blockchain within VANET while preserving the privacy and the anonymity of the vehicle. They relied on distributed trust in order to reduce the block validation time, and hence, become more applicable to VANET environment.

In [13], the authors introduced TrustBit, a reward-based intelligent vehicle communication using blockchain. The main idea behind trust bit is that each communication between vehicles is validated and stored in the cloud. Once a vehicle would like to verify the validity of any data it received, it can verify it through the cloud. One main disadvantage for this approach is that it relies on continuous communication with the cloud which adds overhead to the network. In order to reduce this communication overhead, the authors in [14] proposed a framework that utilizes blockchain and edge computing instead of cloud computing. The authors divided the architecture into three layers: the perception layer, the edge-computing layer and the service layer. Although this framework is more reliable and applicable for VANET environment, it does not help avoid or handle malicious nodes in the network.

Anonymity of the vehicle and its privacy has also been one of the applications of blockchain in recent literature. The authors in [15] introduced blockchain-based anonymous reputation system (BARS), which established a trust model for VANET while ensuring the privacy of the different nodes in the network. Messages are accepted based on the reputation of the vehicle, which is saved in a central authority. One main challenge with this approach is the idea of a certificate authority and its feasibility in a vehicular environment, especially in the aspect of the certificate monitoring and handling.

In [16], the authors introduced a distributed trust management scheme based on the blockchain technology. This system is based on the organization of the vehicles in clusters, and the designation of an elective cluster head. The miner uses fuzzy logic in order to decide on the validity of the data in the packets being transferred between the different vehicles.

Many of the approaches introduced in literature have relied on some form of centralization whether through the use of a PKI system and a certificate authority (CA), or through the use of cloud or edge computing. This approach is not feasible in a VANET environment due to the high speed of vehicles which results in the dynamic topology of the network, which results in the inability of the network to sustain network overhead. Other approaches have used the blockchain technology in order to validate the vehicle itself. However, once the vehicle is validated, it will not be easy to revoke this validation in order to ensure that it did not become malicious after it was able to gain the trust of the system and the surrounding vehicles.

To our knowledge, this framework introduced in this paper is the first to utilize the blockchain technology in addressing the security and the detection of malicious nodes in VANETs in a completely distributed manner by allowing the vehicles to reach a consensus based on the validation of the data exchanged, and at the same time to allow for the immediate revocation or expulsion of the malicious node from within the network by its neighboring vehicles.

III. Security Challenges in VANET

There are several cybersecurity threats and challenges that are specifically applicable to VANET environment. This is due to the unique nature of the communication patterns and mechanisms in the vehicular environment. These threats are highlighted in Fig. 2.

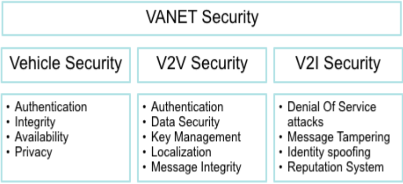

Fig. 2. Different security threats in VANET environment.

Both the V2V and V2I security threats mentioned above are amplified in case the node is malicious. In that case, it is difficult to mitigate the risks that arise from these threats.

In the VANET environment, it is not feasible to use a central authentication system (such as certificate authorities) due to the network overheard from the packets used. This overhead is not feasible in the VANET environment [17]. To overcome this limitation, one of the alternative approaches would be to rely on the authentication of the message being sent and to derive the authentication of the node through the authentication of its communication.

IV. Proposed Solution

In this section, we introduce blockchain and our framework that is based on it.

A. *Blockchain*

The blockchain technology has many benefits, which include transparency, avoidance of malicious nodes, low cost, instantaneous transactions, and network security [18]. The network security aspect of blockchain is due to the fact that the technology uses cryptographic and decentralized conventions. One of the main descriptions of the blockchain technology is that it allows records to be shared across the whole network and is continuously updated in a distributed fashion. The blockchain is a ledger that each node in the distributed network has an identical copy of. Whenever there is a new transaction, the record of this transaction is broadcasted network wide and then it is verified by other nodes in the network. Once this transaction is collectively verified, a new block is added to the blockchain, and the new blockchain propagates through the network so every node has an updated version. However, the fact that the network is distributed, makes the consensus between the nodes challenging, hence, a cryptographic algorithm is used within blockchain that is based on the public-private key cryptography.

