Towards a Blockchain and Software-Defined Vehicular Networks approaches to secure Vehicular Social Network

Youcef Yahiatene
LIMOSE Laboratory, Computer Science department
Faculty of Sciences ,
University MHamed Bougara Boumerdes
Independency Avenue, 35000 Algeria
yahiatene.y@univ-boumerdes.dz

Abderrezak Rachedi
Gaspard Monge Computer Science
Laboratory (LIGM - UMR 8049),
University Paris Est Marne-la-Vallee,
75420 Champs sur Marne, France
rachedi@u-pem.fr

***Abstract*—In this paper, we propose a new framework based on two main concepts: Software-Defined Vehicular Networks (SDVN) and Blockchain to efficiently manage and secure Vehicular Social Network (VSN). Using SDVN makes the network programmable, virtualized, and partitionable, but also it creates a well-known vulnerability named single-point of failure. Hence we propose to introduce a Blockchain paradigm that enables to certify the transactions and provide anonymity of data in distributed way using miners nodes. To this end, we introduce three levels of controllers: Principal controller (PC), Road Side Units (RSU) and miners. The PC has a global overview of the network like network topology. The RSU is an intermediate between the PC and the miners. We select local controllers acting as miners due to safety and performance. In order to select miners, we propose a Distributed Miners Connected Dominating Set algorithm (DM-CDS). The DM-CDS is a distributed algorithm with a single phase that supports dynamic topology. The selection of miners is based on a function called *miner-score* which depends on trust parameter particularly *trust metric* and network parameters such as: the connectivity degree, the average link quality indicator and the rank. The performance of the proposed DM-CDS is evaluated using many scenarios with different parameters like trust metric, node density, node mobility and radio range. The obtained results show the importance of the proposed architecture in terms of number of miners (CDS size) and robustness with different scenarios.**

***Index Terms*—Vehicular Social Networks, Software-Defined Vehicular Networks (SDVN), Distributed Connected Dominating Set (CDS), Blockchain, Miners selection, Trust model.**

I. Introduction

Vehicular Social Networks (VSN) is an emerging concept of communication, which uses two kinds of networks: Vehicular Network and Mobile Social Network (MSN). Thanks to vehicles mobility that positively impact the spacio-temporal data collection process. The social dimension is mainly based on the interaction between different nodes that have similar or close interests like facing traffic condition on the same shared route (path) [1]. The VSN supports diverse kinds of applications which are not only limited to intelligent transportation services (ITS) like traffic management and road safety, but also other services related to sharing data (videos, audios, roads photos, air quality, and so on) [1]. However, these applications require efficient security services such as: confidentiality, integrity, and authentication [2]. The existing security services cannot be directly introduced in VSN because of VSN characteristics. For instance, vehicles cannot have a permanent access to the infrastructure due to mobility of vehicles. That's why, we think that Blockchain approach can contribute to face this issue.

Blockchain is a new way to decentralize the trust-third-party by-passing the classical centralized approach. The problem of this approach is mainly related to trustworthy relationship between vehicles and their connectivity to the infrastructure. The vehicles need to reach the infrastructure whatever their mobility is which is not the case in VSN where vehicles have an intermittent access to security services (located in the infrastructure). Trusting vehicles without going through the infrastructure is critical, hence we propose to use a Blockchain. It makes possible to store and transmit information transparently, securely and without a central control point. Moreover, Blockchain based network is promising solution in privacy preserving in terms of anonymity and integrity of data in VSN.

The aim of this paper consist in proposing a new architecture that enables to select vehicles in VSN to act as *miners*. The role of miners is to secure and certify the transaction and the data exchange between vehicles without using centralized approach. We propose a semi-distributed approach based on Software-Defined Vehicular Networks (SDVN) [3]. Using SDVN makes the network programmable, virtualized, and partitionable. We introduce three levels of controls such as: the Principal Control (PC), Road Side Units (RSU) and the local control called "miners". The PC has global overview of VSN architecture. The RSU is an intermediate controller between PC and the miners. Finally the miners are local controllers managing and relaying data from VSN nodes to the RSU. We propose a new Distributed Miners based on Connected Dominating Set (CDS) algorithms.

