ISSN 2319 – 7595
Volume 7, No.2, March - April 2018
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs01722018.pdf
https://doi.org/10.30534/ijiscs/2018/01722018

BlockChain for Improved Platoon Security

Henry Hexmoor, Suray Alsamaraee, Maha Almaghshi
Southern Illinois University
Carbondale, IL 62903, USA,
{hexmoor@cs, suray.alsamaraee@, mahaalmaghshi@}.siu.edu

ABSTRACT

This paper proposes a novel adaptation of blockchain technology to information exchanges among vehicles traveling in a platoon. The aim is to protect platoon member privacy and security while providing a rapid sharing of telemetry data. We have identified key protocols for a distributed cryptographic authentication among vehicles in transit within a platoon. This work heralds consideration of cyber-attack types on platoons and our proposed remedies.

Key words: Bloch chain, Cryptography, Vehicle Platoons

1. INTRODUCTION

Elsewhere, we have discussed several benefits of vehicular platooning [4] but the obvious security concerns remain. Recently, Blockchain has been shown to provide security and privacy for networked vehicles [1]. We consider application of distributed cryptographic blockchain to vehicular platoons. The most salient concern is privately sharing telemetry data among platoon members discussed in section 2 during initial platoon formation as well as during platooning. We present interactions using transaction blocks and authentication using cryptographic verification. In order to facilitate cryptographic certificate authority, we have envisaged an ad hoc dedicated communication cloud we have dubbed *platoon cloud*. We continue our presentation of communication protocols with possible attacks in section 3. A few open problems are highlighted in section 4. Section 5 concludes our paper.

2. INFORMATION SHARING

To maintain the initial platoon formation, vehicles need to share their local speed for coordination. The platoon leader (PL) must convey its vehicle speed to alert platoon members (PMs) about the highest, safe speed for their road segment, which is also below the legal road speed limit. The PL speed may indirectly communicate congestion and driving status of the road ahead by sharing its speed. Lower reported PL speed may signal congestion or unfavorable road conditions ahead. Security concerns of vehicles in a platoon include privacy and integrity for the shared information. Communication makes the platoon prone to attacks from outsiders. A few common types of reported attacks are *man in the middle*, *denial of service*, and *collision induction* [2]. An attacker may send malicious control messages to its succeeding vehicles leading to crash with other PMs. The attack may also prevent admissions of newer members of the platoon or cause existing succeeding vehicles to separate from the rest of the platoon. Blockchain has been shown to provide security and privacy for networked vehicles [1]. A blockchain is a list of records considered as blocks that are linked together. By employing cryptographic methods on each block for converting ordinary plain text into unintelligible text and vice-versa, a more secure communication is achieved. Every block of the blockchain will contain cryptographic hash function for the former block as well as cryptographic hash function for the current data to be sent. Furthermore, blockchain is distributed over all PMs, making it difficult to change the original data for one of the blocks while keeping the series of blockchain logically consistent [6]. This work combines the distributed cryptography blockchain with formation intelligent vehicles platooning. Whereas sensors in the intelligent vehicle provide the current speed value for each vehicle in the platoon, cryptography of public key system is used to ensure the authenticity for the source of data and the hash function is used to ensure the integrity of data transmitting from alteration among the vehicles [2]. We envision communication to be facilitated largely using roadside units and ad hoc clouds [3] and [7]. Roadside road infrastructures such as vision or ultrasonic sensors can be deployed to enumerate vehicles when they first enter a monitored zone. Using such enumeration technique, vehicles will be assigned numbers based on their order of zone entrance. A patented multi-window vehicular monitoring system exists [5] that can be the method for our proposed enumeration technique. For brevity, we consider vehicles in a cloud sharing information using an ad hoc cloud, dubbed *platoon cloud* (*PC*). PC serves as the checkpoint for the uploaded data (i.e., *transaction*s) from vehicles before rebroadcasting it to all PMs. The PC centrally maintains all platoon data (including all reported speeds), services as well as policies for all platoons. Initial platoon formation is discussed in the following section.

2.1 Platoon Formation

Let us consider the earliest entrant vehicle to a zone (i.e., vehicle number one) to maintain a speed that is slightly below the speed limit. We will call this vehicle front vehicle (FV) who is also a PL. This is in contract to rear vehicles (RVs). When the RV is in the sensory range of the FV, the RV requests FV for its public Key (PK). Then the RV will request

the PC to check whether the PK of FV already exists in PC database as a PM.