In order for a node to add a block to the blockchain, it needs to prove that has accomplished enough computation resources in solving a math puzzle. This effort required grows exponentially with the length of the blockchain, however, the verification process remains simple and does not require much effort from the verifying nodes.

Within the network, the only valid blockchain is the longest blockchain, and any other alternative (i.e. shorter) blockchain is discarded. Fig. 3 demonstrates a sample of what a blockchain can look like.

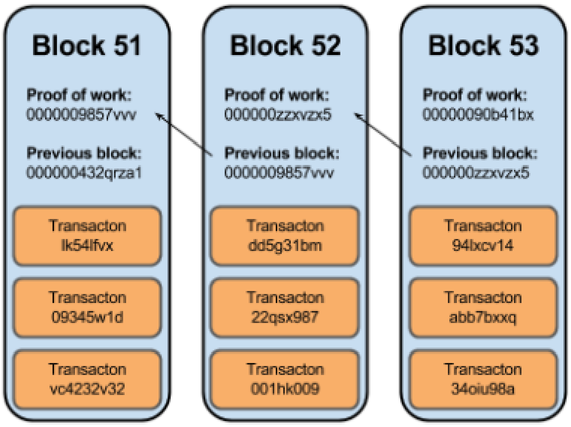

Fig. 3. A sample of how a blockchain can look like [19].

B. *Mini Blockchain*

One of the main challenges of the traditional blockchain technology is the length of the blockchain and size which is not feasible for communication in VANET due to the different environment communication restrictions. In [20], the authors introduced the mini blockchain scheme. In this scheme, the mini blockchain is composed of three components: the account tree, the transaction tree, and the proof of chain. Once one node is able to authenticate a block, it adds it to its blockchain. However, once a block is added, another block can be removed from the end of the blockchain (the account tree and the transaction tree). However, the proof chain is stored in its entirety and no information about any block is removed from it. This ensures that the length of the blockchain remains manageable as the network size increases.

C. General Architecture

In this paper, we focus on two aspects of VANET:

- Authenticating the Vehicle: In this regards, our proposed system aims to make sure that any malicious vehicle within the network can be detected.
- Authenticating Data from Vehicle: In this regards, we are aiming to allow the vehicles to verify the data being received and eliminate any suspicious data.

In order to achieve both requirements mentioned above, we have to propose a system that can deal with malicious nodes or malicious data at the origin. Hence, the system has to be a fully distributed system at which neighboring vehicles are able to verify the authenticity of the vehicle, whether it is malicious or not, and to verify that the data being received is authentic. The approach to achieve the last aspect is to make sure that the neighboring vehicle itself is the one who generated this data, or that it can vouch for the vehicle who generated it. In order to be able to vouch for the generator, the blockchain has to be authentic, and we will see in the next subsection, this is verified through the length of the blockchain which evolves over the lifetime of the network.

Our framework is based on allowing each vehicle to have its own blockchain. However, upon communicating with other vehicles, both vehicles have to reach a consensus on one blockchain, which is the longest of both versions (one for each communicating vehicle). If the vehicle is not able to authenticate the neighbors' blockchain or its data, then they do not exchange blockchains. Once a successful exchange takes place, the blockchain is amended and hence, its length becomes longer. A malicious vehicle will not be able to obtain a copy of the existing blockchain and due to the lack of successful exchanges, the length of its own blockchain will be shorter than the acceptable threshold in the network.

In the next subsections, we will explain the main steps in our proposed framework.

