How Does CSMA/CA Affect the Performance and Security in Wireless Blockchain Networks

Bin Cao*, Mengyang Li, Lei Zhang, Yixin Li, and Mugen Peng*

***Abstract*—The impact of communication transmission delay on the original blockchain, has not been well considered and studied since it is primarily designed in stable wired communication environment with high communication capacity. However, in a wireless scenario, due to the scarcity of spectrum resource, a blockchain user may have to compete for wireless channel to broadcast transactions following Media Access Control (MAC) mechanism. As a result, the communication transmission delay may be significant and pose a bottleneck on the blockchain system performance and security. To facilitate blockchain applications in wireless Industrial Internet of Things (IIoT), this paper aims to investigate whether the widely used MAC mechanism, Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), is suitable for Wireless Blockchain Networks (WBN) or not. Based on tangle, as an example to analyze the system performance in term of confirmation delay, Transaction Per Second (TPS) and transaction loss probability by considering the impact of queueing and transmission delay caused by CSMA/CA. Next, a stochastic model is proposed to analyze the security issue taking into account the malicious double-spending attack. Simulation results provide valuable insights when running blockchain in wireless network, the performance would be limited by the traditional CSMA/CA protocol. Meanwhile, we demonstrate that the probability of launching a successful double-spending attack would be affected by CSMA/CA as well.**

***Index Terms*—Wireless blockchain network, Industrial Internet of Things, CSMA/CA, Tangle, Consensus, Double-spending attack.**

I. Introduction

Recently, blockchain has been regarded as an emerging technology to enable smart contracts in the Industrial Internet of Things (IIoT) ecosystem to provide a trusty system in a decentralized manner at a low cost without the involvement of any third party [1]. As a peer-to-peer network in essence, communication is critical to blockchain consensus, which plays a pivotal role in any types of blockchain systems. The original blockchain systems are primarily designed in stable wired communication environment and running in advanced IIoT devices, which may be not suitable for high dynamic wireless connected IIoT that is mainly composed of massive low-complex and low-power wireless devices, ranging from finance [2], supply chain [3], healthcare [4] and energy trading [5]. Especially through the upcoming 5G network connection, majority of valuable information exchange among the IIoT devices may be through wireless medium. According to IBM report [6], to be a smart, secure and efficient future, blockchain services will be deployed primarily on hundreds of billions IIoT devices by 2025 and majority of them will be connected via near wireless communications. Thus, it is predictable that the Wireless Blockchain Network (WBN) will play an important role in IIoT ecosystems in the near future. However, wireless connections among the peer nodes can be vulnerable due to wireless channel fading and openness, thus may pose a bottleneck on the blockchain system performance and security.

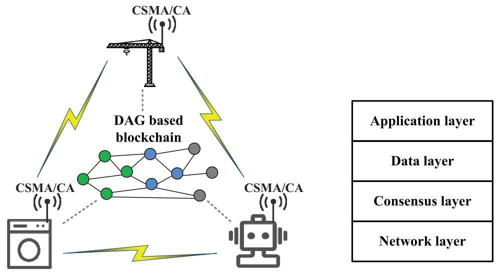
Consensus protocol, as a core component to blockchain for determining how to insert new transaction[1] into the chain securely, replies on frequent information exchange through wired/wireless communications among the peer nodes. The single chain architecture of existing blockchains (such as Bitcoin [7] and Ethereum [8]) limits the TPS and increases consensus delay. In contrast, a forking architecture is allowed in Direct Acyclic Graph (DAG) based blockchain to enable inserting new transactions as soon as possible [9]. In this way, many branches would be simultaneously generated for new transaction processing, and thus the transaction confirmation delay in DAG based blockchain can be improved significantly. Technically, TPS in DAG could be infinite when the transaction arrival tends to infinity compared with that in PoW and PoS [10] according to [11].

Fig. 1 (a) shows an example of CSMA/CA based WBN for IIoT system, where the blockchain is triggered by wireless sensor network when it has a data to be inserted into the DAG consensus network through the CSMA/CA communication protocol. The whole WBN contains two parts as shown in Fig. 1 (a). (1) Wireless network: various IIoT devices are distributed in WBN randomly with one hop coverage of the CMSA/CA, which is the communication protocol that all IIoT devices use to exchange information/transactions. (2) DAG based blockchain: consensus protocol runs on the top of wireless network and makes each IIoT device have the same DAG ledger. Note that the blockchain consensus running in the IIoT devices. Fig. 1 (b) colorredshows the structure of

The corresponding authors are B. Cao (drcaobin@ieee.org) and M. Peng (pmg@bupt.edu.cn). B. Cao , Y. Li and M. Peng are with Beijing University of Posts and Telecommunications, Beijing 100876, China, Bin Cao is also with the State Key Laboratory of Integrated Services Networks (Xidian University). M. Li is with Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, China. L. Zhang is with the James Watt School of Engineering, University of Glasgow, Glasgow, G12 8QQ, U.K.

This work was supported by the State Major Science and Technology Special Project (2018ZX033001023), in part by the National Program for Special Support of Eminent Professionals, the National Natural Science Foundation of China (61701059 and 61831002), the Eighteenth Open Foundation of State Key Lab of Integrated Services Networks of Xidian University (ISN20-05), Chongqing Technological Innovation and Application Development Projects (cstc2019jscx-msxm1322), and Basic and Advanced Research Projects of CSTC (cstc2019jcyj-zdxm0102).

[1]This terminology is first used in the first digital cryptocurrency Bitcoins, However, the terminology "transactions" can be generalized to stand for any value information exchange in the network.



(a) Various IIoT devices communicate each other based on CSMA/CA (b) The struture of a typical IIoT device

Fig. 1: A typical structure of CSMA/CA based WBN and IIoT devices in IIoT system (Note that the DAG based blockchain is running in the IIoT devices on the consensus layer)

typical IIoT devices, it is composed of application layer, data layer, consensus layer and network layer. The function of each layer is requesting to issue transactions, recording transactions ledger, executing consensus protocols to achieve consensus and transmitting transactions with CSMA/CA, respectively.

Although DAG based blockchain has shown the aforementioned dramatic benefits, there remain some issues that are very important but not to be well addressed. From the communication perspective, a typical assumption in the traditional blockchain systems is that communications among the users are perfect without any throughput and delay constraints. However, considering the unstable channel quality, interference, limited resource and various network topologies in the wireless connected blockchain networks, the assumption is hard to meet. In other words, communication is the fundamental bound that limits the performance of blockchain systems.

Communication is not been well considered in analysis and system design in literatures since it was assumed perfect without generating any negative impact on the blockchain system. However, it can be seen from above that communication plays a key role in the system and its impact on the system could be far from perfect to be ignored. For instance, the queuing delay in the CSMA/CA communication protocol can be serious in a high loading network traffic and thus resulting in a lower TPS. Moreover, the computational power and wireless channel competitions between honest user and attacker may affect the WBN security level. To the best of our knowledge, there is no such analytical model dedicated consider the wireless communication impacts on the blockchain system performance and security.

Accordingly, these aforementioned observations inspire us to investigate that how does CSMA/CA affect DAG based blockchain and what are the corresponding consequences, the main contributions of this paper are listed as follows.