If PC confirm the PK already exists, PC will add the PK for RV to the platoon that already exists as well unicasts the specific *cloud public key* (CPK) for the platoon to the RV. This is shown in Figure 1. Once the RV receives CPK from the PC, it considers itself as a newly minted PM and will be

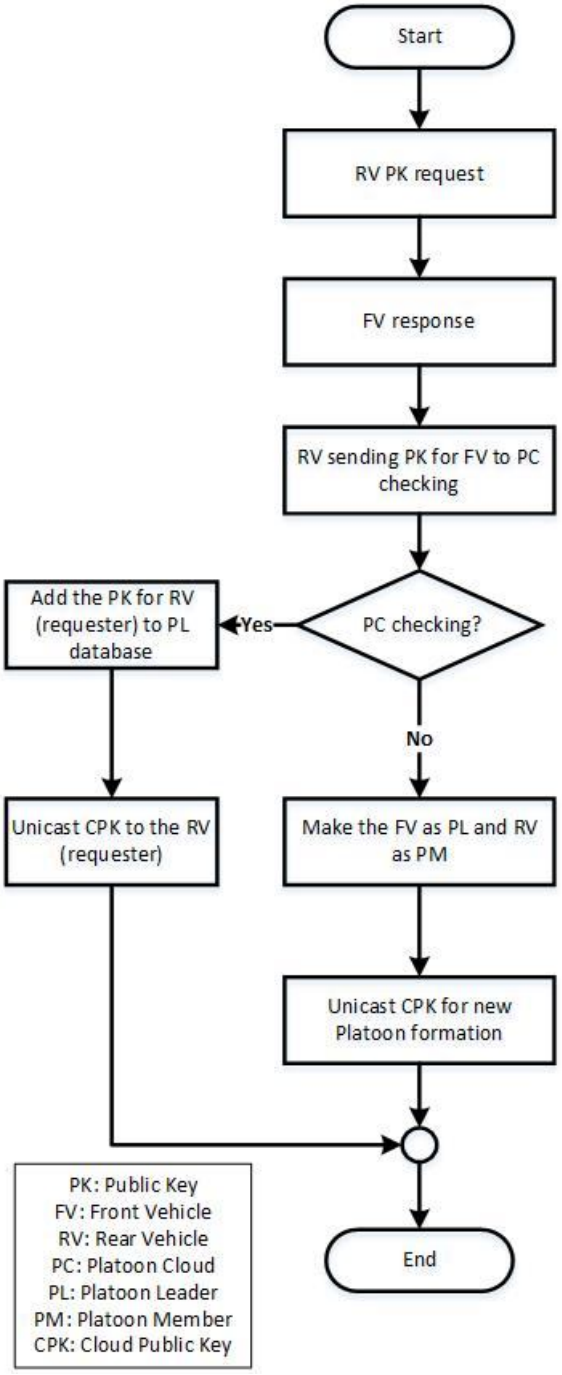

Figure 1 Platoon formation

able to receive the PC information broadcast henceforth. On the other hand, if the reported PK did not exist, the PC will initiate a new platoon identity by assigning the FV as a PL and the RV as a PM. PC will create a new and unique CPK for the newly formed platoon as well unicast the CPK to the new PL and its PM. Since it is likely that a PC will manage or terminate many platoons simultaneously, it is very important to track platoons with specific and unique CPK. This strategy preserves vehicle privacy as well as overall platoon privacy.

To attain confidentiality and integrity, we assume that all exchanged data among vehicles use the shared secret key as well the public key cryptography. The next section outlines transaction blocks as the foundation of blockchain.

2.2 Structure of Transactions

We sketch the structure of transactions in block chain shown in Figure 2. In each transaction block of the transaction chain, the first component of the transaction contains the hash value equal to the previous transaction's hash signature. Transaction data is the second component the third component is a unique has signature for the block to be used in the next block.