D. Validation through Environmental Data

Data validation has been a challenge in communication systems and in vehicular networks for some time. There has been many different approaches introduced in order to validate the data generated in VANET. In [21], the authors relied on the fact that vehicles generate sensory data that can be matched with what should be similar to that of neighboring vehicles. In [22], the authors used Markov chain in order to achieve data validation. Moreover, in [23], the authors used a probabilistic approach that relies on blockchain and the PKI system to ensure the validity of the data through the validation of the vehicle. Other approaches used sensory data as well, such as the approach introduced in [24]. In this approach, the generation of the data is coupled with sensory data in order to ensure the validity of the node and the data.

Environmental sensory data can be used in order to validate the generation of data by a vehicle. In static networks, the discovery of malicious vehicles based on this environmental data has been successful, specially due to the fact that any discrepancy in this data would be flagged as malicious. This can be demonstrated in Fig. 4. In this figure, the rate of detection of malicious vehicles is dependent on the percentage of malicious nodes in this network. This is based on the fact that if the number of malicious nodes increase, the higher the possibility of collusion between the vehicles, and hence the possibility of detection is lower. The requirement for this scenario is that the malicious nodes are in each other's vicinity. This scenario has a lower probability in VANET environments due to the fact of the fast changing topology. Hence, the malicious vehicles staying in each other's vicinity in order to collude has a lower probability that the case of statics networks.

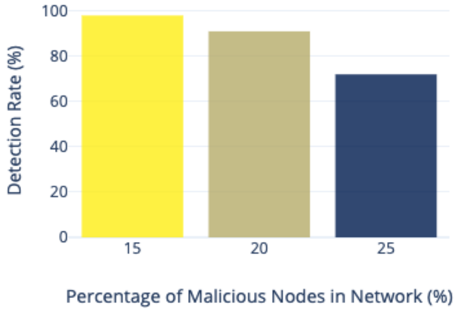

Fig. 4. Detection rate of static malicious nodes using environmental data [24].

However, the impact of environmental data in VANET is different than static networks. This is due to the fact that the vehicles' speed allows for a larger variation in the environmental data sensed. Although some data such as the temperature should not vary in the short time span of the vehicle movement, other readings should vary such as the air pressure. In this case, the vehicle (both transmitting and receiving) should adjust the acceptable threshold and range of data variation in these readings. Once this data is validated, it will be verified that the vehicle transmitting this data is the vehicle that has generated it. In this case, if the actual data is malicious, then the vehicle that generated it is a malicious vehicle. However, if the packet was forwarded by a vehicle, then this does not indicate that the forwarding vehicle is malicious.

E. Our Framework

In order to explain our framework, we will use the scenario presented in Fig. 5. Assume that vehicle 2 (V2) is already existent in the network and vehicle 1 (V1) is trying to join the network. V2 will be required to verify that V1 is not malicious node. The steps of the framework are as follows:

- Once communication takes place between V1 and V2, and V2 receives a packet from V1, V2 considers that the packet is considered a suggestion for what can be considered the next block in the blockchain.
- The packet sent from V1 to V2 includes the data generated by V1 along with the different environmental data such as the location, the air temperature and pressure. This extra information helps V2 verify that V1 is within the vicinity if the environmental data matches with V2's own data as explained in the previous subsection. Before V1 sends its packet, it encrypts it with its private key and includes its blockchain (BC1).
- Once V2 receives BC1, it checks its length. If it finds that the length is significantly lower than its own blockchain BC2, then it will consider V1 to be a malicious vehicle. V2 will drop the packet and the information that it received from V1, and will respond to V1 with a null blockchain.
- If V2 detects that the length of BC1 is valid, then V2 will decrypt V1's data and computes the hash of the environmental data of V1 to make sure that it is within its vicinity.
- Now, V2 will validate the data within the packet that it received from V1.
- If V1 data is valid, then V2 will concatenate V1s block with the longest blockchain between BC1 and BC2. However, V2 will encrypt this block with both its private key and with V1s public key. This is essential so no other vehicles who V2 communicates with will be able to decrypt the last block (and hence, modify it). Once the block is encrypted, V2 sends the longest blockchain produced to V1 and V1 will adopt the new blockchain as its own.
- If V1 data is not valid, then V2 rejects V1 suggested block and doesn't send anything back to V1.