- We first introduce a system model for wireless blockchain network based on CSMA/CA.
- We theoretically analyze the performance of WBN in terms of transaction confirmation delay, TPS and transaction loss probability, with and without the impact of communication transmission delay.
- To analyze the communication protocol impact on the security, we introduce a stochastic model to investigate the probability of successful double-spending attack in WBN.

The rest of this paper is organized as follows. Section II introduces some basic principles of CSMA/CA and DAG based blockchain. The system model is given in Section III. Section IV theoretically analyzes the performance of transaction confirmation delay, TPS and transaction loss probability in WBN. Section V derives the security for double-spending attack in WBN. Simulations are conducted to show the impact of CSMA/CA on the performance and security of WBN in Section VI, and we conclude this paper in section VII.

II. Preliminaries

In this section, we introduce the basic knowledge of C-SMA/CA and DAG based blockchain consensus protocol, respectively. Next, we describe the main procedure illustrating that how to apply consensus protocol with CSMA/CA in WBN to issue a new transaction.

A. *Wireless Network Protocol*

As we known, IEEE 802.11 series have been widely used in wireless network, the basic MAC mechanism is Distributed Coordination Function (DCF) [12], which is a random access mechanism based on CSMA/CA. In this paper, we use CS-MA/CA for media access when any user wants to compete the wireless channel to broadcast a packet (including an amount of new transactions) to WBN.

B. *DAG Based Blockchain*

DAG based blockchain allows a transaction to be recorded in system at anytime and anywhere in a forking manner. In this paper, we use tangle [13] as a typical consensus protocol example to discuss DAG based blockchain since it is the first blockchain proposed for IIoT system with the highest market value of DAG based blockchain.

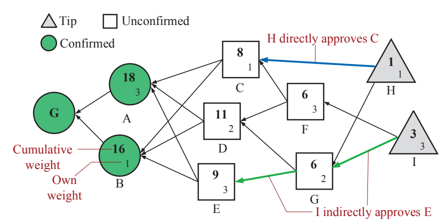


Fig. 2: A typical example of tangle

As shown in Fig. 2, tangle uses DAG ledger to record transactions, each unit in tangle indicates a recorded transaction. In order to understand the analysis and discussion in the following, we introduce some basic concepts in tangle as follows. *Tip*: it is a brand new transaction that just attaches onto tangle. *Own weight*: the own weight of the transaction depends on the power of work by its issuing user. *Cumulative weight*: it is the sum of the unit's own weight and the cumulative weight of other units that directly and indirectly approve it. *Approval*: a directed edge between two transactions represent a approval. *Markov Chain Monte Carlo (MCMC)*: to access tangle, any new transaction must approve an amount of previous ones (typically two) following a tips selection algorithm. Using MCMC, some particles would be placed on the old transactions independently to perform random walks towards the tips, the particles prefer to go through the transactions with a higher cumulative weight to the sub-tangle for security.

C. Consensus Process in Wireless Network

In order to achieve the confirmation, consensus protocol should work to let the new transaction be accepted by other users, after the broadcast procedure following CSMA/CA in wireless network. It it worth to mention again that the consensus is running on the consensus level at the IIoT devices. Thus, the logical tips and users in the consensus protocol are equivalent to the physical IIoT devices, and the communications required by the consensus users are implemented by the wireless modules in the devices. For simplicity, this paper only considers users under the same local area network (LAN), the main procedures are shown as follows.

(i) When a new transaction comes at a user, it should select two non-conflicting tips to approve based on the local information. (ii) The user uses its private key to sign this new transaction. In order to broadcast it to other users through wireless channel, this new transaction should enter into the cache waiting for broadcasting. (iii) The user competes for wireless channel following CSMA/CA while the new transaction queues in the cache following First In First Out (FIFO) [14]. (iv) The user broadcasts the new transaction successfully, otherwise, the new transaction should be rebroadcast with backoff. (v) Other users receive the new transaction and check it to confirm the legality. If yes, this new transaction becomes a new tip waiting for the direct or indirect approvement for confirmation. It can be seen that communication may cause a serious delay in step iii), depends on the network traffic load, which will be analyzed in the next.

For convenience, TABLE I lists the main mathematical notations in this paper.

TABLE I: Notation Descriptions

Notation	Definition
n	The number of users running tangle
λ, μ	The transaction arrival rate of a honest user and that of a malicious attacker respectively
λ_l, λ_h	The transaction arrival rate of a honest user in light and heavy load regime respectively
k	The multiplier representing the cache of each user
m	The number of maximum transactions at one broadcast
h	The average transmission delay to broadcast a packet or the duration time to update the new transaction
$L(t)$	The number of tips in tangle at time t
T_d, $T_d^{'}$	The transaction confirmation delay in expected and practical regime respectively
T_q, $T_q^{'}$	The queuing delay in expected and practical regime respectively
T_a, $T_a^{'}$	The duration time of adaptation sub-period in expected and practical regime respectively
T_l, $T_l^{'}$	The duration time of linear increasing sub-period in expected and practical regime respectively
ω_a, $\omega_a^{'}$	The cumulative weight of the transaction at the end of adaptation sub-period in expected and practical regime respectively
ω	Confirmation threshold
t_0	The time when the attacker broadcasts a payment to the merchant
t_1	The time when the attacker builds a parasite chain
t_2	The time when the payment is confirmed
i_a, i_h	The number of transactions issued by honest users and by attacker from t_1 to t_2 respectively
N_a	The possible number of transactions issued by attacker from t_1 to t_2
$\lambda^{'}$, $\mu^{'}$	The transaction arrival rate of a honest user and that of a malicious attacker respectively
α, $\alpha^{'}$	The probability of the new transaction issued by honest users in expected and practical regime respectively
β, $\beta^{'}$	The probability of the new transaction issued by attacker in expected and practical regime respectively

III. System Model And Definitions

A. System Model

In order to analyze the consensus process of a new transaction in WBN, we divide the process into two periods: the queueing period based on CSMA/CA (the previous mentioned procedures from (i) to (iii)), and weight accumulating period (the previous mentioned procedures from (iv) to (v)) based on consensus protocol. Assume that there are n users running tangle (they are all honest users in performance analysis, and $n-1$ honest users with one attacker in security analysis, respectively), they can communicate with each other directly through wireless channel, and the arrival of new transactions on each user follows the Poisson point process [15]. Let λ be the arrival rate of new transactions on a honest user, μ be the arrival rate of new transactions on a malicious attacker, and the own weight of each transaction be 1.

We define h as the average transmission delay to broadcast a packet (i.e., the time interval between two adjacent broadcasts) through CSMA/CA. According to [16], we can calculate h in detail based on CSMA/CA by the corresponding settings in wireless network. Moreover, m is defined as the number of maximum transactions at one broadcast. I.e., due to the constrain of broadcast capacity, each user can broadcast a maximum packet of m transactions in each time. Additionally, h is also the reveal time to update the new transactions discussed in tangle [13]. Let $Q = km$ $(k \in \mathbb{N})$ be the cache length of each user, $W(t)$ be the cumulative weight of an observed transaction at time t, and $L(t)$ be the total number of tips in tangle at time t, respectively.

Considering the network load condition of WBN, we classify two regimes to describe the queueing state as follows.