The first part of each transaction will contain the value of the hash for the previous transaction. The first part of a

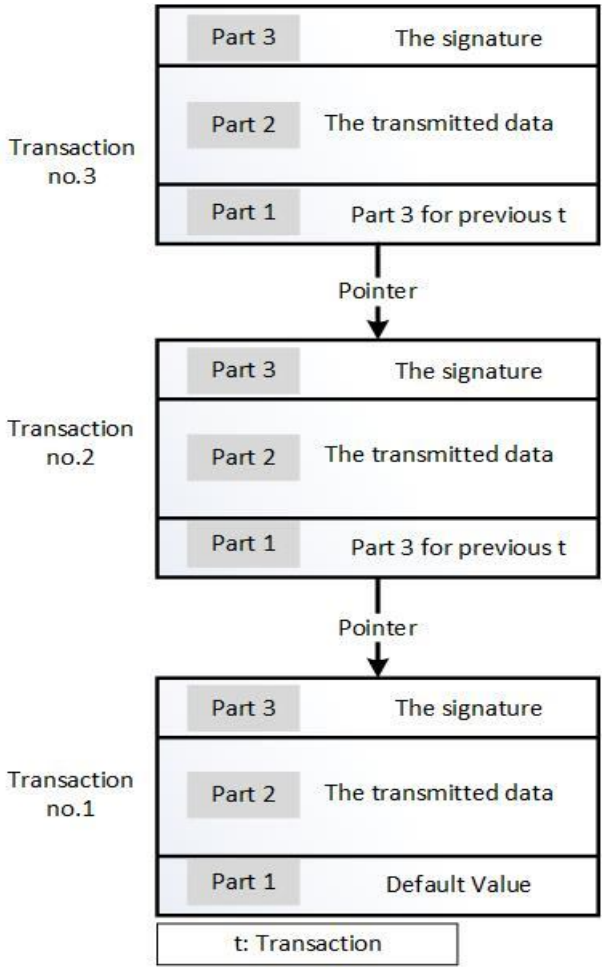

Figure 2. Block-Chain Structure

transaction services as a pointer to a previous transaction. The second part of the transaction maintains the data (i.e., speed information). The last part of the transaction keeps the signature for the first and the second part of the transaction. In other words, the idea of blockchain cryptography is the basic role that we have adopted [1].

To recapitulate, each vehicle is equipped with a wireless vehicle interface (WVI) and local storage, such as a micro SD card. The WVI connects the vehicle to the platoon overlay. The in- vehicle storage is used to store privacy sensitive data, e.g. location and maintenance history, to protect the privacy of the user.

During ordinary highway driving that are characterized by speeds in 40-75 mph, inefficiencies arise from frequent speed changes. This is mitigated by platooning reduces speed fluctuations. Maintaining a narrow speed range among vehicles in a vector of vehicles has a natural, physical limit, which can be experimentally discovered that we leave to future work. Platoons as a vector of vehicles must also adhere to this physical limit. For simplicity, we consider the set of vehicles upon initial platoon formation as the *platoon leader package* (PLP). Our platoon formation protocol does not limit the platoon size and a platoon can be far larger than size of the PLP. We make an observation that vehicles in PLP benefit from that narrow speed differences. Vehicles farther out would maintain speed differences that are larger than in PLP. To the proportion, that speed range differs is inversely related to platooning efficiencies. Exploring platoon efficiencies is postponed to our future work.

Returning to our description of the vehicle information sharing protocol, each vehicle in a PLP generates single signature transactions in pre-defined time intervals containing the signed hash value of the data stored in the in-vehicle storage. This transaction is sent to the PC that the vehicle is associated with and thus stored in the BC. Later, the vehicle can prove that the data within its storage has not changed by verifying the hash contained in this transaction. Since in-vehicle storage has limited capacity, a transaction back up is stored in the ad hoc PC. The vehicle periodically transfers data from the in-vehicle storage to the PC. In this instance, the hash of the backup storage is stored in the BC. Overlay transactions are broadcast and verified by the PL. A PL verifies a transaction by validating the signature of the transaction participants with their PK. In the following section, we describe information authentication.