The main contributions are summarized as follows:

- A new architecture based on Software-Defined Vehicular

Network (SDVN) is proposed. It is based on three levels of controller such as: the Principal Controller (PC), Road Side Units (RSU) and miners.
- A Blockchain concept is used in order to introduce security services using distributed approach. We introduce a Distributed Miners Connected Dominating Set algorithm (DM-CDS) based on trust parameter called "trust metric", and network parameters such as: the connectivity degree, the average link quality indicator and the rank.
- Performance evaluation are conducted through simulation using different scenarios with several parameters including nodes density, radio range node mobility and trust metric.

The remainder of the paper is organized as follows: section II describes the background, in which we present the vehicular social networks and its architecture, an overview of a Blockchain and the Connected Dominating Sets (CDS) algorithms. Section III discusses the proposed framework based-on Blockchain architecture, its different modules and their interaction. Section IV we present the miners selection using CDS algorithms and their different phases. In section V is devoted to discuss and analyze the obtained simulation results, evaluate the performance of proposed DM-CDS. In section VI, we discuss the the security analysis of proposed architecture. The last section VII, we conclude the paper and gives future perspectives.

II. Background

This section presents an overview of VSN and a brief description of Blockchain paradigm. In addition, an introduction to Connected Dominating Sets (CDS) algorithms is presented and discussed.

A. Vehicular Social Networks

Vehicular Social Networks (VSN) are composed of set of vehicles equipped with On-Board Unit (OBU), and Road Side Units (RSU) deployed on roads infrastructure. Different kinds of communication can be distinguished (V2X) which represents Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) [4]. These type of communications can use different technologies such as: 4G/5G, WLAN/WIFI, WIMAX and DSRC/WAVE [5]. Social networks allow users to communicate and share data without any limits, the integration of social network into the VSN provide new applications mainly related to safety and entertainment [6].

The major components of VSN are participants and network infrastructure. We distinguish different stakeholders: drivers, passengers, pedestrians, OBU and RSU. All these participants can take part in communication. Smarts devices integrated on vehicles, drivers and pedestrians can detect neighborhood and may share content like audios, videos and so on. The physical communication architecture of VSN depends on upon the network infrastructure centralized, distributed or hybrid [7].

B. Blockchain overview

The Blockchain is open and distributed ledger for cryptocurrency. It is used on Bitcoin launched in 2008 [8]. The idea of Blockchain is to maintain a distributed, authenticated and synchronized list of transactions. Nodes in the network use their processing power to validate transactions without any centralized administration. Once the block is validated, it will be added to the Blockchain and the transaction will be visible by the entire network

The decentralized character of the Blockchain, added to its security, transparency, anonymity and tractability, promises much broader applications than the monetary domain. The Blockchain is composed by a chain of transactional records, which a subset of the network called miners validate and record them on the global ledger. A block is a structure that contains transactions, which is mined by solving a difficult mathematical problem based on a cryptographic hash algorithm. We present in the next section Connected Dominating Sets (CDS) algorithms. This approach is used to select the subset of nodes that will act as miners. Many parameters are considered in the miners selection process such as : the connectivity degree, the average link quality indicator, the rank and the trust metric. To calculate the trust metric parameter, we integrate the distribute trust model introduced by [9].

C. Connected Dominating Sets (CDS) algorithms

A Connected Dominating Set (CDS) approach is part of graph theory. The CDS is subset of nodes named dominating nodes. This approach is widely used as a virtual backbone in mobile ad hoc network. It can be used into topology control [10], routing [11], broadcasting [12] and so on. It can be classified into two approaches: distributed and centralized. In centralized approach, the topology of network is considered as available, which is not the case with mobile wireless network where nodes' mobility makes the network topology dynamic. However, in the distributed approach, local network information is required and exchanged between nodes to make decision.

Many distributed algorithms for constructing the CDS have been proposed [13]. In this paper, we focus on a Distributed Single-Phase algorithm for constructing a Connected Dominating Set named DSP-CDS [13]. The DSP-CDS is appropriate for dynamic network typology. Each node uses neighborhood information and makes a local decision on whether to join the dominating set. In this paper, we use CDS algorithm to select miners nodes. We propose a Distributed Miner Connected Dominating set algorithm (DM-CDS). It will be detailed in the next section. The *miner-score* function is introduced with different network and security parameters.

III. Blockchain-based architecture

In this section, we investigate in detail the proposed architecture. The main idea consists in selecting some particularly nodes to acts as controllers [14], [15]. We have three control levels such as: Principal controller, Road Side Unit (RSU) and Miners as we can see in Figure 1.