B. Light Network Load Regime (LR)

Assume the network is lightly loaded with $\lambda = \lambda_l$, since each user has the equal probability ($\frac{1}{n}$) to broadcast due to the fairness of CSMA/CA, the average time to compete the broadcasting on each user is nh, and therefore, the cumulative transactions waiting for broadcasting on each user is $nh\lambda_l$, where $nh\lambda_l \leq m$ (i.e., a maximum packet including m transactions) that means all the waited transactions in cache can be broadcasted immediately when the user successfully competes for wireless channel. According to the analysis in [13], if λ_l is very small, $L(t)$ can be approximated as 1, otherwise, $L(t) = 2nh\lambda_l$.

C. Heavy Network Load Regime (HR)

When the network becomes heavily loaded with $\lambda = \lambda_h$, the cumulative transactions on each user is $nh\lambda_h$, where $nh\lambda_h > m$. In this case, the new transactions cannot be broadcasted immediately, and thus the rest of them should queue in the cache waiting for the next broadcasting. Moreover, if the cache is full, the new transaction must be dropped. Moreover, since the maximum broadcasting number of new transaction is m, we have $L(t) = 2m$ in this situation.

IV. Performance Analysis

To achieve the confirmation of a new transaction, two periods of delay may happens in both queuing in communication network and blockchain weight accumulating in consensus process. Based on [13], we can know that the weight accumulating of a new transaction is composed of two sub-periods, i.e., adaptation sub-period and linear increasing sub-period for weight accumulating. Thus, the transaction confirmation delay (T_d) from it is requested by a user to the stage of being confirmed by the consensus network can be expressed as

$$T_d = T_q + T_a + T_l, \tag{1}$$

where T_q is the queuing delay counting from the time that the transaction arrives into cache of a user to the time that it is broadcast to WBN, which is caused by CSMA/CA in this paper. $T_a + T_l$ is the weight accumulating delay caused by consensus protocol, T_a is the time in adaptation and T_l is the time in linear increasing, respectively. Specifically, DAG based blockchain without the communication protocol has been analyzed in [13], but the values of T_a and T_l will be different due to the imperfect communication, thus, will be analyzed in the next one by one.

A. Expected Performance Considering Consensus Protocol

1) Transaction Confirmation Delay: In order to show the running CSMA/CA WBN impact on the consensus process, we first assume that the delay caused by wireless communication network is negligible, i.e., $T_q = 0$ in (1). This case has been analyzed in [13] and we summarize it here for benchmark and further derivations. In this case, in adaptation sub-period, the cumulative weight of a new transaction grows with $W_a(t) = 2\exp(0.352\frac{t}{h})$,which is based on [13]. For more information, the readers can refer to the details of analysis and discussion.

Since the reveal time of new transactions is h, we can assume that tangle in WBN updates with h periodically. Therefore, the consensus process can be seemed as a discrete-time stochastic process, and the duration time of adaption sub-period in different regimes with λ_l or λ_h can be shown as

$$T_a = \begin{cases} \lfloor 2.84 \cdot \ln(2nh\lambda_l) \rfloor \cdot h, & \text{LR}, \\ \lfloor 2.84 \cdot \ln(2nh\lambda_h) \rfloor \cdot h, & \text{HR}. \end{cases} \tag{2}$$

When a transaction has been fully covered by the tips through direct and indirect approvals, the adaptation sub-period is over to enter linear increasing sub-period, where the cumulative weight increases linearly with λ. Assume the cumulative weight of the transaction at the end of adaptation sub-period is ω_a, the duration time from ω_a to the confirmation threshold ω of linear increasing sub-period is

$$T_l = \begin{cases} \frac{\omega - \omega_a}{\lambda_l}, & \text{LR}, \\ \frac{\omega - \omega_a}{\lambda_h}, & \text{HR}. \end{cases} \tag{3}$$

where

$$\omega_a = \begin{cases} 2\exp(0.352 \cdot \lfloor 2.84 \cdot \ln(2nh\lambda_l) \rfloor), \text{LR}, \\ 2\exp(0.352 \cdot \lfloor 2.84 \cdot \ln(2nh\lambda_h) \rfloor), \text{HR}. \end{cases} \tag{4}$$

As a result, the expected transaction confirmation delay, which does not consider the impact of queuing and competing in CSMA/CA, can be expressed as follows,

$$T_d = \begin{cases} \lfloor 2.84 \cdot \ln(2nh\lambda_l) \rfloor \cdot h + \frac{\omega - \omega_a}{\lambda_l}, \text{LR}, \\ \lfloor 2.84 \cdot \ln(2nh\lambda_h) \rfloor \cdot h + \frac{\omega - \omega_a}{\lambda_h}, \text{HR}. \end{cases} \tag{5}$$

2) TPS: As another important performance metric, TP-S is to demonstrate the transaction processing capacity of blockchain system, it can be calculated as the number of new transactions in a broadcast interval time divided by confirmation delay, which is shown as follows,

$$TPS = \begin{cases} \frac{nh\lambda_l}{\lfloor 2.84 \cdot \ln(2nh\lambda_l) \rfloor \cdot h + \frac{\omega - \omega_a}{\lambda_l}}, \text{LR}, \\ \frac{nh\lambda_h}{\lfloor 2.84 \cdot \ln(2nh\lambda_h) \rfloor \cdot h + \frac{\omega - \omega_a}{\lambda_h}}, \text{HR}. \end{cases} \tag{6}$$

3) Transaction Loss Probability: In order to measure the Quality of Service (QoS) of DAG based blockchain, we define the transaction loss probability (P_{tl}) recording the ratio that a new transaction cannot be insert into blockchain. Without consideration of the restriction of access control in CSMA/CA, all the new transactions could enter into blockchain system successfully (no queuing and competing). Therefore, we can have

$$P_{tl} = 0, \tag{7}$$

which means there is no transaction loss in this case.

B. Practical Blockchain Performance based on CSMA/CA

Communication protocol can significantly affect the blockchain performance in terms of confirmation delay, TPS and transaction loss probability. We will analyze them one by one as follows.

1) Transaction Confirmation Delay: Usually, h is assumed as a constant value to evaluate the broadcasting time in the existing work for analysis [13]. In contrast, considering the impact of CSMA/CA in wireless network, we need to know how to calculate h accordingly.

In CSMA, the collision probability of each packet (ρ) can be expressed as [16]

$$\rho = 1 - (1 - \tau)^{n-1}. \tag{8}$$

Due to backoff procedure, the probability of a user transmitting in a randomly chosen slot time (τ) is given by

$$\tau = \frac{2(1-2\rho)}{(1-2\rho)(CW_{min}+1)+\rho CW_{min}(1-(2\rho)^s)}. \quad (9)$$

Using iterative solution, we can obtain the value of τ from (8) and (9).

