An Efficient Blockchain Authentication Scheme for Vehicular Ad-Hoc Networks

Matthew Wagner, Bruce Mcmillin

Chapter 1

EFFICIENT BLOCKCHAIN AUTHENTICATION SCHEME FOR VANETS

Matthew Wagner and Bruce McMillin

Abstract As the use of autonomous vehicles increase, the transportation infrastructure as a whole becomes more susceptible to cyber-attacks due to the increase of components that can communicate with one another and the Internet. It has been shown that autonomous vehicles benefit greatly from cooperating to perform many cost and life-saving applications such as tailgating, advanced collision warning, and even traffic routing. To secure the transportation infrastructure against this increasing risk, this paper presents an efficient blockchain scheme for vehicular ad-hoc networks of autonomous vehicles. In the proposed scheme, every vehicle maintains blocks generated by its platoon which contain transactions that evaluate the actions of every vehicle. Thus, vehicles will possess different blocks and thus different blockchains as they join and leave platoons. No central blockchain is maintained. These blocks are used as a token by the vehicle to gain access to future platoons. The proposed scheme uses the Schnorr digital signature scheme to create a secure signature and reach consensus within the platoon. It is proven to be secure under the given assumptions.

Keywords: blockchain, cyber-physical systems, physically verifiable, distributed systems, vehicular ad hoc network, Schnorr digital signature

1. Introduction

Critical infrastructures include telecommunications, electrical power systems, gas and oil systems, banking and finance, water supply systems, emergency services, and transportation systems [7]. These systems are essential for everyday living. In recent years, they have become targets for cyber-attacks [13]. Currently, these attacks have been limited to systems with large cyber-component or central control systems such as the supervisory control and data acquisition systems that manage electrical

power systems. However, it is only a matter of time before these attacks expand to other critical infrastructures including those proposed to manage national transportation systems.

With autonomous vehicles on the rise, national transportation systems are primed to become a key target for cyber-attackers. This becomes increasingly true with the large push for vehicular ad-hoc networks (VANETs) which help increase efficiency in our national transportation system resulting in large cost savings. The savings from enabling VANETs are calculated by the United States Department of Transportation (USDOT) to be approximately $202 billion from crash-prevention alone [15]. This does not include the savings in fuel efficiency from the large scale deployment of tailgating maneuvers or traffic rerouting applications. Unfortunately, the proposed architecture for VANETs is estimated to cost $2.5 trillion initially with approximately $121.5 billion per year in maintenance costs to build that required infrastructure [12]. Thus, a solution to securing our national transportation systems without the added cost is needed.

This paper proposes a method for securing autonomous transportation systems without the need for the infrastructure of a typical VANET. In the proposed scheme, blockchain technology is leverage for its useful properties including immutability, verifiability, non-repudiation, and ability to reach a consensus in a distributed system.

This paper continues as follows. Section 1.2 presents background information need for this work. Section 1.3 steps through the proposed architecture and the primary differences between it and previous architectures. Section 1.4 presents a security proof of the proposed system. Section 1.5 presents work related to this research area. Finally, section 1.6 concludes and addresses future research areas.

2. Background

This paper proposes a solution to secure a minimal-infrastructure VANET using a distributed blockchain. Additionally, it uses Multiple Security Domain Nondeducibility (MSDND) to prove that the proposed cyber-physical blockchain is secure compared to other versions of blockchains. Thus, a brief explanation of VANETs, blockchains, digital signatures, and MSDND is provided.

2.1 VANETs

A VANET is a set of vehicles that communicate with one another and cooperate for some specific purpose, such as to perform a driving-base application like tailgating [3]. In this work, it is assumed that the

VANET consists of autonomous vehicles that possess the ability to monitor the actions of one another via sensor readings. Additionally, it is assumed that each autonomous vehicle has a secure GPS that is used to navigate and synchronize the processor of all vehicles in a platoon. The architecture of VANETs has typically consisted of an infrastructure made of many road-side units (RSUs), some centralized authority (CA), and vehicles driving around on the roadways. RSUs act as interaction points between the CA and the vehicles which allow for high-speed verification of messages, identities, and even information. RSUs are estimated to cost $\$51,600$ each and are required to cover all roadways [15]. Due to this cost, a VANET architecture without them is used in this work. Additionally, the only time the CA is involved in the proposed system is when a vehicle is initially registering to participate in the VANET.

In VANETs, vehicles travel in groups, called platoons. Platoons generally have a leader which is tasked with issuing commands to and managing the platoon. This paper proposes a solution to securing platoons and the entire VANET during joining, leaving, and other platoon operations.

2.2 Blockchains

A blockchain is a state agreement mechanism that allows a distributed, untrusted network to reach consensus and create a computationally immutable ledger. Blockchains consist of basic components such as a consensus mechanism, a digital signature scheme, transactions, blocks, and a network. Transactions are the raw data that is stored in the blockchain and are signed by the participants using a digital signature scheme to ensure non-repudiation and immutability. There must be some verification mechanism to ensure the veracity of the data within each transaction. A consensus mechanism is used to create blocks that signify the ordering of transactions. The consensus mechanism should be hard or impossible to replicate by a single participant, resulting in an immutable ordering of events. Blockchains have currently seen use in a wide variety of cryptocurrencies and many other applications. However, there exist four main issues with applying this technology to VANETs that are solved by this work: cyber-only transactions, a system-wide ledger in a disconnected network, real-time transaction requirements, and no registration for participants [11].

2.3 Digital Signatures

In the proposed scheme, both asymmetric digital signatures and multi-digital signatures schemes are used. An asymmetric digital signature

scheme is a scheme where there exist some public and private key owned by a signer. The signer can sign a message using their private key that can be verified using their public key. The proposed protocols do not specify an asymmetric digital signature scheme.

To generalize how these schemes work, the digital signature scheme has some key generation function, signing function, and verification function. The key generation function is: $(Key_{Public}, Key_{Private}) \leftarrow KeyGen(X)$ where Key_{Public} is the public key, $Key_{Private}$ is the private key, and $KeyGen(X)$ is the key generation algorithm given some set of inputs X. The signing function is $M' \leftarrow Sign(Key_{Private}, M)$ where M' is the signed messaged and $Sign(Key_{Private}, M)$ is the signature creation function given an input private key $Key_{Private}$ and a message M. The verification function is $Output \leftarrow Verify(Key_{Public}, M')$ where $Output$ is either accept or reject and the verification algorithm $Verify(Key_{Public}, M')$ with and input key Key_{Public} and signed message M'.