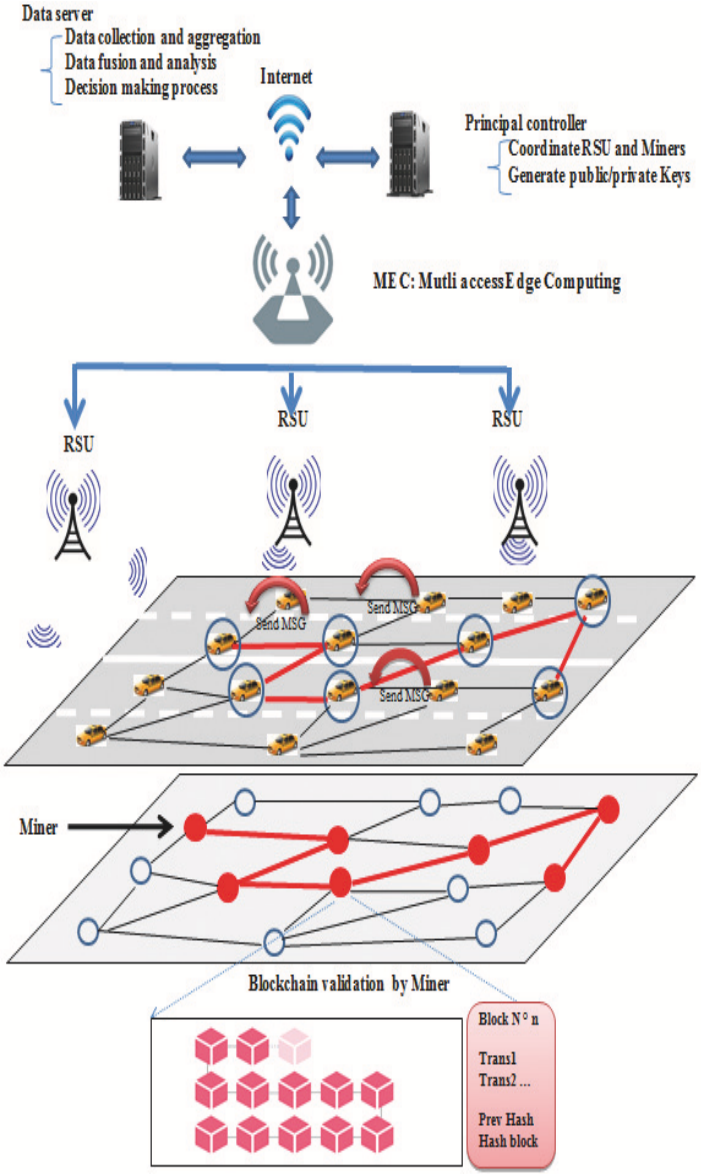

Fig. 1. A global view of the Architecture

A. The Control module

We classify the control module into three kinds of controllers: 1) the Principal Controller (PC), 2) Road Side Unit (RSU) and 3) the miners.

1) The Principal Controller: The PC is a centralized controller that is located at the first level of the architecture (as illustrated in Fig. 1). The PC has a global overview of the network in term of topology. The principal roles of the PC is illustrated as : coordinates the RSU and miners, configuration of the network, managing the different resources of the network. We consider that Key distribution is an important issue in VSN, so we assume that the key distribution is done through PC as we see in Figure 1

2) The Road Side Unit Controller : The RSU is a device located on the road which is connected to the infrastructure and Internet. The RSUs are acting as intermediate node between the PC and On-Board Unit (OBU). They are designed to manage a group of OBUs within their communication range. The RSU participate to select relevant OBU to act as miners. The selection process is based on the Connected Dominated Sets approach (CDS) and particularly a Distributed Miner Connected Dominating set algorithm (DM-CDS).

3) The Miners Controller : The miners are specific nodes of access network, their roles consist in validating and certificating transactions on Blockchain. The selection of miners as we see in Figure 1 is based on several parameters such as : connectivity degree, link quality indicator with their neighboring nodes, their position in the network topology and the trust metric. In the proposed solution, we use the Connected Dominating set (CDS) algorithm to select and the miners.

B. The Data module

The data module is represented by data server which is responsible for the management of data exchanged between VSN entities. The main role of data module is: data collection, data analysis and data management.