Based on τ, considering n users competing to the wireless channel, the probability of at least one broadcasting in a slot time (P_{tr}) can be expressed as

$$P_{tr} = 1-(1-\tau)^n. \quad (10)$$

Similarly, the probability P_s that one user broadcasts successfully in a slot time, and the probability P_c that broadcast collision occurs in a slot time (more than one user to broadcast), are shown as follows,

$$P_s = \frac{\tau(1-\tau)^{n-1}}{P_{tr}/n} = \frac{n\tau(1-\tau)^{n-1}}{1-(1-\tau)^n}, \quad (11)$$

$$P_c = 1-P_s. \quad (12)$$

Let T_s be the average time the channel is detected busy due to a successful broadcasting, and T_c be that during a collision, σ be the duration of an empty slot time. Meanwhile, considering their corresponding probabilities of $1-P_{tr}$, $P_{tr}P_s$ and $P_{tr}P_c$, we can have the expression of h as follows,

$$h = (1-P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}P_cT_c. \quad (13)$$

Moreover, define $E[P]$ as the average packet payload size, the expression of T_s and T_c in four-way handshaking scheme are shown as,

$$\begin{cases} T_s = T_{RTS}+SIFS+\delta+T_{CTS}+SIFS+\delta+H \\ \qquad +T_{E[P]}+SIFS+\delta+T_{ACK}+DIFS+\delta \\ T_c = T_{RTS}+DIFS+\delta \end{cases} \quad (14)$$

where T_{RTS}, $SIFS$, δ, T_{CTS}, $T_{E[P]}$, $H = PHY_{hdr} + MAC_{hdr}$, T_{ACK} and $DISF$ are broadcast time of RTS, that of short interframe space, propagation delay, that of CTS, that of packet payload, that of packet header, that of ACK and distributed interframe space, respectively.

Considering the fairness of CSMA/CA, each user has the equal probability to access the wireless channel to broadcast. we know the cache on each user has less than m transactions when the network load is light, thus, it can broadcast all transactions in the cache at once time. Specifying single user, the average queuing time for a new transaction is $\frac{nh}{2}$ in LR where the cache is non-full. In contrast, the cache on each user is full due to the heavy load. Therefore, if a user competes successfully, it would broadcast m transactions, and thus it can store m new transactions accordingly. Meanwhile, with the incoming of new transactions, the cache would be full again. Moreover, considering the average time to compete for broadcasting on each user is nh, we have the average queueing time for a new transaction in HR is $knh-\frac{m}{2\lambda_h}$, where k is competition times for broadcasting due to FIFO (any new arrival transaction must wait in the cache until the previous transactions have been sent), and $\frac{m}{2\lambda_h}$ is the average duration time for a new transaction counting from the time that cache has space to store to the time that it becomes full again.

Therefore, the queuing delay is shown as follows,

$$T_q' = \begin{cases} \frac{nh}{2}, & \text{LR}, \\ knh-\frac{m}{2\lambda_h}, & \text{HR}. \end{cases} \quad (15)$$

Moreover, since $L(t) = 2m$ in HR considering CSMA/CA based on the previous analysis, the duration time of adaption sub-period in different regimes can be shown as

$$T_a' = \begin{cases} \lfloor 2.84\cdot\ln(2nh\lambda_l)\rfloor\cdot h, & \text{LR}, \\ \lfloor 2.84\cdot\ln(2m)\rfloor\cdot h, & \text{HR}. \end{cases} \quad (16)$$

Because the maximum number of transactions is m in once broadcasting considering CSMA/CA, the upper bound of new transactions arrival rate entering tangle network is $\frac{m}{nh}$. As a result, the duration time of linear increasing sub-period is shown as follows,

$$T_l' = \begin{cases} \frac{\omega-\omega_a'}{\lambda_l}, & \text{LR}, \\ \frac{\omega-\omega_a'}{m/nh}, & \text{HR}. \end{cases} \quad (17)$$

where

$$\omega_a' = \begin{cases} 2\exp(0.352\cdot\lfloor 2.84\cdot\ln(2nh\lambda_l)\rfloor), & \text{LR}, \\ 2\exp(0.352\cdot\lfloor 2.84\cdot\ln(2m)\rfloor), & \text{HR}. \end{cases} \quad (18)$$

note that in heavy load regime, due to the restrain of transmission capacity, the cumulative weight of a new transaction has changed in the end of adaptation sub-period compared to expected DAG based blockchain.

Accordingly, we can have the practical transaction confirmation delay as follows,

$$T_d' = \begin{cases} \frac{nh}{2}+\lfloor 2.84\cdot\ln(2nh\lambda_l)\rfloor\cdot h+\frac{\omega-\omega_a'}{\lambda_l}, & \text{LR}, \\ knh-\frac{m}{2\lambda_h}+\lfloor 2.84\cdot\ln(2m)\rfloor\cdot h+\frac{\omega-\omega_a'}{m/nh}, & \text{HR}. \end{cases} \quad (19)$$

2) TPS: Based on T_d' given in (19), we can have the expression of in the two regimes as follows,

$$TPS' = \begin{cases} \frac{nh\lambda_l}{\frac{nh}{2}+\lfloor 2.84\cdot\ln(2nh\lambda_l)\rfloor\cdot h+\frac{\omega-\omega_a'}{\lambda_l}}, & \text{LR}, \\ \frac{m}{knh-\frac{m}{2\lambda_h}+\lfloor 2.84\cdot\ln(2m)\rfloor\cdot h+\frac{\omega-\omega_a'}{m/nh}}, & \text{HR}. \end{cases} \quad (20)$$

3) Transaction Loss Probability: In HR, since only an amount of new transactions can enter the cache after a successful broadcasting, the rest new transactions would be dropped due to no space to store. As a result, transaction loss occurs. In each broadcasting, m new transactions can be stored in cache since m previous transactions have been broadcast. However, the average time for a broadcasting on a user is nh, and thus the overall number of incoming new transaction is $nh\lambda_h$. Therefore, we can have the transaction loss probability as

$$P_l' = \begin{cases} 0, & \text{LR}, \\ 1-\frac{m}{nh\lambda_h}, & \text{HR}. \end{cases} \quad (21)$$

V. Double-spending Attack Analysis

In this section, we first introduce the most typical double-spending attack by considering a perfect wireless communication [17]. Then, we analyze the successful attack probability for double-spending considering imperfect CSMA/CA protocols.

A. Attack Process and Model

As shown in Fig. 3, the typical approach to launch a double-spending attack by a malicious user is to build a parasite chain [18], the main procedures are illustrated as follows.

(i) At t_0, the attacker broadcasts a payment to the merchant and the honest users would begin to approve it.

(ii) At t_1, the attacker builds a parasite chain to approve a conflicting transaction with the payment in an off-line manner, which attaches to the current tips secretly. Note that t_1 is the end of adaptation sub-period for the payment at t_0.

(iii) At t_2, the payment has been confirmed where its cumulative weight reaches ω, then the merchant would send the production to the attacker (it might be a useful information or service).

(iv) After t_1, the attacker uses its own computational power to continually issue meaningless transactions to increase the cumulative weight of the conflicting transaction.

(v) As long as the cumulative weight of the conflicting transaction outweighs the achieved payment after t_2, the attacker will broadcast the off-line branch to the whole WBN.

(vi) The attacker contends for the wireless channel to broadcast the off-line branch updating the tangle at once, and the conflicting transaction would be accepted by other honest users in WBN based on MCMC algorithm due to the higher cumulative weight. Finally, the achieved payment would be orphaned in tangle, the merchant cannot receive the payment (it would be cancelled) even though it has provided the production, and thus the double-spending attacking is successful.