This framework can be demonstrated using the steps specified in Fig. 5:

1. V1 computes the different environment data such as temperature, air pressure, etc.
2. V1 sends its blockchain (BC1) along with the environmental data and actual data to V2.
3. V2 receives the data, and separates the BC1 from the environment data and the actual data.
4. V2 starts the verification process by checking that:
   i. the environmental data is valid.
   ii. BC1 length is not significantly different that BC2 by the threshold value.
   iii. The actual data provided by V1 is valid and does not contradict with other data received by V2 from other vehicles.
5. Once V2 verifies all data from step 4, then it will send the largest blockchain (between BC1 and BC2) back to V1.
6. V1 will receive the new blockchain and replace it with the blockchain it had.

The different steps of the framework are demonstrated in flowchart shown in Fig. 6.

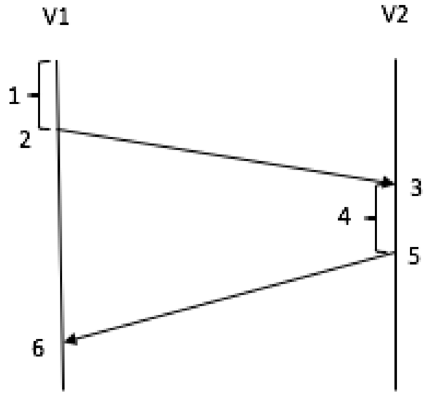

Fig. 5. A demonstration of framework in communication between vehicles according to steps (1 – 5) highlighted in explanation.

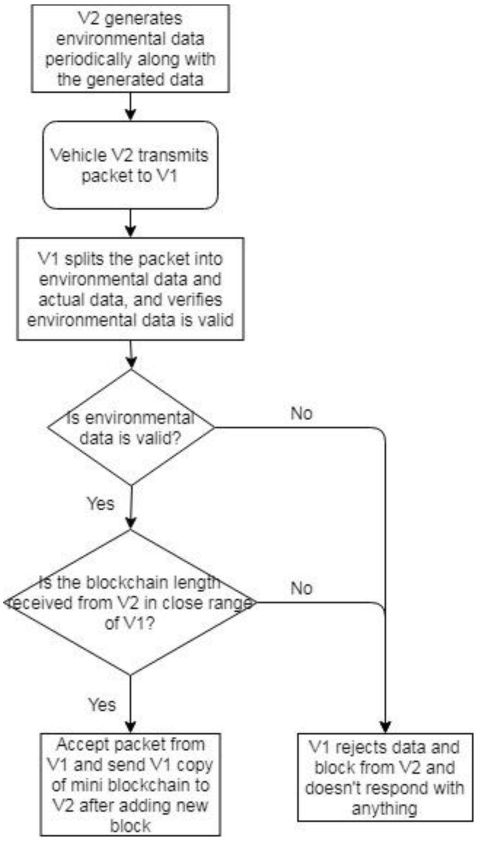
V2 generates environmental data periodically along with the generated data
Vehicle V2 transmits packet to V1
V1 splits the packet into environmental data and actual data, and verifies environmental data is valid
Is environmental data is valid?
No
Yes
Is the blockchain length received from V2 in close range of V1?
No
Yes
Accept packet from V1 and send V1 copy of mini blockchain to V2 after adding new block
V1 rejects data and block from V2 and doesn't respond with anything

Fig. 6. Flowchart illustrating the different steps of the framework.

IV. Discussion

In order to present the effectiveness of our framework, we will assume that there is a malicious vehicle and it is trying to infiltrate the network. This malicious node will attempt to communicate with the neighboring vehicles in order to get a copy of their blockchain. Once this communication is not successful, the malicious node will have one of two choices:

1. Delete its block chain and start all over again as a new node. If the vehicle decides to delete its blockchain, it will be dealt with as a new node joining the network, and hence, it will have to provide non-malicious activity in order to receive a legitimate copy of the blockchain within the network. However, at any step, if the vehicle sends any malicious activity, then it will be risking its own blockchain and will have to resort to either deleting its blockchain or to resort to an earlier version of it.