1) The Data collection and analysis: The Data collection and analysis represents a smart collection's techniques. They are used to extract relevant information from different entities on VSN, with network characteristics need to be considered: bandwidth, overhead, latency, and fault tolerance. In the proposed architecture, the data analysis selects the optimized techniques in terms of Quality of Services(QoS) and energy consumption.

C. Cloud Computing module

The cloud computing module can be used in the proposed architecture to offer different services to VSN entities, among these services we can quote software as a service (SaaS), which can be used by VSN entities such as passengers, drivers and so on. The cloud computing module can directly interact with the data collection and analysis by offering storage and computation services. It is used to reduce network congestion, and improve application performance by achieving related task processing closer to the user. Further, it aims to improve the delivery of content and applications to those users.

D. Security and privacy module

The security and privacy module is used to ensure and manage the main security services such as: confidentiality, integrity, authentication, availability and traceability. The proposed architecture considers dynamic security services which can be added or removed and customized according to the applications requirements. We introduce the Blockchain model to distribute the trust management [16]. In addition, this model enables to monitor and dynamically track the behaviors (selfish and malicious entities) of VSN' nodes. That's why the trust metric (Tm) is introduced in the miners selection process and to track and avoid the misbehaving nodes [17]. VSN nodes that have a low Trust metric ($Tm \leq$ threshold) will be exclude from the selection of miners.

IV. The Miners selection using CDS algorithms

The miners have an importance role in the Blockchain paradigm in terms of security, but also in the network performance like the network overhead related to validate transactions exchanged between VSN nodes. In this section, we detail the CDS algorithm to select subsets of VSN nodes that will act as miners. Moreover, we present the *miner-score* function to make the selection approach adaptable to different case.

We use the Distributed Single Phase (DSP) approach for CDS algorithm. This latter gives better performance in terms of delay and CDS size [13]. The algorithm starts by giving a white flags to all VSN nodes, after running the different phases of DSP-CDS, some nodes change their flags to black and act as dominating nodes. Only nodes with a black flags can act as miners. The proposed solution named Distributed Miners Connected Dominating set algorithm (DM-CDS) which is based on several network and security parameters such as: the trust metric, the connectivity degree, the average neighboring link quality indicator and the rank. In DM-CDS each VSN node has following characteristics: unique ID (**NodID**) and sub-set on connected VSN nodes (**SetID**). In addition, three flags **flags** are used to define VSN nodes status: **white** (non dominating node), **gray** (intermediate phase) and **black** (dominating node).

1) Network parameters assessment phase: In this phase, each node computes the needed network parameters: 1) **the connectivity degree**, this represents the number of direct connected neighbor; 2) **The average link quality indicator**, this represents the average link with VSN of node ; 3) **The Rank**: represents the distance in terms of hops number from the RSU. From the security point of view the trust parameter named 4) **Trust metric**: represents the degree of trust and honesty of VSN node. These four parameters are used as input for the "miner-score" function.

2) Competition and decision phase: In this phase, each VSN node computes its "miner-score" function to select nodes who will act as miners. We distinguish two nodes: sender and receiver that are running two algorithms *Algorithm_sender* and *Algorithm_receiver* respectively as illustrated below.

In the case of sender VSN node, once his "miner-score" is computed, this will be compared with non-black neighboring nodes. Then, the decision is made to keep or to change its flag color. If the flag color changes to black, then it broadcasts these parameters: **NodID, flag_color, SetID and miner_score**.

In the case of VSN receiver, after it receives packet from black node with greater **SetID**, then the VSN receiver updates its **SetID** to became in the same **sub-set**. However, in the case of the white receiver, it updates its **SetID** as we can see in (Algorithm_receiver) and updates his flag_color to gray.