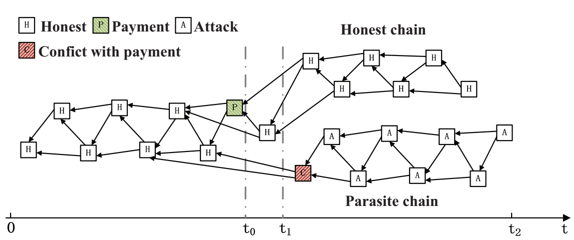


Fig. 3: Parasite chain for double-spending attack

Recall that the own weight of each transaction is 1, to launch an attack, the cumulative weight comparison between the attacker and the honest users can be treated as transactions issuing competition, where the ability to generate transactions is a kind of computational power for the attacker.

Next, we can describe the above attack process as a Markov chain. Assume i_h and i_a are the number of transactions issued by honest users and that by attacker from t_1 to t_2. As shown in Fig. 4, the state is the difference of issued number of transactions between honest users and attackers, where the

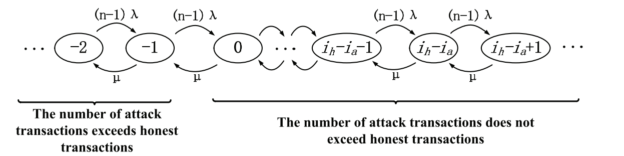


Fig. 4: A state flow for transactions issuing competition between attacker and honest users

initial state is the difference at time t_2 that is $i_h - i_a$, and the state "+1" or "−1" would be determined by the who (i.e., the attacker or honest user) issues the next new transaction.

According to above analysis, the successful attack probability for double-spending can be expressed as

$$P\{attack\ succeeds\} = P\{attack\ succeeds\ at\ t_2\} + \\ (1 - P\{attack\ succeeds\ at\ t_2\})P\{attack\ succeeds\ after\ t_2\}. \tag{23}$$

Note that the attacker cannot broadcast the parasite chain to public before t_2, since the payment has not been confirmed yet. In an other word, the double-spending attack must occur at t_2 or after it as long as the attacking requirement is met.

B. Expected Successful Attack Probability

In order to show the impact of CSMA/CA running in WBN on the security, we first analyze the successful attack probability without considering communication protocol, we call it as "expected" successful attack probability.

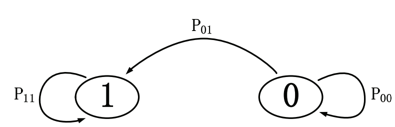


Fig. 5: A state transition probability in expected attack

For simplicity, we define that state "0" means that the number of transactions issued by attacker has not exceeded that by honest users, and state "1" means the attacker wins. Therefore, the state transition flow in Fig. 4 can be converted into a probability transfer state diagram shown in Fig. 5.

Let the probability that the new transaction issued by honest users be α, which can be expressed as follows,

$$\alpha = \frac{(n-1)\lambda}{(n-1)\lambda + \mu}. \tag{24}$$

Meanwhile, let the probability that the new transaction issued by attacker be β, which is

$$\beta = \frac{\mu}{(n-1)\lambda + \mu}. \tag{25}$$

To this end, the attack process can be treated as independent Bernoulli trials [15]. At t_2, the attacker would like to broadcast its parasite chain if the number of issued transactions is more than that of honest users. Otherwise, it should keep on issuing. Therefore, the number of transactions issued by attacker from t_1 to t_2 can be treated as a stochastic process N_a, and we can

$$P_e\{attack\ succeed\} = P_1(t_2) + P_0(t_2)P_{01}$$
$$= \sum_{i_a=i_h+1}^{\infty} \binom{i_a+i_h-1}{i_h-1} \alpha^{i_h}\beta^{i_a} + \sum_{i_a=0}^{i_h} \binom{i_a+i_h-1}{i_h-1} \alpha^{i_h}\beta^{i_a}(\min(\beta/\alpha,1))^{i_h-i_a+1} = \begin{cases} 1-\sum_{i_a=0}^{i_h}\binom{i_a+i_h-1}{i_h-1}(\alpha^{i_h}\beta^{i_a}-\alpha^{i_a-1}\beta^{i_h+1}), \alpha>\beta, \\ 1, \qquad \alpha\leq\beta. \end{cases} \tag{22}$$

obtain the probability mass function of N_a based on negative binomial distribution theory [15] as follows,

$$P\{N_a = i_a\} = \binom{i_a+i_h-1}{i_h-1}\alpha^{i_h}\beta^{i_a}. \tag{26}$$

Accordingly, we can have the probabilities that attacker does not win ($P_0(t_2)$) and attacker wins ($P_1(t_2)$) at t_2 as follows,

$$P_0(t_2) = \sum_{i_a=0}^{i_h}\binom{i_a+i_h-1}{i_h-1}\alpha^{i_h}\beta^{i_a}, \tag{27}$$

$$P_1(t_2) = \sum_{i_a=i_h+1}^{\infty}\binom{i_a+i_h-1}{i_h-1}\alpha^{i_h}\beta^{i_a}. \tag{28}$$

If $N_a > i_h$, the double-spending attack will succeed at t_2. Otherwise, in order to win, the attacker should catch up the difference of issued transactions until the cumulative weight of conflicting transaction in parasite chain outweighs that of payment in honest chain after t_2. Therefore, the attacker should catch up the difference of $i_h - N_a + 1$ transactions at least, and the corresponding probability to catch up is shown as follows,

$$P_{01} = \begin{cases} (\beta/\alpha)^{i_h-i_a+1}, & \alpha>\beta, \\ 1, & \alpha\leq\beta. \end{cases} \tag{29}$$

From this, the successful attack probability is shown in (22) on the top of this page.

At t_1, the number of transactions approving the payment is $W(t_1) - 1$. Therefore, at t_2, we can have $i_h = \omega - (W(t_1) - 1)$. Based on (22), the successful attack probability can be expressed as

$$P\{attack\ succeeds\} = \begin{cases} f(\omega - W(t_1) + 1), & \alpha>\beta, \\ 1, & \alpha\leq\beta, \end{cases} \tag{30}$$

where $f(x) = 1 - \sum_{i_a=0}^{x}\binom{i_a+x-1}{x-1}(\alpha^x\beta^{i_a} - \alpha^{i_a-1}\beta^{x+1})$ and $W(t_1)$ is the cumulative weight at the end of adaption period. To distinguish the impact of network load on α and β, let $\alpha_l = \frac{(n-1)\lambda_l}{(n-1)\lambda_l+\mu}$, $\beta_l = \frac{\mu}{(n-1)\lambda_l+\mu}$, $\alpha_h = \frac{(n-1)\lambda_h}{(n-1)\lambda_h+\mu}$, and $\beta_h = \frac{\mu}{(n-1)\lambda_h+\mu}$, respectively.

C. Practical Successful Attack Probability

Then, we analyze the successful attack probability from the perspective of wireless communication, we call it as "practical" one.

In this case, the attacker should win the transactions issuing competition as well as broadcast the parasite chain successfully. The maximum number of broadcast transactions would be limited by CSMA/CA that is m, and therefore, the maximum new transactions arrival rate is $\frac{m}{nh}$. In contrast, in previous analysis, it grows with λ without any limitation.