A multi-digital signature scheme is a protocol that allows a group of signers to produce a short, joint signature on some common message. This message can be verified using the group public key that is generated when signing the message [6]. This paper uses Schnorr multi-signature. An adaptation of the scheme is presented in section 1.3 as part of the proposed protocols.

2.4 MSDND

MSDND is a method created for evaluating the information flow across an architecture to formally analyze the trust in cyber-physical systems using modal logic [4]. The formal definition of MSDND is given below.

$$\begin{gathered}\text{MSDND(ES): } \exists w \in W \vdash [(s_x \vee s_y)] \wedge \sim (s_x \wedge s_y) \\ \wedge [w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))]\end{gathered}$$

This can be simplified to the following definition based on basic Boolean logic and the definition of exclusive-or.

$$\begin{gathered}\text{MSDND(ES): } \exists w \in W \vdash [(s_x \oplus s_y)] \\ \wedge [w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))]\end{gathered}$$

It is important to note that if a system or information flow path is MSDND secure, then it is vulnerable to a Stuxnet-like attack in a model that is trying to maintain high integrity. However, if it is MSDND secure, then the architecture is secure under a privacy model.

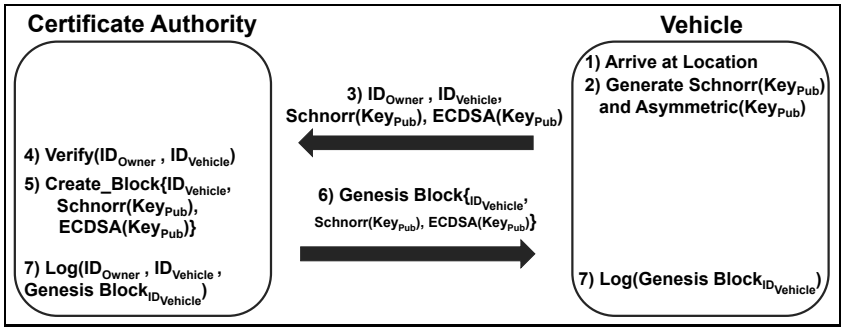

Figure 1. Vehicle Registration Protocol

MSDND proofs are presented in section 1.4 to show the security of the proposed schemes. They are used to show that a cyber-only or physical-only blockchain are insecure in the face of these attacks and that the cyber-physical blockchain presented in the paper is secure to the same attacks.

3. Proposed Scheme

This section presents the protocols used by participants in the VANET. In particular, vehicle registration, platoon join, block creation, intra platoon communication, and platoon leave protocols are presented. The only protocol where the CA or any infrastructure component is present is the vehicle registration protocol.

3.1 Vehicle Registration Protocol

The proposed system uses private blockchains. This means that all users must be registered with a CA to participate. The CA is charged with inspecting the vehicle, requesting any fees or taxes, and creating a certification for the vehicle. This certification allows the vehicle to begin participating in the VANET and take advantage of the cost-saving opportunities it provides and can be considered the genesis block of the vehicle's blockchain. The Vehicle Registration Protocol is outlined in figure 1.

Once this protocol is complete, the vehicle is free to join its first platoon and benefit from the cost-saving applications of the VANET. It will not need to register again unless it gets kicked out of the platoon for possessing a "bad" block.

In the proposed system, a "good" block simply denotes a vehicle that has behaved correctly while a "bad" block indicates a vehicle that has not. The definition of correctness is explained in section 1.4.

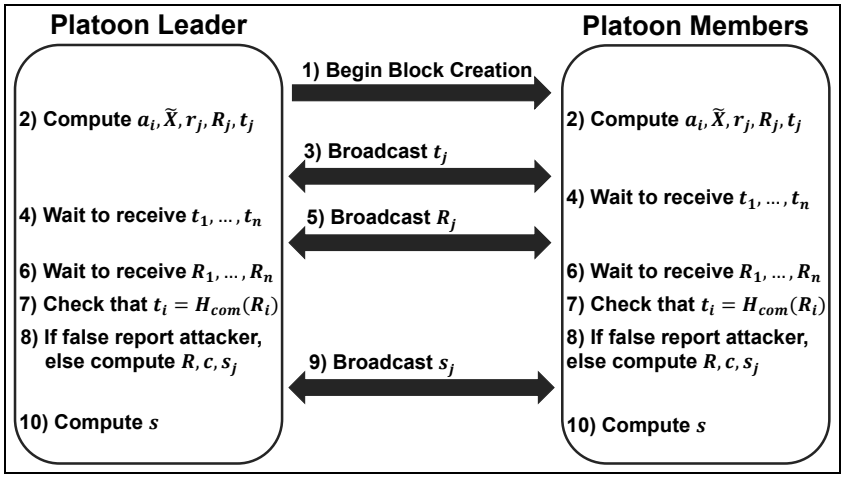

Figure 2. Block Creation Protocol

3.2 Block Creation Protocol

Blocks are generated whenever there is a change in state of the platoon. This protocol is adapted from the Schnorr Multi-Signature scheme and applied to a platoon. It must be carried out and a platoon signature created for a vehicle when they want to leave the platoon to be allowed to join another platoon. If a vehicle does not possess a valid block when they leave, they will not be able to join any future platoons. The block generated by the protocol serves as certification showing that the vehicle behaved correctly while a part of the platoon according to all cyber and physical actions performed by the vehicle. An outline of the protocol is seen in figure 2 and works as follows.

1 The platoon leader indicates to the platoon that they will begin the block creation protocol via broadcasting a signed message.

2 For $i \in 1, ..., n$, every vehicle in the platoon then computes $a_i = H_{agg}(L, X_i)$. The aggregated public key for the platoon is then $\tilde{X} = \prod_{i=1}^{n} X_i^{a_1}$. Each platoon member also generates a random $r_j \leftarrow \mathbb{Z}_p$, computes $R_j = g^{r_j}$, and $t_j = H_{com}(R_j)$.