2.3 Authentication and integrity of transaction

Transactions are validated using an algorithm shown in Figure 3a. PL sensors will be sensing the speed and dynamically record it in the local vehicle memory. Therefore, PL speed information is ready for use within the platoon. PL will be switched to the *listening mode* with respect to PC. Periodically, the PC will seek to collect the speed information

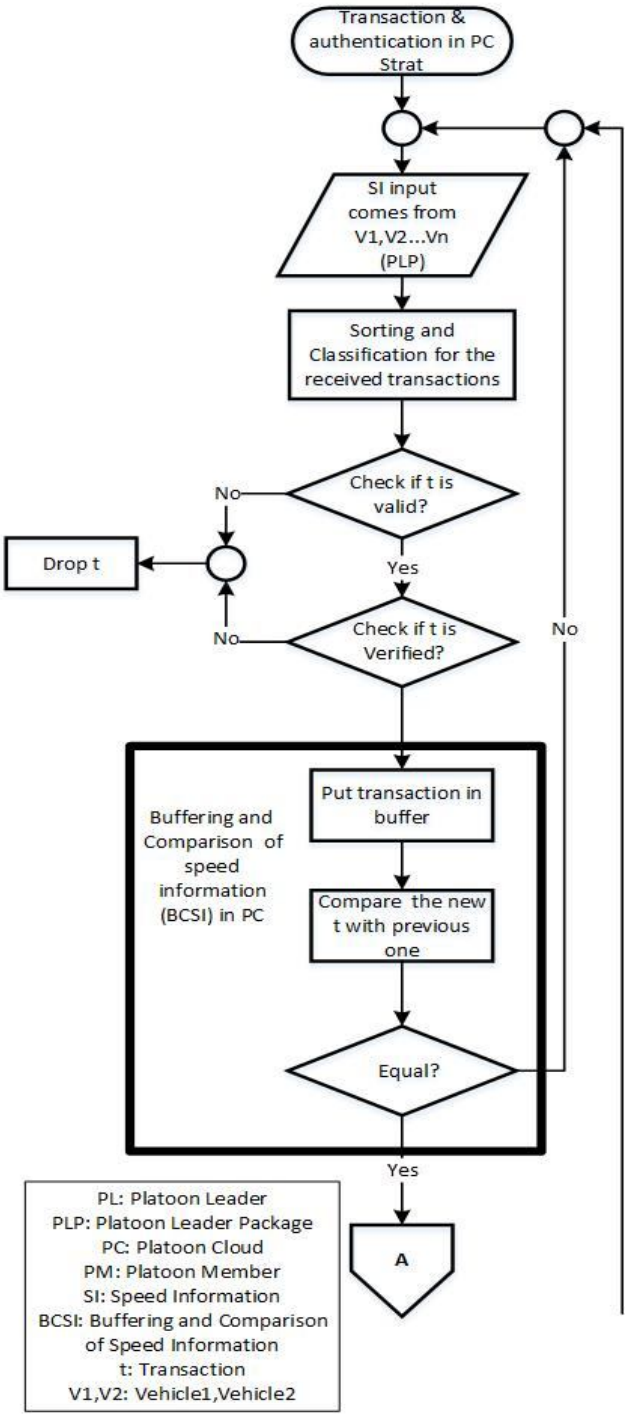

Figure 3a. Authentication and Integrity

transaction from PL; therefore, PC will request PL for its speed status. Then, PL will send the transaction of speed information to PC. Once the transaction is received by the PC, it will be checked in two parts. The algorithm will sort and classify the received transaction. The received transaction will already be appended with PK of the PM vehicle that transmitted the transaction. The component labeled *sorting and classification function* will match the PK with the one PC already holds in its database of platoon formation. The task of *sorting and classification* function is very important for

avoiding the overlap in the received transaction. Therefore, the transaction will be prepared for the next step of the two-part algorithm outlined next.

In the first stage, PC will check whether the transaction sequence is valid. While the new transaction is downloading in the PC buffer, the PC has already maintained the former transaction. The PC will be able to check whether the first part of the new transaction has the same hash value as the third component of the previous transaction Therefore, PC will be able to check whether the first part of the new transaction has the same hash value for the second and the last part of the previous transaction. In case that the result of checking is positive, i.e., the new transaction is deemed correct in sequence at that time, the algorithm will allow the moving transaction to the next checking which is called signature checking step [1]. Otherwise, the transaction will be ignored by the PC. In the signature checking step, the PC will compare the hash value that is calculated from the first and second part of an incoming transaction with its signature. If the outcome comparison was equal, the algorithm will leave the transaction proceeding to next step, which is labeled the *Buffering and Comparison of Speed Information* in the Platoon Cloud abbreviated as BCSI. BCSI consists of two portions. The first portion is the buffering that will take care of storing the incoming transaction one by one, which has the speed information. The second portion of BCSI will compare the data of speed information that is already stored with the transaction. The comparison process starts in BCSI once the buffering portion has received the transaction. By assuming the incoming transaction is the first one, the comparison will be with a default value such as zero. This is because there are no previous transactions stored in buffering to compare with. In this case, certainly, the result of the comparison will be negative, which leads to the next step of the algorithm shown in Figure 3b.