Algorithm 1: Competition phase at VSN sender

Input : NodID, Score, SetID, neighbors(i),i
Output: Decision to change flag_color

N is the number of VSN entities
for *(VSN entity(i)*$\in N$) **do**
  miner_score(i)=computeScore();
  if $((Miner\_score(i) \neq 0) and (i.flag\_color \neq black))$ **then**
    for $(K \in non\_black\_neighbor)$ **do**
      $S = Max\_score(K)$
      if $miner\_score(i) > S$ **then**
        $i.falg\_color = black;$
        $i.SetID = i.NodID$;
        $Broadcast(i.SetID, i.NodID, miner\_score(i))$
      end
    end
  end
end

Algorithm 2: Competition phase at VSN receiver

Input : NodID, SetID, flag_color,j
Output: A connected dominated set with black flag

for *(VSN entity j receives packet from black entity i)* **do**
  if $((j.flag\_color = black) OR (j.flag\_color = gray)) AND (i.SetID > j.SetID)$ **then**
    $J.SetID = i.SetID$
  else
    if $(J.flag\_color = white)$ **then**
      $j.SetID = i.SetID;$
      $J.flag\_color = gray$
    end
  end
end

V. Performance analysis

In this section, we focus on the performance evaluation of the proposed DM-CDS algorithm with taking into account different performance metrics with several scenarios. We implement DM-CDS algorithm and we discuss the obtained results.

A. The simulation setup

All nodes are randomly deployed in a square length L varied from $40Km$ to $120Km$. The Range is varied between 10 to 20. The number of nodes (N) is given $N = L \times L \times \rho$, which ρ represent the node density. The simulations parameters are presented in table I. We consider the node density that determines the number of neighboring nodes. In addition, the node mobility is introduced to evaluate the impact on the stability, but also network connectivity and radio range are considered. Finally, in terms of security the trust metric is considered to evaluate its impact on the number of miners.

All the simulations carried out show the impact of trust metric, node mobility, radio range R and node density ρ parameters in the selection of miners nodes. The DM-CDS size represents the number of connected dominating nodes (miners). The connected miners are constructed by the Connected Dominating Set (CDS) in the network.

TABLE I
SUMMARY OF SIMULATION PARAMETERS OF DM_CDS

Network Scenario	Number of Node (N)	Node density ρ	Network Lenght	Radio Range (R)	Dynamic
S1	64 to 567	0.03	40 to 120	10	N.A
S2	64 to 567	0.04	40 to 120	10 to 20	Withdrawing
S3	64 to 567	0.05	40 to 120	10 to 20	joining
S4	64 to 567	0.06	40 to 120	10 to 20	Moving

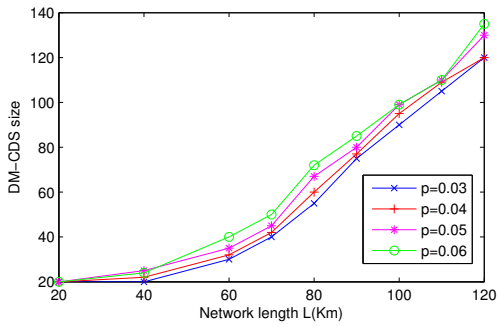

Fig. 2. Number of miners node according to node density

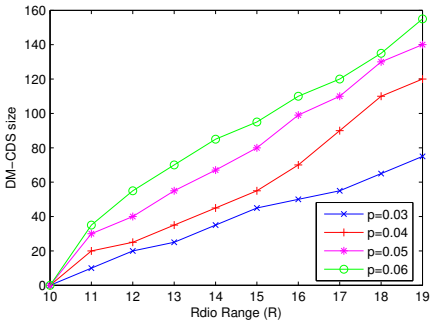

Fig. 3. Number of miners node according to Radio Range

B. The simulation results and analysis

In this subsection, we evaluate the performance of our proposed architecture through different simulation results.

The impact of the node density: Figure 2 shows the impact of node density and network length on the selection process of miners nodes (DM-CDS size). As discussed above, the selection strategy is based on Rank, link quality index (LQI) and connectivity degree (Deg). Nodes with low LQI are not considered in the selection process. From figure 2 we remark that nodes density and network length impact the number of selected miners. When nodes density increases that means that the number of neighboring nodes increases the number of selected miners increases too. We remark the same impact when the network length increase. The increasing number of the miners nodes are mainly due the important number of nodes that will participate in the competition phase.

The impact of the radio range: Figure 3 illustrates the number of selected miners according to different radio range with several nodes density. We remark that the radio range has an important impact on the miners nodes selection process. When the radio range increases, the connectivity degree (Deg) parameter will be higher due to neighboring nodes density and then the number of selected miners increases too. In addition, when nodes density increases the number of miners nodes increases too till a certain limit because of the LQI parameter. In the DM-CDS algorithm when the average link quality index (LQI) of candidate node is poor then this node is excluded from the competition phase.