3 Each platoon member broadcasts t_j to all other members of the platoon.

4 The platoon waits until it receives all t from every platoon member.

5 Once every platoon member gets $t_2, ..., t_n$ from the other platoon members, it broadcasts R_j to the entire platoon.

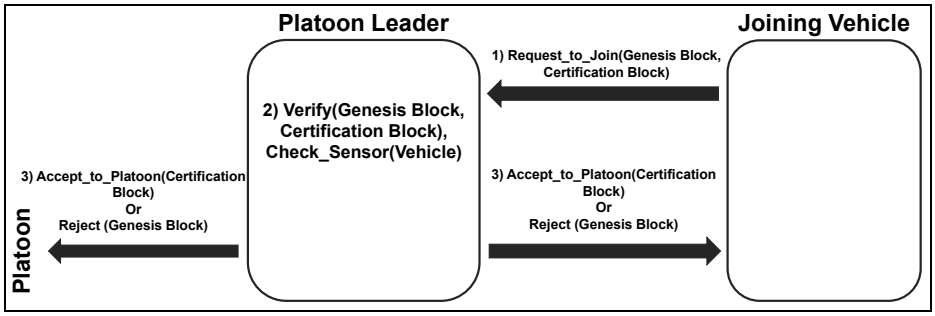

Figure 3. Platoon Join Protocol

6 The platoon waits until it receives all R from every platoon member.

7 Once it gets $R_2, ..., R_n$ it checks that $t_i = H_{com}(R_i)$ for all $i \in 2, ..., n$.

8 If it is not true, the platoon aborts the computation and creates a transaction evaluating the faulty vehicle. Otherwise, every vehicle in the platoon computes $R = \prod_{i=1}^{n} R_i$, $c = H_{sig}(\tilde{X}, R, m)$,, $s_j = r_j + ca_j x_j modp$.

9 Every vehicle in the platoon sends s_1 to all other platoon members.

10 Once the all vehicles in the platoon receive $s_2, ...s_n$ from the platoon members, it computes $s = \sum_{i=1}^{n} s_1 modp$ and the signature for the message is $\sigma = (R, s)$.

To ensure that consensus on the values broadcast at steps 3, 5, and 9, Algorithm 2 is applied from [2] which is used to reach consensus in the face of Byzantine faults under partially synchronous communication and synchronous processors when authentication is present. In the proposed protocol, the digital signature is used when sending messages. Additionally, a secure GPS is located within each car that is used for navigation. It is used to synchronize the processors of all the vehicles in the platoon.

3.3 Platoon Join Protocol

Whenever a vehicle attempts to join a platoon, its last certification block must be verified by the platoon it is attempting to join. When a vehicle joins a platoon, its secure GPS reports the total distance it has traveled. The platoon is trusting that the previous platoon behaved correctly and gave the vehicle the appropriate designation of "good" or "bad". The correctness of this assumption is proven in section 1.4. To understand how this protocol works, an outline is given in figure 3.

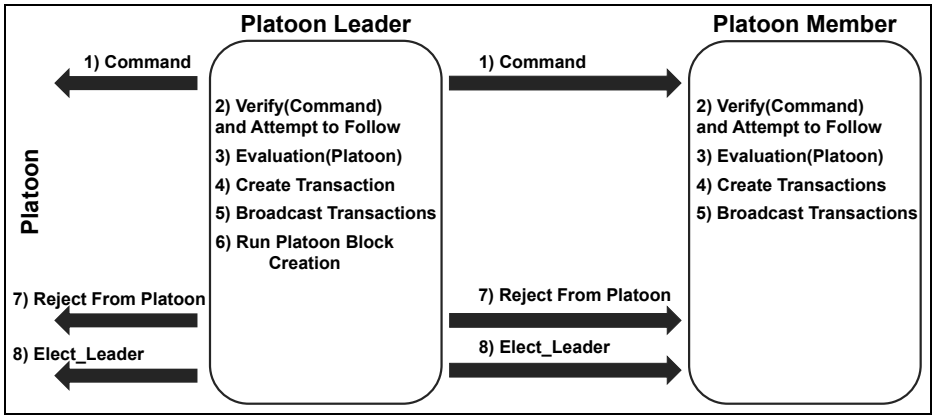

Figure 4. Intra Platoon Communication Protocol

3.4 Intra Platoon Communication Protocol

Every time a command is issued by the platoon leader, this protocol is run to disseminate transactions and detect faults by vehicles within the platoon. A brief outline of this protocol is given in figure 4 and described below.

1 The platoon leader issuing a command to the platoon.

2 Every vehicle within the platoon then receives the command, verifies that it is from the platoon leader, and attempts to follow the command assuming that the result will not end in a bad state.

3 As the platoon members are following the command, they monitor one another according to the invariants of the system. Once the platoon maneuver is complete, every vehicle creates transactions for every other vehicle in the platoon.

4 Every vehicle in the platoon broadcasts its transactions to the other vehicles within the platoon.

5 The platoon will run the block creation protocol to reach consensus on the actions of the vehicles within the platoon.

6 If any vehicles behaved inappropriately during the maneuver, they are deemed untrustworthy and kicked from the platoon.

7 If the platoon leader is kicked, a new platoon leader is elected from the remaining vehicles.

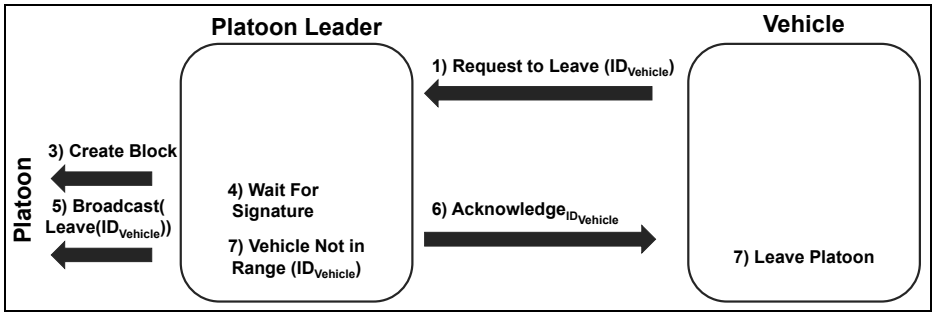

Figure 5. Platoon Leave Protocol

3.5 Platoon Leave Protocol

To leave the platoon, a vehicle must receive a certification block from the platoon. Otherwise, it will not be allowed to join any future platoons. A brief description of this protocol can be seen is figure 5. Once the vehicle leaves the platoon, it will use the last signed leave-platoon request to join the next platoon.