In the next step, the PC will request to get speed status from the second vehicle in the PLP. All previous steps will repeat until the transaction of the second PLP reaches the buffering portion of BCSI. At that time, the comparison portion will match the new transaction with the previous one. In the case that the match result is negative, PC will do another request to the third vehicle in PLP and so on. In contrast, when the result of match is positive, then the algorithm will add one credit to the credibility of PL. Alongside this action, the algorithm verifies whether the value of credit equal to PLP size (say 10). In case credibility is not equal to PLP size (say 10), the PC will do another request to the next vehicle in the PLP; else, the algorithm will perform two functions. In the first function, PC will broadcast the first transaction of PL to the entire PM community as well as add the transaction to the pool, which is a buffer for counting and collecting. The pool will keep counting the incoming transactions until its equal to pool size's parameter [1]. Until then, the algorithm will do two functions. The first one, PC will form a block then broadcast the block itself to all PM. Finally, the PC will store the block in block-chain memory as a documentation or history for Platoon formation.

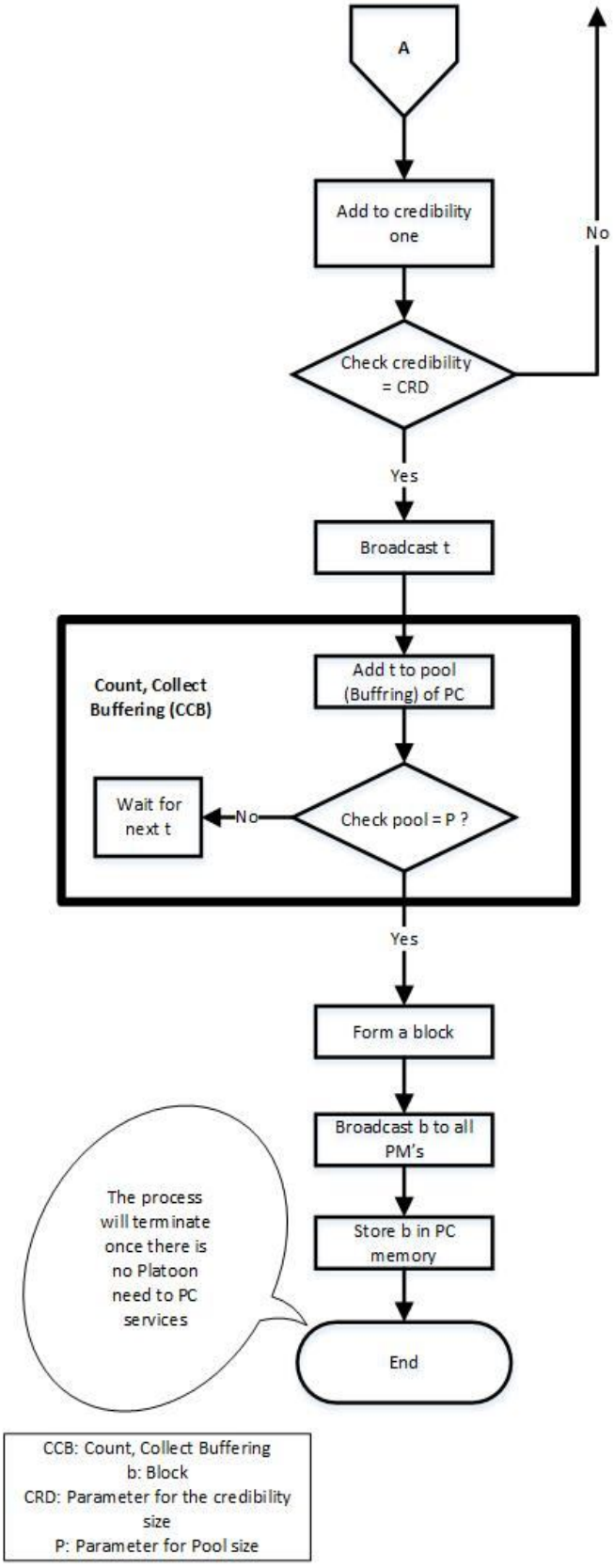

Figure 3b. Authentication and Integrity

Figure 4 illustrate the continual interaction between the PC and vehicles in a platoon using the platoon cloud. In the following section, we discuss a few possible attack types. This is followed up with concluding remarks and plans or future work.