Recall that we assume there are $n-1$ honest users and 1 attacker in a one-hop wireless network, we denote λ' and μ' instead of λ and μ respectively in the practical scenario as follows,

$$\begin{cases} \lambda' = min\{\lambda, \frac{m}{nh}\} \\ \mu' = min\{\mu, \frac{m}{nh}\} \end{cases} \tag{31}$$

Let the probability that the broadcast transaction issued by honest users be α', which can be expressed as follows,

$$\alpha' = \frac{(n-1)\lambda'}{(n-1)\lambda' + \mu'}. \tag{32}$$

Meanwhile, let the probability that the broadcast transaction issued by attacker be β', which is

$$\beta' = \frac{\mu'}{(n-1)\lambda' + \mu'}. \tag{33}$$

Similarly, based on (22), the successful attack probability is shown as follows,

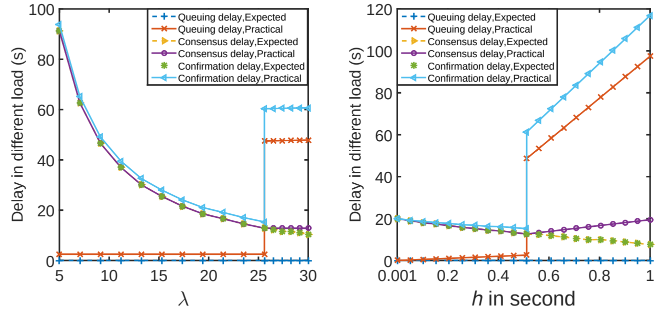
$$P_p\{attack\ succeed\} = \\ = \begin{cases} 1-\sum_{i_a=0}^{i_h}\binom{i_a+i_h-1}{i_h-1}(\alpha'^{i_h}\beta'^{i_a} - \alpha'^{(i_a-1)}\beta'^{(i_h+1)}), \alpha'>\beta', \\ 1, \qquad \alpha'\leq\beta'. \end{cases} \tag{34}$$

VI. SIMULATION AND DISCUSSION

In this section, we conduct several experiments to numerically evaluate the practical results in WBN, in order to illustrate the impact of CSMA/CA on the performance and security of blockchain in wireless scenario. Meanwhile, in order to provide a comparison, we also show the corresponding expected results in blockchain system without any queueing and competition caused by CSMA/CA. In particular, we assume that the average payload size is $E[P] = 1024$ bytes and the size of each transaction is 64 bits. Therefore, we can have a payload including transactions $m = 128$, and set the cache length $k = 10$. Moreover, each result shown in the figures are averaged more than 100 repeatable simulations.

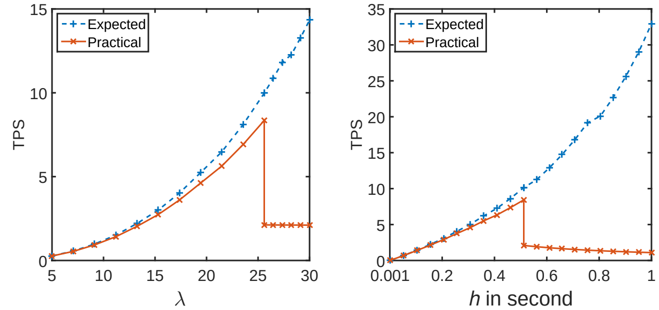
A. Performance Comparisons

For performance comparisons, let the number of users $n = 10$ and the confirmation threshold $\omega = 500$. In the first experiment, we evaluate queueing, consensus and confirmation delay by varying the new transaction arrival rate λ and transmission delay h, respectively. Fig. 6 (a) shows queueing,



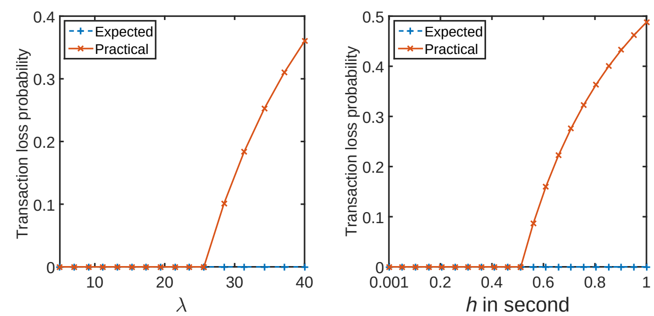
(a) delay vs λ (with $h = 0.5$)   (b) delay vs h (with $\lambda = 25$)

Fig. 6: Queuing, consensus and confirmation delay versus new transaction arrival rate and transmission delay.



(a) TPS vs λ (with $h = 0.5$)   (b) TPS vs h (with $\lambda = 25$)

Fig. 7: TPS versus new transaction arrival rate and transmission delay.



(a) Transaction loss probability vs λ (with $h = 0.5$)   (b) Transactions loss probability vs h (with $\lambda = 25$)

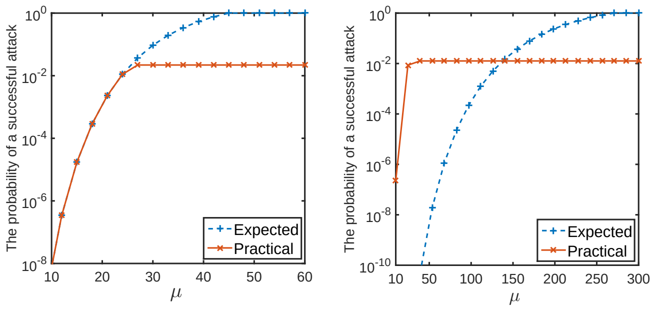
Fig. 8: Transaction loss probability versus new transaction arrival rate and transmission delay.

consensus and confirmation delay with the increasing of λ from 5 to 30 when $h = 0.5$. Since the impact of CSMA/CA has not been considered in the expected case, where all the new transactions can enter the blockchain system in a DAG manner without queueing and competition, we can see that the queuing delay is zero, and thus the consensus delay is equal to confirmation delay. However, in practical WBN, the communication protocol (CSMA/CA) plays a key role in the consensus process, which is evaluated and shown in the practical results. Specifically, when the network load is light (i.e., $\lambda \in [5, 25.6]$), the queueing delay is small, and the practical and expected consensus delay have the same performance. In this situation, all the new transactions in the cache can be broadcast once the user competes successfully, which results in the constant average queueing delay that is $\frac{nh}{2}$. In contrast, when $\lambda \geq 25.6$, the network becomes heavily loaded, and thus the cache would be full finally. In this regime, the queueing delay increases sharply to $knh - \frac{m}{2\lambda h}$ and consensus delay would keep constant, and these consequences validates the previous analysis in Section IV. Since the confirmation delay includes queueing delay and consensus delay, we can see that the practical confirmation delay is close to the expected one when network load is light, and the performance gap becomes significant in heavy network load.

In Fig. 6 (b), we vary transmission delay h from 0.001 to 1 second with the fixed $\lambda = 25$. We can observe that the practical queueing delay becomes large with the increasing of h, the reason is that the higher transmission delay would cause the more new transactions to cache, which results in the higher queueing delay finally. This result is also matched with our previous analysis in (15). Moreover, we can see that queueing and consensus delay increase suddenly when $h = 0.512$ due to the boundary of network load. When $h < 0.512$, $nh\lambda$ is less than l, and thus all the new transactions waiting in the cache can be broadcast in single transmission. In contrast, when $h \geq 0.512$, $nh\lambda$ would be larger than m, and the cache becomes full to be heavy network load. In light network load, according to (15)-(17), we can know that the higher h would result in the higher ω'_a, and thus T'_a would be increased while T'_l declines. Meanwhile, since T'_l changes more quickly compared with T'_a and T'_q is very small, the practical confirmation delay T'_d declines with h when $h < 0.512$. In contrast, when network load becomes heavy ($h \geq 0.512$), the practical confirmation delay increases with h, this is because that T'_q increases significantly due to the deteriorated queueing delay. Additionally, we can also see that the expected queueing delay is always zero, the expected consensus and confirmation delay decrease with h due to no consideration of CSMA/CA.