4. Security Proof

To formally prove the security of the proposed scheme, several different theorems about this work are proven. First, a list of seven different assumptions that are assumed in the model are given. After those are presented, some basic definitions of proposed system are laid-out. Lastly, several theorems that show the strength of the protocols are proven.

Assumption 1. *The CA that generates the certificates for the vehicles is a trusted entity and will not reveal any information about a vehicle* $\boldsymbol{V}$ *to an attacker* $\boldsymbol{A}$*.*

Assumption 2. *A vehicle* $\boldsymbol{V}$ *will not reveal its private signing information.*

Assumption 3. *There are a limited number of attackers* $\boldsymbol{A}$ *where* $A < 3N + 1$*. N is the number of vehicles in a platoon. This assumption is based on previous work discussing the maximum number of attackers to reach consensus under partial synchronicity in the face of the byzantine faults with authentication.*

Assumption 4. *There is a tamper proof GPS.*

Assumption 5. *There is a bounded distance D_B that a vehicle can drive without receiving a new certification block before it will no longer be allowed to join a platoon.*

Assumption 6. *A vehicle* ***V*** *can only be a part of one platoon at a time.*

Assumption 7. *For every action that is in the blockchain, there must be a certifiable action, either cyber or physical, that is evaluated by the platoon.*

Throughout this section, correctness refers to a vehicle's actions both in the cyber and physical domains of the vehicle. This paper's description of correctness follows directly from Assumption 7.

Definition 1. A vehicle is behaving correctly if it passes the evaluation and certification of its actions by other vehicles within the platoon that will be stored in its blockchain.

The description of correctness is purposefully left vague to avoid requiring in-depth and lengthy proofs. Based on the aforementioned assumptions, the proposed scheme can be described with the following definitions. The description of a platoon in a VANET, the requirements to join a platoon is given, and the result of leaving a platoon is given.

Definition 2. Platoon **P** is a group of **N** vehicles that drive in the proximity of one another and cooperate for some particular application where **N** is bounded. The vehicles within the platoon carry out the proposed communication protocols as needed when vehicles join or leave and whenever a physical action is carried out by the platoon.

Definition 3. To join platoon **P**, vehicle **V** must possess a valid certification block C_V, be moving in the same direction as the platoon, and by physically sensible by the platoon.

Definition 4. Whenever a vehicle **V** leaves platoon **P**, it will receive a valid certification block C_V that will denote whether it is behaving correctly based on definition 1.

Now that the proposed scheme and protocols have been defined in terms of the system and the base assumptions of the been discussed, the security proof begins by proving several base theorems about the proposed system.

Theorem 4.1. *A vehicle* ***V*** *can only be a part of one block creation event at a time.*

Proof. Theorem 4.1 is proven by contradiction. Assume that **V** created two blocks at the same time. Blocks are generated by joining a platoon and subsequently leaving the same platoon (definition 4) or by participating in a platoon maneuver as denoted in section 1.3. Thus, **V** would have had to join two platoons and participated in a maneuver within both or subsequently left both. To join a platoon, a vehicle must have a valid certification block that shows that they behave correctly and must be physically a part of that platoon (definition 3). Since **V** cannot be two places at once, it cannot be a part of two separate platoons. Thus, it cannot create two blocks during a single period and Theorem 1 is proven. □

Theorem 4.2. *A vehicle **V** will not be able to change the contents of their certification block C_V when they are not a part of a platoon.*

Proof. Theorem 4.2 is proven by contradiction. Assume that vehicle **V** was able to change their certification block C_V when they were not a part of a platoon. To change C_V two case could have happened. First, **V** could have reverted back to a previous certification block. Secondly, **V** could have changed the contents of C_V.

Case 1: Assume the first case where **V** reverted to a previous certification block. To begin, assume that **V** has traveled more than the bounded distance D_B since receiving the previous certification block. In this case, the certification block would contain GPS reading D_O. No GPSs can be falsified due to assumption 4. Given the current GPS reading D_C, $D_C - D_O > D_B$, thus it will not be able to join a platoon due to assumption 5

Secondly, assume that **V** has traveled less than D_B since receiving the previous certification block. Since it has traveled less than D_B, the vehicle has either not moved since leaving the last platoon or it could be moving. Given its current GPS reading D_C and the GPS reading contained within the certification block D_O that $D_C - D_O < D_B$. If it was not moving **V** would be unable to participate in a platoon since the traffic would be moving and a **V** is required to be moving with the platoon and be physically sensible by the platoon to join (definition 3). Thus, **V** would be unable to use C_V to participate in any platoon when it cannot join due to the physical constraints of the platoon-join requirements. Thus, **V** would be unable to use the previous certification block to participate due to assumption 5. If **V** was moving, then it will have a period before it travels D_B until the previous certification block is invalid. Thus, **V** will eventually be caught using a false certification block and not be allowed to join a platoon.

Case 2: Assume the second case where **V** changed the contents of C_V. If **V** changed the contents of C_V then **V** would have to possess the private signing information of all vehicles in the prior platoon that was used to create C_V or a fork was created in the platoon's blockchain. However, a vehicle will not reveal it's private signing information due to Assumption 2. Furthermore, it cannot create two blocks simultaneously due to Theorem 4.1. Thus, they could not have changed the contents of C_V.

Since **V** could not use a previous certification block and could not have changed the contents of C_V, there assumption that **V** was able to change their certification block C_V is incorrect. This proves theorem 4.2. □

Theorem 4.3. *A vehicle **V** will always have a valid certification block C_V whenever it attempts to join a platoon.*

Proof. Theorem 4.3 will be proven by induction. First, the proof begins with the base case. Let us prove that a vehicle **V** will have a valid certification block C_V when it attempts to join its first platoon, P_1. In this case, its last certification block will have been created by the CA. Due to Assumption 1, this certification block is valid. Additionally, based on Theorem 4.2, **V** was unable to change C_V. Since the vehicle has received a valid certification block from the CA and was unable to change it, **V** will join P_1 with a vehicle certification block. Thus, **V** will be allowed to join the platoon if C_V says **V** has behaved correctly or will be denied if it says **V** has behaved incorrectly.