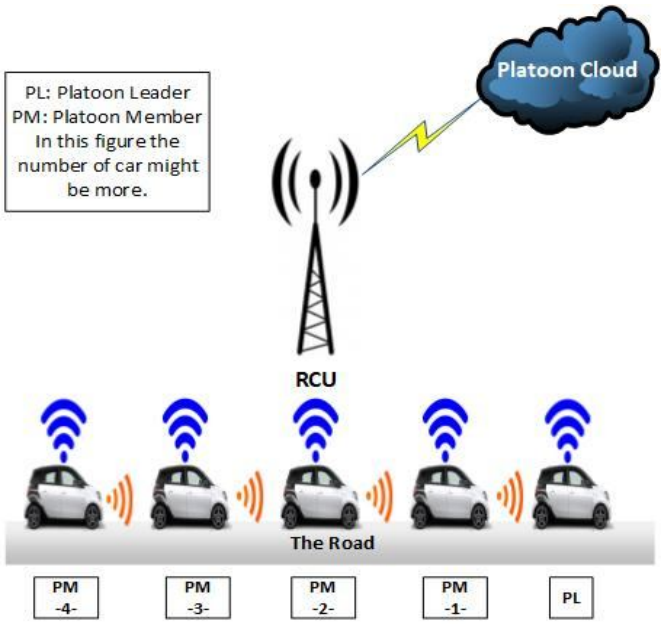

Figure 4. Continual Interaction

3. ATTACK SCENARIOS

There are many possible security attack types. Sudden, outsider attacks are averted using our distributed cryptographic approach. However, an attacker might become a PL for an extended period where it is not detected as malicious. This is a possible attack when an attack vehicle attempts to assume the role of a PL and nefariously divert traffic. Once such an impersonator is trusted, it might engage is attack behavior. As such the infected platoon might join a larger platoon that contains the attacker vehicle shown in Figure 5.

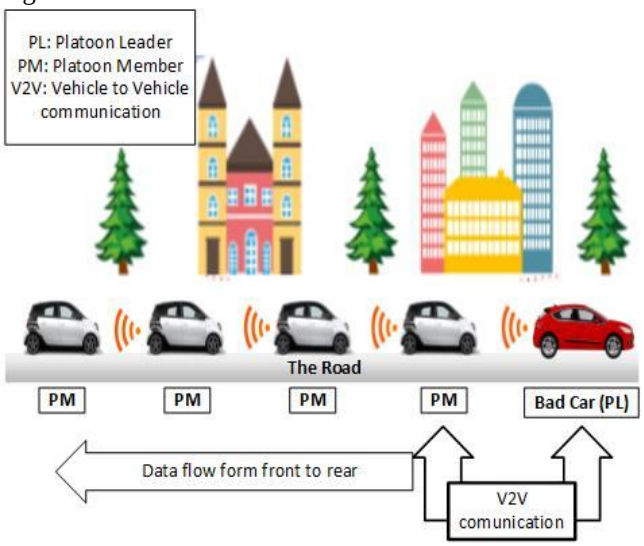

Figure 5. A default platoon attacked by a fake PL

Another attack shown in Figure 6 might be perpetrated by a vehicle who has become a PM in a platoon and may engage in *jamming* to disrupt normal communication or alter its speed to cause disruption in platooning.