The impact of the node mobility: The mobility impact is simulated based on link stability which is represented by two main parameters: withdrawing and joining. Figure 4 shows the number of selected connected miners nodes according to the network length and the link stability in terms of link withdrawing percentage. We remark that when the percentage of node withdraw randomly the network is varied from 0 to 10% the number of selected miners is stable (the variation is small).

Figure 5 illustrates the impact of joining nodes (link creation) on the number of selected connected miners. We remark that the impact is limited on the number of selected connected miners when the joining nodes is lower than 10%. From Figures 4 and 5, we conclude that in the case of low nodes movement the impact on the number of connected miners is limited. This prove that DM-CDS algorithm support low mobility of nodes.

The impact of trust metric: Figure 6 shows the impact of the trust metric (Tm) variation on the number of connected miners. We remark that the trust metric has an important impact on the selection of miners nodes. When the trust metric increases that means that nodes have higher trust level (more confident and trusted nodes exist in VSN), the number of connected miners nodes increases too. In the case of nodes with lower trust metric $(Tm = 0)$, the number of connected miners is zero. We remark that for the performance of DM-CDS, there is a difference of 40% of miners generated in the network with the variation of trust metric (20% and 60%), due to the impact of Tm on the DM-CDS algorithm.

VI. SECURITY ANALYSIS

In this section, we focus on the security analysis of our proposed solution and we discuss important security properties of our architecture.

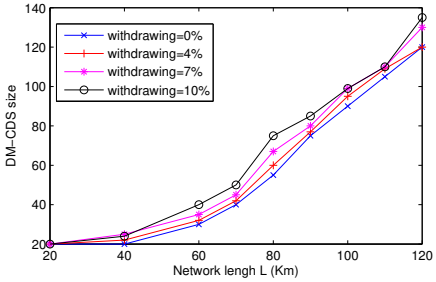

Fig. 4. Number of miners node according to withdrawing

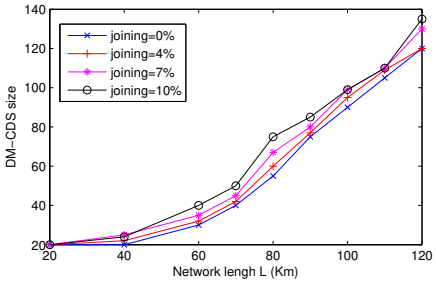

Fig. 5. Number of miners node according to joining

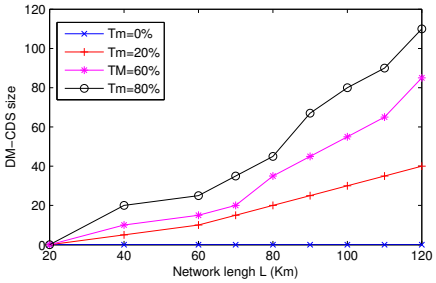

Fig. 6. Number of miners node according trust metric

A. Attacks resistance

In this subsection, we present attacks resistance of the proposed architecture. We discuss two kind of security issues: distributed trust model/metric and threats of leaking privacy in VSN. In the case of leaking privacy in VSN, we classify the attacks into three categories as illustrated in Figure 7, including 1) identity-based attack,2) eavesdropping attack and 3) service based attack

1) Distributed trust metric: The purpose of trust model is to establish a valid and truthful links between miners nodes. We use the model proposed by [9] to update and to track the trust metric. We assume that each VSN node is equipped with a Trust Platform Module (TPM), which is a hardware device proposed by TPM group [18], and used in [19]. TPM performs cryptography capabilities, combined with Blockchain while being tamper-proof. The proposed architecture is semi-distributed, so when VSN nodes communicate with each others (V2V mode). The trust model is used to enhance the integrity of data exchanged using Blockchain. This latter allow us to protect personal data with guarantee of [20]:

- the anonymity of data exchanged between VSN nodes. In a Blockchain the sender and receiver address are replaced by an hash.
- the integrity is ensured by using a cryptographic hash. All exchanged data is signed using a private key before sending.
- the tracking (monitoring) the malicious nodes and misbehaving nodes.
- the transparency: all nodes network exchanges are cleared in the Blockchain.
- no risk of fraud, when a Blockchain is exchanged, it can not be canceled by the sender
- filtered out VSN nodes with lower trust metric ($Tm = 0$).