Next, the inductive case is proven. Assume that **V** has a valid certification block C_V holds whenever **V** joined P_N. Let us prove that **V** has also has a valid certification block C_V when **V** tries to join P_{N+1}. Before **c**an join P_{N+1}, it must leave P_N due to theorem 4.1 and assumption 6. When **V** leaves the platoon P_N, it will create a secure certification block for **V**. If there are **X** vehicles in the platoon not including **V**, then it follows that there are only up to **Y** attackers where $Y < \frac{X}{3}$ based on assumption 3. In the block creation algorithm, vehicles exchange evaluations of other vehicles with one-another and the majority score for any vehicle is taken as the cumulative value. Thus, when the cumulative trust value for a vehicle is calculated, the output will follow the answer created by the honest portion of the platoon since the number of honest vehicle **H** since $H = X - Y$ thus $H >= \frac{2X}{3}$. This results in **V** receiving a valid certification block when they leave the platoon.

Due to theorem 4.2, **V** cannot alter C_V after it leaves P_N. Thus, **V** will use C_V to join P_N+1. When **V** attempts joining P_N+1 using C_V it

Table 1. Table of Symbols for MSDND Proof

Symbol	Definition
CP	The consensus protocol of the platoon
LB_2	The local blockchain of vehicle 2
VC_1/VC_2	The vehicle controller of vehicle 1 or vehicle 2 respectively
VO_2	The physical vehicle operations of vehicle 2
CC_1/CC_2	The cyber communications of vehicle 1 or vehicle 2 respectively
S_1	The sensor unit of vehicle 1
FP_2	The future platoon of vehicle 2

will be allowed to join the platoon if C_V says **V** has behaved correctly or will be denied if it says **V** has behaved incorrectly.

Since theorem 4.3 holds when **V** joins P1 and it was shown that if C_V is valid when **V** joins P_N then C_V will be valid when it attempts to join P_N+1, theorem 4.3 is proven. □

Theorem 4.4. *The "cyber-physical" blocks that are created in the form of certification blocks encapsulate both the cyber and physical domains.*

Proof. Theorem 4.4 is proven by contradiction. Assume that the certification blocks do not encapsulate both the cyber and physical domains. This means that it can either not encapsulate the cyber system or not encapsulate the physical system. assumption 7 says that for every transaction in the blockchain that evaluates a vehicle **V**, it will be the cyber representation of some action by **V**. These actions can fall into two categories: cyber and physical. Cyber actions are the actions that **V** takes as part of the system that does not result in direct physical action. This includes evaluating other vehicles, making actions of other vehicles, and simply replying to messages from the platoon within a specified time bound. Physical actions are any action that **V** takes that result in physical action by V. These include braking, accelerating, and turning. Thus, by assumption 7, the blockchain will include both cyber and physical actions since they are both verifiable actions. □

Now that some basic properties of the proposed protocol have been proven, some theorems describing the benefit of the proposed approach to evaluating both the physical and cyber portions of the system, instead of one or the other, are presented and proven. These proofs use MSDND to show the security of the approach. In MSDND, $IBT_{1,2}Val$ is a macro used to describe the information flow from one entity to another in a system model [9]. It means that entity 2 reported to entity 1 the value Val is true and entity 1 believes entity 2.

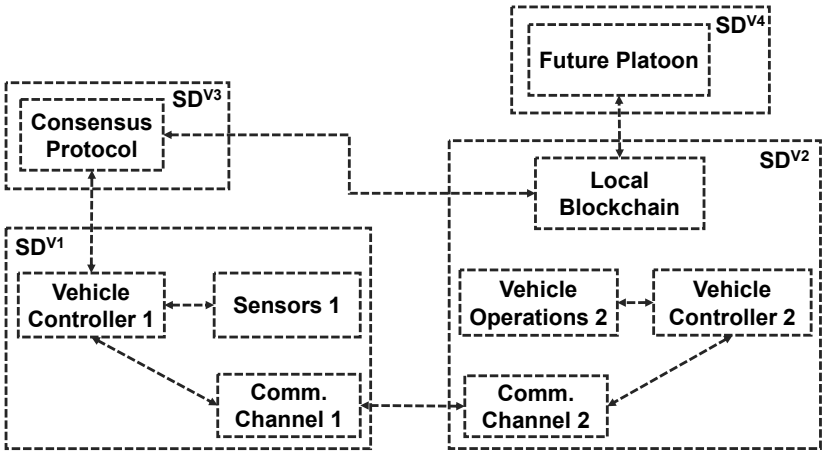

Figure 6. Cyber Only Blockchain Information Flow Diagram

In a physical-only blockchain, there is no information flow path from VO_2 to S_1 as seen in figure 6. A table of shorthand notations used for this and following proofs can be seen in table 1. Let φ_1 be the statement "Vehicle 2 is maneuvering correctly". Let φ_2 be the statement "Vehicle 2 is communicating correctly with other vehicles". The definition of correctness comes from definition 1. Either φ_1 or $\neg\varphi_1$ must be true at all times. Similarly, either φ_2 or $\neg\varphi_2$ must be true at all times. Finally, $\varphi = \varphi_1 \wedge \varphi_2$ means that the vehicle is behaving correctly. In this system, repeated evaluations of other vehicles that are noted in the local blockchain are used by future platoons to evaluate the trustworthiness of a vehicle. Thus, there is an information flow path from the consensus protocol of the platoon to the local blockchain of a vehicle and a path from the local blockchain of a vehicle to any future platoons of that vehicle.

Theorem 4.5. *A cyber-only blockchain is not MSDND secure under an attack on the cyber communications of a vehicle.*

Proof. Assume that in a cyber-only blockchain, some function f exists to determine whether φ_2 is true or false that is owned by CP. This follows from assumption 7. In the model, assume that CP will always be honest due to the bounded number of attackers in assumption 3.

1 $\neg\varphi_2 = true$; Vehicle 2 is not sending correct cyber communications.