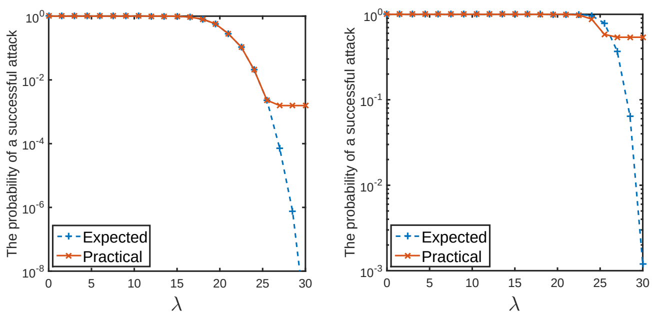
Similarly, we can see that the performance comparisons of TPS and transaction loss probability in Figs. 7 and 8, respectively. The network load condition is determined by λ and h, and thus affects the consensus process. When network load is light, the gap between the two curves is very small. TPS increases due to more new arrival transactions and transaction loss probability keeps zero. The reason is that the wireless network capacity is capable of new transactions broadcasting in this regime. However, when network load is heavy, the gap becomes significantly, this is due to the limitation of CSMA/CA that refrains the consensus process, and thus the practical TPS in WBN cannot improve as the expected pure blockchain system. Meanwhile, due to the cache becomes full finally, the new transactions cannot be stored any more, as a result, some of them would be lost.

In summary, from these experiments, we can see clearly that CSMA/CA in practical wireless network plays a significant role in consensus process in WBN. To be specific, the queuing delay plays a important role in the performance of WBN when network load is heavy. Otherwise, it is the weight accumulating delay when network load is light. Technically, the higher new transactions arrival rate can result in the smaller transaction



(a) The probability of a successful attack in $\lambda = 5$ (light network load)
(b) The probability of a successful attack in $\lambda = 30$ (heavy network load)

Fig. 9: The successful attack probability versus new transaction arrival rate of the attacker.



(a) The probability of a successful attack in $\mu = 10$ (light network load)
(b) The probability of a successful attack in $\mu = 30$ (heavy network load)

Fig. 10: The successful attack probability versus new transaction arrival rate of an honest user.

confirmation delay, which is a common opinion for DAG based blockchain [13]. In fact, considering the transmission capability of wireless network, we cannot afford a very high new transactions arrival rate, since the performance of WBN would be deteriorated if the network load condition across the limitation of transmission capability (like the jump point in these experiments).

B. Security Comparisons

Next, we examine the probability of the successful attack varying μ from 0 to 60 in LR with $\lambda = 5$. As shown in Fig. 9 (a), we can observe that the expected successful attacking probability increases with μ until it reaches 1. However, the practical successful attacking probability increases with μ, and tends to be steady about 2% when $\mu \geq 26.5$. Similarly, we can also observe that in Fig. 9 (b), the practical successful attacking probability increases when $\mu < 26.5$, and it keeps 1.3% with the increasing of μ after that. In contrast, the expected successful attacking probability gradually increases to 1 with μ. The rationale behind is that the maximum number of transactions broadcast by the attacker is limited by CSMA/CA that is m, which means the capability of launching an attack would be restrained due to the broadcasting limitation in wireless networks.

Last, we fix μ and vary λ to examine the probability of the successful attack as well. On the one hand, we can see that the expected successful attacking probability decreases with λ, since a higher λ can guarantee the security in pure DAG based blockchain system. On the other hand, in practical scenario, due to CSMA, the honest users cannot broadcast their issued new transactions as many as possible. As a result, the heavy network load in wireless networks cannot secure the DAG based blockchain system as the expectation claimed in [19].

According to the previous analysis in Section V, it is a common opinion that the higher new transactions arrival rate of honest users (that of attacker) can result in the higher (lower) security. However, through this work, we can know that the computational power of the honest users and attacker (i.e., the capability to issue the new transactions) would be limited by broadcast capability due to CSMA/CA in WBN. In summary, the security concern is jointly affect by the consensus in blockchain system and the transmission protocol in wireless networks.

VII. Related Work

In the last decades, there are a lot of research work to study CSMA/CA in wireless networks. In [16], the author proposes a simple and accurate system model to analyze the throughput using CSMA/CA scheme assuming a finite number of terminals and ideal channel conditions. In [20], Ni *et al.* extend the analysis model proposed in [16] to investigate the saturation throughput performance achieved at the MAC layer, in both congested and error-prone channels. Considering unsaturated traffic conditions, the authors in [21] use the traditional M/G/1 queueing model for CSMA/CA to analyze its unsaturated throughput performance.

Nowadays, several DAG based consensus protocols are proposed. In [22], Byteball is a decentralized system that allows tamper proof storage of arbitrary data, including data of social value such as money. The difference is that the transaction fee is collected by other users who later confirm the newly added unit in this consensus compared to tangle. Hashgraph is proposed for replicated state machines with guaranteed Byzantine fault tolerance in [23]. The participants build distributed ledger for recording each transaction based on a gossip protocol, and Byzantine agreement to be achieved through virtual voting.

In order to provide some insightful understandings of blockchain in a mathematical manner, some analytical models have been proposed recently. In [24], the authors analyze the impact of the block dissemination delay and the forking security on wide area network, and show a balance between the adjustment of the working difficulty target value and the defense of the adversarial attack. As a previous work, we investigate the impact of network load on the blockchain performance and security in [19]. Considering unsteady network load, we first propose a Markov chain model to capture the behavior of DAG consensus process under dynamic load conditions, and leverage a stochastic model to analyze the probability of a successful double-spending attack in different network load regimes. Moreover, in [11], we introduce serval consensus protocols in details and illustrate some challenges in applying consensus protocols to IoT on the perspectives of communications and networks. In [25], we propose an analytical model for the blockchain-enabled wireless IoT system to analyze the performance of communication and blockchain. According to performance analysis, we design an algorithm to determine the optimal node deployment to maximize transaction throughput.

However, these related work have not fully considered the limitation of the underlying wireless network, and no research focuses on the performance and security analysis on the perspectives of blockchain system and wireless network simultaneously. To the best of our knowledge, it is the first time to mathematically analyze and discuss the performance and security in the practical wireless scenarios considering the impact of CSMA/CA.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, the impact of CSMA/CA on a typical DAG based wireless blockchain network is investigated. We first analyze the blockchain performance in terms of confirmation delay, TPS and transactions loss probability, and study the probability of launching the successful double-spending attack in a wireless connected scenario. By identifying two network load regimes in CSMA/CA based WBN, we draw conclusions that the performance of WBN and the computational power of all users (whether honest or malicious) is both limited by transmission capability. Different from the conclusions in previous work that only consider the overlaid blockchain system ignoring the transmission on underlaid wireless network, analysis and simulation results provide an insightful understanding in WBN, we find that the claimed dramatic performance of DAG based blockchain is constrained in wireless network significantly, and the WBN based security is also affected obviously due to the limitation of transmission capacity.