2) Identity based attack: The attacks in this categorize are related to manipulate user's identity. Among these attacks we can quote: the sybil attack, impersonation attack, revealing and theft attacks.

A) Sybil attack: During the sybil attack, attacker tries to bypasses the reputation system, he creates a large amount of identities and using them to have an influence in the network. The purpose of the attacker is to be a destination of messages in the network. In our proposed architecture, the sybil attack can not happen, due to using signature of messages before sending them. If an attacker wants to alter or falsify messages in the network, he will be detected and excluded from the network.

B) Impersonation attack: This kind of attack, an adversary node tries to record identity of victims during registration process. Which can be used later by an attacker in order to realize other type of attacks such as identity theft attack [21] and identity revealing attack. As the sybil attack, these attacks can not happen in our solution, due to using signature of messages before sending them, identity of source and destination nodes are replaced by an hash using a Blockchain.

3) Eavesdropping based attack: This kind of attacks is based on eavesdropping the network communication, among theses attacks we quote: eavesdropping attack and hole attack

A) Eavesdropping attack: It happens when malicious node try to attain transmission exchanged between nodes in the VSN. After that it tries to perform attacks such as: modification attack, forgery attack, packet analysis attack. In our proposed scheme, the modification attack or forgery attack can not happen, due to using the Blockchain, all exchanges between nodes are signed before sending them. So modification is not permitted. Also malicious node, which tries the forgery attack, it can be tracked and blacklisted in the network with our trust metric.

B) Hole attack: This attack is mainly based on three techniques: worm hole attack, gray attack and black hole attack. In worm hole attack a node creates a fake routes. This attack is detected in our scheme using the two-hop" intermediates nodes. Black hole attack is a type of denial of service attack, which redirects packets to an non existent node in the network and that node drops the entire packet. Some nodes drop packets selectively, this attack is called Gray hole. Our approach is used to detect and avoid the hole attack, we use the ACK messages and exclude nodes if they misbehave.

4) Service based attack: This kind of attacks is based on: spam attack and denial of service attack, aiming to make a service unavailable.

A) Spam attack: This kind of attack used to disrupt data in the network and to spy the storage of VSN entities. Using the ACK messages in our scheme to calculate satisfaction and exclude nodes if they misbehave.

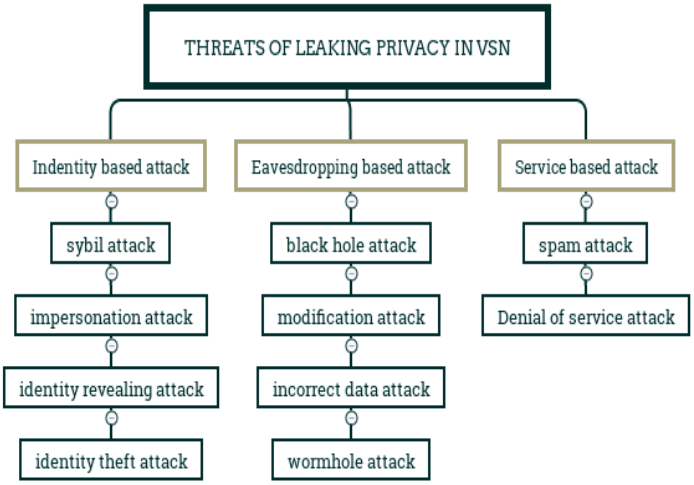

Fig. 7. Classification of attack of leaking privacy in VSN

B) Denial of service attack: The purpose of this attack is to put a service unavailable during communication. As an example: injecting packets to saturate bandwidth, disruption of delivering process and so on. In our proposed architecture, the denial of service attack can not happen. Introducing packets in the purpose to disrupt routing process and to saturate bandwidth, we calculate the trust metric to detect a node misbehavior, if that is the case, the node will be blacklisted. Despite these robustness. Our architecture suffer from some weakness, which can be quoted:

- the application of this architecture is not possible when the number of VSN entities is limited.
- when the infrastructure is not present, we can not select miners, the selection of miners is based on Principal Controller (PC) and the Road Side Unit (RSU).
- the trust metric is very selective, when the $tm = 0$, this means that the network is compound of malicious nodes. So the selection of miners are not possible.