2 $w \vDash V_{\varphi_2}^{VC_2}(w) = true$; VC_2 observes that they are communicating correctly.

3 $IBT_{CC_2,VC_2}\varphi_2$; VC_2 lies to CC_2 and tells it that the cyber communicating are correct.

4 $w \vDash V_{\varphi_2}^{CC_2}(w) = true$; CC_2 observes that the cyber communications from V_2 are correct.

5 $IBT_{CC_1,CC_2}\varphi_2$; CC_2 sends the correct cyber communications to CC_1.

6 $w \vDash V_{\varphi_2}^{CC_1}(w) = true$; CC_1 observes that V_2 sent the correct cyber communications.

7 $IBT_{VC_1,CC_1}\varphi_2$; CC_1 tells VC_1 that V_2 sent the correct cyber communications.

8 $w \vDash V_{\varphi_2}^{VC_1}(w) = true$; VC_1 observes thatV_2 sent the correct cyber communications.

9 $IBT_{CP,VC_1}\varphi_2$; VC_1 tells CP that V_2 sent the correct cyber communications.

10 $w \vDash V_{\varphi_2}^{CP}(w) = true$; CP observes that V_2 sent the correct cyber communications.

11 $\neg\varphi_2 \Rightarrow \neg f$; since $\neg\varphi_2 = true$ then function $\neg f = true$.

12 $IBT_{CP,f}\neg\varphi_2$; f tells CP that V_2 sent the incorrect cyber communications.

13 $w \vDash V_{\neg\varphi_2}^{CP}(w) = true$; CP has now deduced that V_2 sent the incorrect cyber communications.

14 $w \vDash V_{\neg\varphi_2}^{CP}(w) = true \implies w \vDash V_{\neg\varphi_2}^{FP_2}(w) = true$; since a valuation function exists at CP to evaluate φ_2 it follows that there also exists a valuation function at FP_2 to evaluate φ_2.

15 $IBT_{LB_2,CP}\neg\varphi_2$; CP tells LB_2 that V_2 sent the incorrect cyber communications.

16 $w \vDash V_{\neg\varphi_2}^{LB_2}(w) = true$; LB_2 observes that V_2 sent the incorrect cyber communications.

17 $IBT_{FP_2,LB_2}\neg\varphi_2$; LB_2 tells FP_2 that V_2 sent the incorrect cyber communications.

18 $w \vDash V_{\neg\varphi_2}^{FP_2}(w) = true$; FP_2 observes that V_2 sent the incorrect cyber communications.

19 $\neg$MSDND(ES): $\exists w \in W \vdash [(\varphi_2 \oplus \neg\varphi_2)] \wedge [w \models (\exists V_{\varphi_2}^{FP_2}(w))]$

FP_2 has a valuation of φ_2. Therefore, the cyber action readings are not MSDND secure to FP_2. This means FP_2 will know the truth behind whether V_2 was behaving correctly on a cyber level in prior platoons. □

Theorem 4.6. *A cyber-only blockchain is MSDND secure under an attack on the physical maneuvers of a vehicle.*

Proof. This proof follows similarly to the last except for the valuation function f. Thus, FP_2 believes the false physical action reading reported by LB_2. Therefore, the physical action readings are MSDND secure to FP_2. This means FP_2 will not know the truth behind whether V_2 was behaving correctly on a physical level in prior platoons. □

Lemma 1. *Since CP is the only entity with an information flow to LB_2 and LB_2 is the only entity with information flow to FP_2 it follows that if there exists a world such that $w \vDash V^{CP}_{\neg\varphi_2}(w) = true \implies w \vDash V^{FP_2}_{\neg\varphi_2}(w) = true$.*

Proof. This lemma follows from the fact that LB_2 cannot change its history since it is a read-only ledger belonging to V_2. Thus, since LB_2 cannot be malicious, it follows that it will pass on the same information that it receives from CP. Thus, if CP has a valuation function that can evaluate the truth of φ_2, then so does FP_2. □

Lemma 2. *FP_2 will receive the correct information regardless of whether V_1 is malicious or not.*

Proof. Since the number of attackers in bounded by assumption 3, CP will always have a valuation function that satisfies both the adapted IC1 and IC2. Thus, it will reach the correct valuation regardless of the presence of a bounded number of malicious vehicles. □

Corollary 2.1. *It follows that in a cyber-only blockchain, that the physical actions of vehicle 2 can be successfully altered while the cyber actions of vehicle 2 cannot be successfully altered to deceive the future platoon of vehicle 2.*

Proof. Both state variables φ_1 and φ_2 are independent of one another. This means that a vehicle can behave incorrectly on either the cyber level or physical level without forcing incorrect actions at the other level. □

This proof shows the inherent weakness of a cyber-only blockchain applied to a cyber-physical system. If a future platoon can be deceived about what a vehicle's actions were in past platoons then it is insecure since it cannot fully trust the joining vehicle. Now, a proof is presented

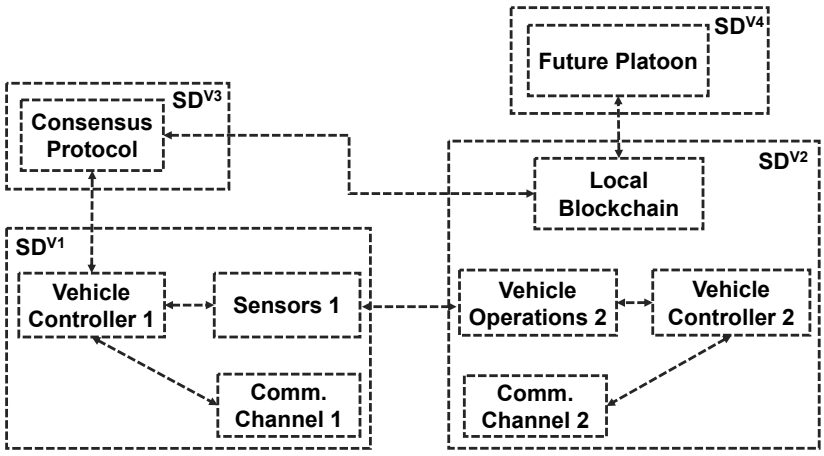

Figure 7. Physical Only Blockchain Information Flow Diagram

proving the security of a physical-only blockchain in the proposed architecture. In a physical-only blockchain, there is no information flow path from CC_2 to CC_1 as seen in figure 7.