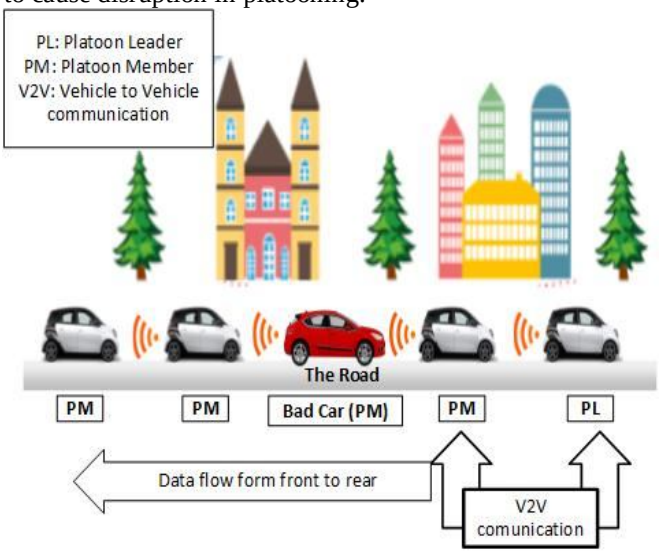

Figure 6. A default platoon attacked by a PM

4. LIMITATION FUTURE WORK

Figure 7 depicts another attack scenario. Two adjacent vehicles might simultaneously request the FV for the PK during the time of platoon formation. The RV will ask PC to proceed with platoon formation. The PC will process the request by adding the PK for RVs to the database of platoon even if one of these vehicles is on the adjacent lane. We will leave the remaining security concerns and analysis for future work. We also plan to explore efficiency of platooning for vehicles joining a platoon. Our hypothesis is that vehicles near the PL will experience the least benefit. Furthermore, vehicles in PLP will experience more platooning benefits than the PMs farther out from the PL. Opportunities to exit a

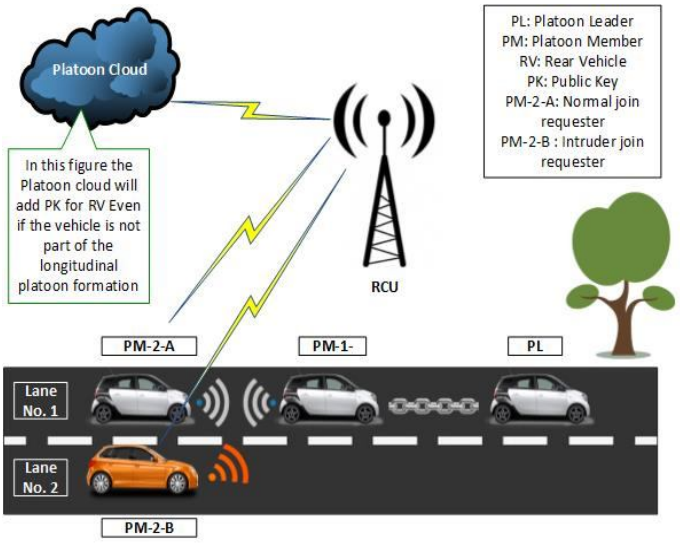

Figure7. Platoon Cloud Confusion

platoon due to inefficiencies are proportional to delayed information transmission from the PL, which is proportional to a PM's position in the platoon vector. Analysis of such concerns will be explored in the future.

REFERENCES

1. A. Dorri, S. A. Kanhere, R. Jurdak, and P. Gauravaram. **BlockChain: A Distributed Solution to Automotive Security and Privacy**, IEEE Communications Magazine, Vol. 55, No. 12, pp. 119-125, IEEE press, 2017.
2. J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague. **Convoy: physical context verification for vehicle platoon admission**, In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, pp. 73-78, ACM.press, February 2017. https://doi.org/10.1145/3032970.3032987
3. H. Hexmoor and B. Gupta. **Policies Guiding Cohesive Interaction among Internet of Things with Communication Clouds and Social Networks**, In the Second IEEE international Workshop on Communication, Computing, and Networking in Cyber Physical Systems, pp. 32-36, ICDCS-2017, IEEE press, 2017.
4. H. Hexmoor and K. Yelasani., **Economized Sensor Data Processing with Vehicle Platooning**, In 20th International Conference on Web Intelligence, World Academy of Science, Engineering, and Technology Press, 2018.
5. S. H. Li. **U.S. Patent No. 6,989,739**, Washington, DC: U.S. Patent and Trademark Office, 2006.
6. M. Singh and S. Kim. **Blockchain Based Intelligent Vehicle Data Sharing Framework**, in Computing Research Repository, 2017.
7. D. Singh, M. Singh, I. Singh, and H. Lee. **Secure and reliable cloud networks for smart transportation services**, 17th International Conference on Advanced Communication Technology (ICACT), pp. 358-362, 2015. https://doi.org/10.1109/ICACT.2015.7224819