VII. Conclusion

In this paper, we propose a new architecture based on two approaches: Software-Defined Vehicular Networks (SDVN) and the Blockchain for Vehicular Social Network (VSN). Regarding the Blockchain, the connected miners nodes selection algorithm based on Connected Dominating Set approach is proposed. In terms of SDVN approach, we introduce three levels of controllers: Principal, Road Side Unite (RSU) and miner (local controller). The idea is to distribute some functions of the controller and make the services closer to the vehicles. To this purpose we propose a new algorithm named DM-CDS. DM-CDS uses network and security parameters combined on one function called *miner-score* to select miners nodes. This function depends on several parameters such as: The connectivity degree, the link quality indicator, trust metric and the rank which is the distance in terms of hops from the road side unit. In order to evaluate our proposed architecture and DM-CDS algorithm, we conduct different simulation scenarios. The obtained results show the importance of the proposed model and its sensitivity and reactivity to the different network parameters and trust metric. As future works, we plan to consider other mobility models and to experiment our framework with a real test-bed platform.

References

[1] F. Xia, L. Liu, J. Li, J. Ma, A. V. Vasilakos, Socially aware networking: A survey, IEEE Systems Journal 9 (3) (2015) 904–921.
[2] A. Rachedi, A. Hasnaoui, Advanced quality of services with security integration in wireless sensor networks, Wireless Communications and Mobile Computing 15 (6) (2015) 1106–1116.
[3] A. Akhunzada, M. K. Khan, Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues, IEEE Communications Magazine 55 (7) (2017) 110–118.
[4] M. A. Ferrag, L. Maglaras, A. Ahmim, Privacy-preserving schemes for ad hoc social networks: A survey, IEEE Communications Surveys & Tutorials 19 (4) (2017) 3015–3045.
[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, Journal of network and computer applications 37 (2014) 380–392.
[6] A. M. Vegni, V. Loscri, A survey on vehicular social networks, IEEE Communications Surveys & Tutorials 17 (4) (2015) 2397–2419.
[7] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, S. K. Das, Vehicular social networks: A survey, Pervasive and Mobile Computing 43 (2018) 96–113.
[8] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf.
[9] N. Haddadou, A. Rachedi, Y. Ghamri-Doudane, A job market signaling scheme for incentive and trust management in vehicular ad hoc networks, IEEE transactions on vehicular technology 64 (8) (2015) 3657–3674.
[10] K. Mnif, B. Rong, M. Kadoch, Virtual backbone based on mcds for topology control in wireless ad hoc networks, in: Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, ACM, 2005, pp. 230–233.
[11] J. Wu, H. Li, On calculating connected dominating set for efficient routing in ad hoc wireless networks, in: Proceedings of the 3rd international workshop on Discrete algorithms and methods for mobile computing and communications, ACM, 1999, pp. 7–14.
[12] I. Stojmenovic, M. Seddigh, J. Zunic, Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks, IEEE Transactions on parallel and distributed systems 13 (1) (2002) 14–25.
[13] B. Yin, H. Shi, Y. Shang, An efficient algorithm for constructing a connected dominating set in mobile ad hoc networks, Journal of Parallel and Distributed Computing 71 (1) (2011) 27–39.
[14] D. Bendouda, A. Rachedi, H. Haffaf, Programmable architecture based on software defined network for internet of things: Connected dominated sets approach, Future Generation Computer Systems 80 (2018) 188–197.
[15] D. Bendouda, A. Rachedi, H. Haffaf, An hybrid and proactive architecture based on sdn for internet of things, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International, IEEE, 2017, pp. 951–956.
[16] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet of Things Journal 4 (6) (2017) 1832–1843.
[17] T. Gazdar, A. Benslimane, A. Rachedi, A. Belghith, A trust-based architecture for managing certificates in vehicular ad hoc networks, in: Communications and Information Technology (ICCIT), 2012 International Conference on, IEEE, 2012, pp. 180–185.
[18] T. Main, Part 2 tpm structures, Specification version 1.
[19] G. Guette, O. Heen, A tpm-based architecture for improved security and anonymity in vehicular ad hoc networks, in: Vehicular Networking Conference (VNC), 2009 IEEE, IEEE, 2009, pp. 1–7.
[20] M. Swan, Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc.", 2015.
[21] B.-Z. He, C.-M. Chen, Y.-P. Su, H.-M. Sun, A defence scheme against identity theft attack based on multiple social networks, Expert Systems with Applications 41 (5) (2014) 2345–2352.