Theorem 4.7. *A physical-only blockchain is not MSDND secure under an attack on the physical level of the system.*

Proof. Assume that in a cyber-only blockchain, some function f exists to determine whether φ_1 is true or false that is owned by CP. This follows from Assumption 7. In the model, it is assumed that CP will always be honest due to the bounded number of attackers in assumption 3.

1 $\neg\varphi_1 = true$; The V_2 is not maneuvering correctly.

2 $w \vDash V_{\varphi_1}^{VC_2}(w) = false$; VC_2 observes that V_2 is not maneuvering correctly.

3 $IBT_{VO_2,VC_2}\varphi_1$; VO_2 lies to VO_2 and tells it that V_2 is maneuvering correctly.

4 $w \vDash V_{\varphi_1}^{VO_2}(w) = true$; VO_2 observes that the V_2 is maneuvering correctly.

5 $IBT_{S_1,VO_2}\varphi_1$; VO_2 tells S_1 that V_2 is maneuvering correctly.

6 $w \vDash V_{\varphi_1}^{S_1}(w) = true$; S_1 observes that V_2 is maneuvering correctly.

7 $IBT_{VC_1,S_1}\varphi_1$; S_1 tells VC_1 that V_2 is maneuvering correctly.

8 $w \vDash V_{\varphi_1}^{VC_1}(w) = true$; VC_1 observes that V_2 is maneuvering correctly.

9 $IBT_{CP,VC_1}\varphi_1$; VC_1 tells CP that V_2 is maneuvering correctly.

10 $w \vDash V_{\varphi_1}^{CP}(w) = true$; CP observes that V_2 is maneuvering correctly.

11 $\neg\varphi_1 \Rightarrow \neg f$; since $\neg\varphi_1 = true$ then function $\neg f = true$.

12 $IBT_{CP,f}\neg\varphi_1$; f tells CP that V_2 is maneuvering incorrectly.

13 $w \vDash V_{\neg\varphi_1}^{CP}(w) = true$; CP has now deduced that V_2 is maneuvering correctly.

14 $w \vDash V_{\neg\varphi_1}^{CP}(w) = true \implies w \vDash V_{\neg\varphi_1}^{FP_2}(w) = true$; since a valuation function exists at CP to evaluate φ_1 it follows that there also exists a valuation function at FP_2 to evaluate φ_1.

15 $IBT_{LB_2,CP}\varphi_1$; CP tells LB_2 that V_2 is maneuvering correctly.

16 $w \vDash V_{\varphi_1}^{LB_2}(w) = true$; LB_2 observes that V_2 is maneuvering correctly.

17 $IBT_{FP_2,LB_2}\varphi_1$; LB_2 tells FP_2 that V_2 is maneuvering correctly.

18 $w \vDash V_{\varphi_1}^{FP_2}(w) = true$; FP_2 observes that V_2 is maneuvering correctly.

19 $\neg$ MSDND(ES): $\exists w \in W \vdash [(\varphi_1 \oplus \neg\varphi_1)] \wedge [w \models (\exists V_{\varphi_1}^{FP}(w))]$

FP_2 has a valuation of φ_2. Therefore, the physical action readings are not MSDND secure to FP_2. This means FP_2 will know the truth behind whether V_2 was behaving correctly on a physical level in prior platoons. □

Theorem 4.8. *A physical-only blockchain is MSDND secure under an attack on the cyber-level of the system.*

Proof. This proof follows similarly to the last except for the valuation function f. FP_2 does not have a valuation of φ_2. Therefore, the cyber action readings are MSDND secure to FP_2. This means FP_2 will not know the truth behind whether vehicle 2 was behaving correctly on a cyber level in prior platoons. □

Lemma 3. *Since CP is the only entity with an information flow to LB_2 and LB_2 is the only entity with information flow to FP_2 it follows that if there exists a world such that $w \vDash V_{\neg\varphi_1}^{CP}(w) = true \implies w \vDash V_{\neg\varphi_1}^{FP_2}(w) = true$.*

Corollary 3.1. *It follows that in a physical-only blockchain, that the cyber actions of vehicle 2 can be successfully altered while the physical actions of vehicle 2 cannot be successfully altered to deceive the future platoon of vehicle 2.*

Proof. See corollary 2.1 for a similar proof. □

Theorem 4.9. *A cyber-physical blockchain is not MSDND secure to either a cyber or physical level attack.*

This model is similar to figure 7 and figure 6 except that there is an information flow path from VO_2 to S_1 and CC_2 to CC_1.

Proof. Assume that in a cyber-physical blockchain, some function f_{φ_1} exists to determine whether φ_1 is true or false that is owned by CP and some function f_{φ_2} exists to determine whether φ_2 is true or false that is owned by CP. This follows from Assumption 7. In the model, it is assumed that CP will always be honest due to the bounded number of attacker in Assumption 3. Thus, since CP is the only entity with an information flow to LB_2 and LB_2 is the only entity with information flow to FP_2 it follows that if there exists a world such that $w \vDash V^{CP}_{\neg\varphi_1}(w) = true \implies w \vDash V^{FP_2}_{\neg\varphi_1}(w) = true$ and $w \vDash V^{CP}_{\neg\varphi_2}(w) = true \implies w \vDash V^{FP_2}_{\neg\varphi_2}(w) = true$. It follows from Theorem 4.7 and Theorem 4.8 that in a cyber-physical blockchain, neither cyber or physical actions of vehicle 2 can be successfully altered in order to deceive the future platoon of vehicle 2. □

Lemma 4. *A blockchain is only secure against an attack if it has a verification mechanism for attacks coming from that component in the system.*

This lemma shows the inherent weakness in many previous approaches to applying blockchains to cyber-physical systems.

5. Related Work

Significant research has been done to use blockchains to solve many of the issues in VANETs. The authors in [5] proposed a blockchain-based anonymous reputation system (BARS) that preserves privacy by removing the linkability between real identities and public keys in VANETs. In their work, they use multiple different blockchains to store different information such as messages, certificates, and revoked public keys. In their architecture, RSUs are used to reach consensus on the separate blockchains using proof-of-work (PoW).