2. Start with the blockchain of the last acceptable blockchain length. If it chooses to attack again another vehicle, over some time it will suffer from having a very short block chain compared to the average accepted block chain size in the network. Therefore, at that point, no other vehicle will accept any communication from this vehicle and it will be considered malicious from all the other vehicles, and thus will be forced to delete its block chain and start all over again.

This decentralized approach, where attacks are being handled locally guarantees the anonymousness of all the involved vehicles, as it does not deal with their identities. The handling of the anonymity of the vehicles is essential in order to be able to avoid Sybil attacks, where identities can't be forged and block chains can't be manipulated.

Moreover, this framework allows for the vehicles to reach consensus between each other on one common blockchain that propagates through the network. It is expected that the length of this blockchain will keep growing, and hence, it one point it will have to be purged. In order to overcome this issue, each block in the blockchain will have a time to live (TTL) field, after which, this block will have to be deleted from the blockchain in order to avoid the consumption of network resources in overhead. This is done based on the mini blockchain introduced earlier, in which the proof of chain is not purged, however, the account tree and the transition tree are.

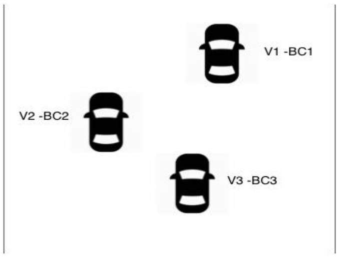

Fig. 7. Vehicles in vicinity with each one its own Blockchain (BC).

One main advantage of this approach is the ability to detect a malicious vehicle once it becomes malicious. In other words, if a vehicle is considered non-malicious and communicates through the network, and then it is attacked and starts sending malicious data, the neighboring vehicles will be able to invalidate the data being sent from this vehicle. The vehicle that was flagged as malicious will continue to be flagged as malicious till it starts sending non-malicious data. Once that is the case, it can start building its mini blockchain and communicating with other vehicles.

Fig. 7. Show Vehicles in vicinity with each one its own Blockchain (BC)

V. Enhancements and Future Work

The approach introduced in this paper has several advantages as mentioned earlier. However, there are two main limitations and future enhancements. These two are:

1. The data validation is still a challenge. A malicious vehicle can wait on generating the environmental data and generate the actual data at the same time. Once it achieves that, it can replace the actual data generated with malicious data. In this case, the actual data has to be validated. While this case is highly unlikely due to the fact that this requires time for generating the actual data, and hence it can scale down the amount of attacks being carried, it is still a possibility. In order to overcome this attack, the solution would be to validate the actual data being sent by the vehicle, besides the validation of the environmental data. Although the environmental data has to be validated on continuous basis, the actual data can be validated at a lower rate.

2. The second challenge would be to create a reputation system tied to the identity of the vehicle. Due to the fact that there is an actual physical contact between the vehicles (they are in the same vicinity), the identity of the vehicle can be based on the image of the vehicle. Vehicles are not identical due to the existence of license plate numbers, hence, the image of the vehicle can be considered as a fingerprint. This can be achieved through image processing techniques, and this is becoming more of a possibility based on the fact that vehicles are being equipped with high technology including cameras in order to allow for the autonomous vehicle technology and smart vehicles.

VI. Conclusions

To sum up, this paper introduces a general approach to detect malicious vehicles based on the blockchain technology. This framework utilizes the advancements and advantages of the blockchain technology which includes the distributed nature, and the ability to reach consensus on one common ledger between all nodes within the network. Our framework is based on vehicles communicating their blockchains to each other. This blockchain will be based on environmental information and the validation of the data between the vehicles. This framework manages to detect malicious nodes by the adjacent vehicles, hence, reduces the cost of a centralized approach. We discuss the possible attacks by the malicious nodes and how our proposed framework addresses them.

References

[1] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, “Towards software-defined vanet: Architecture and services,” in *Proc. 13th Annual Mediterranean Ad Hoc Networking Workshop*, 2014, pp. 103–110.