This paper clearly indicates that communication protocol plays an important role in the blockchain performance and security. Therefore, to design efficient and safe blockchain system, researcher should make a balance between communication and consensus protocols in the future. In addition, some voting based consensus protocols such as Raft and PBFT need massive information/traffic exchange, the additional overhead should be further considered especially in wireless communications. Meanwhile, unlike DCF studied in this paper, the point coordination function (PCF) is also the basic MAC mechanism and how does it affect the blockchain system is another interesting but unaddressed topic.

REFERENCES

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[2] L. C. C. De Biase, and *et al.*, "Swarm Economy: A Model for Transactions in a Distributed and Organic IoT Platform," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4561-4572, June 2019.

[3] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: a Lean approach for designing real-world use cases," in *IEEE Access*, vol. 6, pp. 62018-62028, Oct. 2018.

[4] X. Liang, J. Zhao, and *et al.*, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," In *Proceedings of the IEEE 28th Annual International Symposium on PIMRC*, Oct. 2017.

[5] Z. Li, J. Kang, and *et al.*, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690-3700, Aug. 2018.

[6] IBM Institute for Business Value, "Device democracy: saving the future of the Internet of Things," 2015. [Online]. Available: https://www.ibm.com/services/us/gbs/thoughtleadership/internetofthings/.

[7] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," White paper, 2009. [Online]. Available:https://bitcoin.org/bitcoin.pdf.

[8] V. Buterin, "A next-generation smart contact and decentraliaed application platform," White paper, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[9] S. D. Lerner, "Dag Coindraft," 2015. [Online]. Available:https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf.

[10] G. BitFury, "Proof of stake versus proof of work," White paper, Sep. 2015.

[11] B. Cao, Y. Li, and *et al.*, "When Internet of Things meets blockchain: challenges in distributed consensus," accepted by *IEEE Network*, Early Acess, pp. 1-7, July. 2019.

[12] Y. Li, Y. Du, B. Cao, and X. H. You, "Cooperative MAC for wireless networks," *Journal of Software*, vol. 22, no. 1, pp. 101-114, Mar. 2011.

[13] S. Popov, "The tangle," White paper, 2018. [Online]. Available: https://www.iota.org/research/academic-papers.

[14] P. Huang, C. Chang, and *et al.*, "Recursive Constructions of Parallel FIFO and LIFO Queues With Switched Delay Lines," in *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1778-1798, May 2007.

[15] S. M. Ross, "Introduction to Probability Models," Academic Press, 2014. 11th edition.

[16] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," in *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, March 2000.

[17] M. Rosenfeld, "Analysis of hashrate-based double-spending," 2014. [Online]. Available: https://arxiv.org/pdf/1402.2009.pdf.

[18] Philip Staupe, "Quasi-Analytic Parasite Chain Absorption Probabilities in the Tangle, vol. 20, no. 3, pp. 15-18, 31 Dec 2017.

[19] Y. Li, B. Cao, and *et al.*, "Direct acyclic graph based blockchain for Internet of Things: performance and security analysis," 2019. [Online]. Available: https://arxiv.org/abs/1905.10925.

[20] Q. Ni , Li T, and *et al.*, "Saturation throughput analysis of error-prone 802.11 wireless networks." *Wireless Communications & Mobile Computing*, vol. 5, no. 8, pp. 945-956, 2005.

[21] Lee. Wookwon , C. Wang , and K. Sohraby, "On use of traditional M/G/1 model for IEEE 802.11 DCF in unsaturated traffic conditions," *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, Las Vegas, NV, 2006, pp. 1933-1937.

[22] A. Churyumov, "Byteball: a decentralized system for storage and transfer of value," White paper, 2016. [Online]. Available: https://byteball.org/Byteball.pdf.

[23] L. Baird, "The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance," White paper, 2016. [Online]. Available: http://www.swirlds.com/developer-resources/whitepapers/.

[24] N. Papadis, S. Borst, and *et al.*, "Stochastic models and widearea network measurements for blockchain design and analysis," In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, Honolulu, USA, Apr. 2018.

[25] Y. Sun, L. Zhang, and *et al.*, "Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment," in *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 5791-5802, June 2019.

BIN CAO is an associate researcher in the Institute of Network Technology at Beijing University of Posts and Telecommunications. Before that, he was an associate professor at Chongqing University of Posts and Telecommunications. He received his Ph.D. degree (Honors) in communication and information systems from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China in 2014. From April to December in 2012, he was an international visitor at the Institute for Infocomm Research (I2R), Singapore. He was a research fellow at the National University of Singapore from July 2015 to July 2016. He also served as symposium cochair for IEEE ICNC 2018, workshop cochair for CyberC 2019 and TPC member for numerous conferences. His research interests include blockchain system, internet of things and mobile edge computing.

MENGYANG LI received the M.E degree in information and communication engineering from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2021. He currently is pursuing his Ph.D. degree at School of Electronic Information and Communications, the Huazhong University of Science and Technology, Wuhan, China. His research interests include blockchain and wireless communication.

LEI ZHANG (SM'18) received his Ph.D. from the University of Sheffield, U.K. He is now a Lecturer at the University of Glasgow, U.K. His research interests broadly lie in the Communications and Array Signal Processing, including radio access network slicing (RAN slicing), wireless blockchain systems, new air interface design, Internet of Things (IoT), multi-antenna signal processing, massive MIMO systems, etc. He is holding 16 US/UK/EU/China granted parents on wireless communications. Dr Lei Zhang also holds a visiting position in 5GIC at the University of Surrey. He is an associate editor of IEEE ACCESS and a senior member of IEEE.

YIXIN LI received the M.E degree in information and communication engineering from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2020. He currently is pursuing his Ph.D. degree at the Institute of Network Technology, the Beijing University of Posts and Telecommunications of China, Beijing, China. His research interests include blockchain and internet of things.

MUGEN PENG (M'05, SM'11) received the Ph.D. degree in communication and information systems from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2005. Afterward, he joined BUPT, where he has been a Full Professor with the School of Information and Communication Engineering since 2012. During 2014 he was also an academic visiting fellow at Princeton University, USA. He leads a Research Group focusing on wireless transmission and networking technologies in BUPT. He has authored and coauthored over 90 refereed IEEE journal papers and over 300 conference proceeding papers. His main research areas include wireless communication theory, radio signal processing, cooperative communication, self-organization networking, heterogeneous networking, cloud communication, and Internet of Things.

Dr. Peng was a recipient of the 2018 Heinrich Hertz Prize Paper Award, the 2014 IEEE ComSoc AP Outstanding Young Researcher Award, and the Best Paper Award in the JCN 2016, IEEE WCNC 2015, IEEE GameNets 2014, IEEE CIT 2014, ICCTA 2011, IC-BNMT 2010, and IET CCWMC 2009. He is currently or have been on the Editorial/Associate Editorial Board of the *IEEE Communications Magazine, IEEE ACCESS, IEEE Internet of Things Journal, IET Communications, and China Communications*.