The proof-of-event (PoE) consensus algorithms proposed to validate traffic events in a VANET [17]. This algorithm is run by RSUs and collects state information from passing vehicles. Once a threshold value is hit, the event is claim as true and broadcast to the rest of the VANET. All valid traffic events are published to a blockchain with the proof used to validate them.

Trust management of vehicular message is proposed in [16] via using RSUs to collect the state of the roadways from reporting vehicles. The RSUs use POW to reach consensus on the state of the road across the entire network. With the state collect, individual reports can be used to calculate the trust and accuracy of vehicles, determine their credibility, and find malicious vehicles.

In [10], the authors proposed branch-based blockchains to allow for a single ledger maintained across a large geographic area for intelligent vehicle networks. In their work, they propose to keep branches of the blockchain that are maintained by the infrastructure and represent a subsection of the entire geographic area. They propose the use of this architecture to allows vehicles to communicate with one another without compromising their private information.

The USDOT has also proposed a solution to security VANETs [14]. Their work doesn't use blockchains but proposes a system to secure the national transportation infrastructure. However, the issue with all of these previous works, including the solution proposed by the USDOT is that they are heavily reliant on a costly infrastructure, something avoided in the proposed system.

6. Conclusion

This paper presents a secure blockchain authentication scheme for VANETs that uses private blockchains which represent the history of a vehicle and is used as a token to join future platoons. The blocks use the Schnorr digital signature scheme to create a group signature that is signed by the entire platoon. This scheme is proven to be secure under a bounded number of attackers. The consensus mechanism presented uses basic Byzantine Fault Tolerance algorithms to reach an agreement by the platoon during the block creation algorithm. This scheme provides significant cost savings over other solutions by reducing infrastructure components.

In previous work, it was shown that their solution met the real-time requirements of a VANET [12]. In their approach, a vehicle's entire blockchain was transmitted so that it could be verified. It would eventually take too long and force the vehicles to re-certify with the CA. The scheme proposed in this paper outperforms prior work and also meets the same real-time requirements due to the fact it takes advantages of a group digital signature. This signature allows for all vehicles in the platoon to agree on a single block. Thus, only a single block is required to join the next platoon, saving considerably time.

This paper also shows the need for physical-level verification mechanisms when applying blockchains to cyber-physical systems. The verification mechanism presented in this paper is the use of other vehicles' sensors within a platoon to determine if a vehicle's actions are correct or incorrect. Future work includes discovering more verification mechanisms and applications for blockchains in cyber-physical systems so that the benefits of blockchains can be leveraged.

7. Acknowledgment

This work was supported in part by the Missouri University of Science and Technology's Chancellor's Distinguished Fellowship and grants from the US National Science Foundation under awards CNS-1505610 and CNS-183747.

References

[1] M. Amoozadeh, H. Deng, C. Chuah, H. Zhang, D. Ghosal, Platoon management with cooperative adaptive cruise control enabled by VANET, *Vehicular Communications*, vol. 2(2), pp. 110–123, 2015.

[2] C. Dwork, N. Lynch and L. Stockmeyer, Consensus in the presence of partial synchrony, *Journal of the ACM*, vol. (35)2, pp. 288–323, 1988.

[3] H. Hartenstein and L. P. Laberteaux, A tutorial survey on vehicular ad hoc networks, *IEEE Communications Magazine*, vol. (46)6, pp. 164–171, 2008.

[4] G. Howser and B. McMillin, A modal model of Stuxnet attacks on cyber-physical systems: A matter of trust, *Proceedings of the Eighth International Conference on Software Security and Reliability*, pp. 225–234, 2014.

[5] Z. Lu, Q. Wang, G. Qu, Z. Liu, BARS: A blockchain-based anonymous reputation system for trust management in VANETs, *Seventeenth IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, pp. 98–103, 2018.

[6] G. Maxwell, A. Poelstra, Y. Seurin and P. Wuille, Simple Schnorr multi-signatures with applications to Bitcoin, *Designs, Codes and Cryptography*, vol. (87)9, pp. 2139–2164, 2019.

[7] J. Moteff, C. Copeland and J. Fischer, Critical Infrastructures: What Makes an Infrastructure Critical?, Congressional Research Service, Washington, DC, (`apps.dtic.mil/dtic/tr/fulltext/u2/a467306.pdf`), 2003.

[8] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (bitcoin.org/bitcoin.pdf), 2008.

[9] P. Palaniswamy, B. McMillin, Cyber-physical security of an electric microgrid, *Proceedings of the Twenty-Third IEEE Pacific Rim International Symposium on Dependable Computing*, pp. 74–83, 2018.

[10] M. Singh and S. Kim, Branch based blockchain technology in intelligent vehicle, *Computer Networks*, vol. 145, pp. 219–231, 2018.

[11] M. Wagner and B. McMillin, Cyber-physical transactions: A method for securing VANETs with blockchains, *Proceedings of the Twenty-Third IEEE Pacific Rim International Symposium on Dependable Computing*, pp. 64–73, 2018.

[12] M. Wagner and B. McMillin, Formal verification of cyber-physical blockchain transactions in VANETs, Missouri University of Science and Technology, Rolla, Missouri, USA, (drive.google.com/file/d/1RwZLG6kjbGsbO7eDVu_vgQtO3ybHktJl/view?usp=sharing), 2019.

[13] D. Wagner and B. Schweitzer, The growing threat of cyber-attacks on critical infrastructure, *HuffPost*, May 24, 2016.

[14] J. Walker, Security Credential Management System (SCMS), U.S. Department of Transportation (www.its.dot.gov/resources/scms.htm), Washington, DC.

[15] J. Wright, J. Garrett, C. Hill, G. Krueger, J. Evans, S. Andrews, C. Wilson, R. Rajbhandari, B. Burkhard, National Connected Vehicle Field Infrastructure Footprint Analysis Final Report, FHWA-JPO-14-125, U.S. Department of Transportation, Washington, DC, 2014.

[16] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs, *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[17] Y. Yang, L. Chou, C. Tseng, F. Tseng, C. Liu, Blockchain-based traffic event validation and trust verification for VANETs, *IEEE Access*, vol. 7, pp. 30868–30877, 2019.