[2] N. Radziwill, “Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world,” *Quality Management Journal*, vol. 25, no. 1, pp. 64–65, 2018.

[3] I. Bentov, A. Gabizon, and A. Mizrahi, “Cryptocurrencies without proof of work,” in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 142–157.

[4] M. S. A. Walid and A. A. Mostafa, “Malnod: Malicous node discovery in internet-of-things through fingerprints,” in *Proc. European Conference on Electrical Engineering and Computer Science*, Bern, Switzerland, 2017.

[5] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in vanets,” in *Proc. 1st ACM International Workshop on Vehicular Ad Hoc Networks*, New York, NY, USA: ACM, 2004, pp. 29–37.

[6] V. L. Praba and A. Ranichitra, “Isolating malicious vehicles and avoiding collision between vehicles in vanet,” in *Proc. International Conference on Communication and Signal Processing*, April 2013, pp. 811–815.

[7] J. Rezgui and C. Doucet, “Detection of malicious vehicles with demerit and reward level system,” in *Proc. International Symposium on Networks, Computers and Communications*, May 2017, pp. 1–6.

[8] J. Rezgui and S. Cherkaoui, “Detecting faulty and malicious vehicles using rule-based communications data mining,” in *Proc. IEEE 36th Conference on Local Computer Networks*, 2011, pp. 827–834.

[9] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in *Proc. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2017, pp. 618–623.

[11] P. Memarmoshrefi and D. Hogrefe, “Self-managed and blockchain-based vehicular ad-hoc networks,” in *Proc. ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, New York, NY, USA: ACM, 2016, pp. 137–140.

[12] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” in *Proc. Second International Conference on Internet-of-Things Design and Implementation*, New York, NY, USA: ACM, 2017, pp. 173–178.

[13] M. Singh and S. Kim, “Trust Bit: Reward-based intelligent vehicle commination using blockchain paper,” in *Proc. IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 62-67.

[14] X. D. Zhang, R. Li, and B. Cui, “A security architecture of VANET based on blockchain and mobile edge computing,” pp. 258-259, 2018.

[15] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, “A privacy-preserving trust model based on blockchain for VANETs,” *IEEE Access*, vol. 6, pp. 45655-45664, 2018.

[16] A. Kchaou, R. Abassi, and S. Guemara, “Toward a distributed trust management scheme for VANET,” in *Proc. 13th International Conference on Availability, Reliability and Security*, 2018.

[17] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmuller, “Secure and efficient beaconing for vehicular networks,” in *Proc. Fifth ACM International Workshop on VehiculAr Inter-NETworking*, 2008, pp. 82–83.

[18] P. K. Sharma, S. Y. Moon, and J. H. Park, “Block-vn: A distributed blockchain based vehicular network architecture in smart city,” *JIPS*, vol. 13, no. 1, pp. 184–195, 2017.

[19] M. Bernard. (2017) Bitcoin’s hot but blockchain for cleantech is interesting. [Online]. Available: https://cleantechnica.com/2017/12/12/bitcoins-hot-blockchain-cleantech-interesting/

[20] J. D. Bruce. (2014). The mini-blockchain scheme. [Online]. Available: http://www.cryptonite. info/files/mbc-scheme-rev2.pdf

[21] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs,” in *Proc. 1st ACM International Workshop on Vehicular ad Hoc Networks*, October 2004, pp. 29-37.

[22] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, “A distributed advanced analytical trust model for VANETs,” in *Proc. IEEE Global Communications Conference*, December 2012, pp. 201-206.

[23] F. Picconi, N. Ravi, M. Gruteser, and L. Iftode, “Probabilistic validation of aggregated data in vehicular ad-hoc networks,” in *Proc. 3rd International Workshop on Vehicular Ad Hoc Networks*, September 2006, pp. 76-85.

[24] A. Walid, A. Mostafa, and M. Salama, “MalNoD: Malicous Node Discovery in Internet-of-Things through Fingerprints,” in *Proc. European Conference on Electrical Engineering and Computer Science (EECS)*, Bern, 2017, pp. 280-285.