Blockchain-Aided Access Control for Secure Communications in Ad Hoc Networks

Mingming Wu(✉), Yulan Gao, and Yue Xiao

National Key Laboratory of Science and Technology on Communications,
University of Electronic Science and Technology of China, Chengdu 611731, China
mingmingwuuestc@163.com, yulanggaomath@163.com, xiaoyue@uestc.edu.cn

Abstract. A novel blockchain technology aided peer-to-peer connection (P2P)-based access control protocol is proposed for the distributed ad hoc networks. More specifically, the access process conceived can improve the security performance as an explicit advantage of blockchain technology, which is capable of preventing from the security threatens, e.g., being eavesdropped, being tampered, and malicious access imposed by the lack of the authentication center and the nature of the multi-hop routing. Meanwhile, a reasonable punishment mechanism is integrated into the access protocol that reinforces punishment upon the increase of dishonest or malicious node behaviors and hence, is particularly beneficial for the robustness of the long-term systems. Furthermore, a low-complexity match scheme based on competition access (MCA) is utilized for designing the appropriate multi-hop routings, which considers the min-max delay optimization objective. Numerical results demonstrate that the blockchain-aided access control protocol achieves the lower delay in comparison to the conventional first come, first serve access scheme, random access scheme, and the single-hop access scheme, while improving the security performance of access process in ad hoc networks.

Keywords: Ad hoc networks · Blockchain · Access control · Secure communications

1 Introduction

With thebibliography proliferation of the mobile terminals and the required data [1], ad hoc networks based on peer-to-peer connection and supporting the dynamic topology and self-organization characteristics has attracted extensive research interests in military communications and the industry fields [2]. This is because ad hoc network as an infrastructureless network architecture can improve the robustness and transmission performance without increasing the burden of the base station or other central controllers. More specifically, ad hoc networks can be an independent network architecture, applied to the distributed system [3,4], e.g., wireless sensor network (WSN), vehicular ad hoc

J. Zheng et al. (Eds.): ADHOCNETS 2019, LNICST 306, pp. 87–98, 2019.
https://doi.org/10.1007/978-3-030-37262-0_7

network (VANET), and emergency communications. On the other hand, ad hoc networks can also assist the centralized network [5,6], e.g., the D2D-assisted cellular mobile network, internet of things (IoT), to expand the coverage area, offload the network loads, and improve the performance of devices on the edge of networks. However, in addition to the mentioned advantages, ad hoc networks easily suffer from hostile attacks, e.g., being eavesdropped, being tampered, and malicious access due to the lack of the authentication center and the nature of the multi-hop routing.

To deal with such security risks, it is beneficial to employ effective distributed access control protocols in ad hoc networks [7]. Recently, blockchain as a novel decentralized protocol has gained substantial attention due to its high security performance, owing to the integration of the advanced storage structure, encryption algorithms, and consensus mechanisms [8]. More specifically, blockchain constructs a distributed database shared among nodes that includes data into transactions, stores transactions into blocks, and connects blocks in the form of a chain. Moreover, asymmetric encryption algorithms guarantee the integrity and confidentiality of transactions, and the related consensus mechanisms e.g., proof of work (PoW) and proof of stake (PoS), prevent information recorded in blocks from being tampered. However, the high security performance of blockchain is achieved at the cost of a high delay and a high computation complexity imposed by generating and verifying blocks, which can be tolerated in the field of digital currency but may become particularly challenging in certain communication scenarios, requiring low delays or having limited computation resources. Following this line, [9] proposed a novel blockchain structure called 'Prism', for reducing the delay to the communicable level by deconstructing the entire process into different sub-modules.

Motivated by both the benefits and limitations of ad hoc networks and blockchain technologies, in this paper, we conceive a blockchain-aided access control protocol for ad hoc networks, which is capable of improving the security performance with a tolerable delay level. More specifically, access requests containing the embedded state information are stored in blocks, which allows us to compare the request contracts with the executive results, thereby, punishing the dishonest or malicious node behaviors, with the aid of a reasonable punishment mechanism. Meanwhile, the PoS consensus mechanism is invoked for the balance between the security and delay, with the optimization of the number of alternative relays and verified blocks. Furthermore, a match scheme based on competition access (MCA) is proposed for the design of multi-hop routings, which attains appreciable system delay performance at a low complexity.

The remainder of this paper is organized as follows. In Sect. 2, we detail the system model, which includes the introductions of relay forwarding process and the descriptions of blockchain-aided access control structure. In Sect. 3, the access control problem is formulated into an integer programming model, which considers min-max system delay as the optimization objective. A low-complexity match scheme is proposed for designing multi-hop routings in Sect. 4. Section 5 shows numerical results, which validates the effectiveness and superiority of the proposed scheme. Finally, we conclude in Sect. 6.

2 System Model

Considering an ad hoc network scenario, where several wireless terminals have the requirement of data transmission, denoted as the set of source nodes $S = \{s_1, s_2, \ldots, s_N\}$ and let $D = \{d_1, d_2, \ldots, d_N\}$ as the set of the corresponding destination nodes. We assume that the communication link between nodes is based on P2P connections without the aid of the base station or any access points. Thus, when the source nodes are far away from the destination nodes, the multi-hop transmission mode needs to be employed, and the potential relay nodes set is defined as $R = \{r_1, r_2, \ldots, r_M\}$. To avoid the mutual interference, we assume that different nodes occupy independent bandwidth and the relay forward mode is amplify-and-forward (AF).

2.1 Relay Forwarding

Under the assumption of a multi-hop transmission scenario, we further consider that the connections between source nodes and relay nodes are one-to-one, i.e., each source node only chooses one relay node to forward data at the same time, while a destination node can receive different messages from multiple relay nodes. For simplicity, consider two-hop transmission as the typical example of the multi-hop transmission. The relay rate of two-hop transmission can be expressed as

$$R_{ij} = 0.5B\log(1 + SNR_{ij}), \forall s_i \in S, r_j \in R, d_{\tilde{i}} \in D, \tag{1}$$

where we have

$$SNR_{ij} = \frac{p_i^s p_j^r h_{ij} h_{j\tilde{i}}}{N_0(p_i^s h_{ij} + p_j^r h_{j\tilde{i}} + N_0)}, \tag{2}$$

where p_i^s, p_j^r are the transmit power of the source nodes and the forward power of the relay nodes, respectively, $h_{ij}, h_{j\tilde{i}}$ represent the channel coefficients between the source nodes and the relay nodes, and the relay nodes and the destination nodes respectively, N_0 is the power of the background noise, B is the channel bandwidth. Note that, coefficient 0.5 is attributed to the effect of the two-hop transmission.

The rate of the single-hop transmission is given by

$$R_{i\tilde{i}} = B\log(1 + \frac{p_i^s h_{i\tilde{i}}}{N_0}), \forall s_i \in S, d_{\tilde{i}} \in D, \tag{3}$$

where $h_{i\tilde{i}}$ is the channel coefficient between the source nodes and the relay nodes. When sending a data package whose size is Q, the transmission delay can be derived by

$$T_i^{\text{trans}} = \sum_{j=\tilde{i},1}^{M} x_{ij} \frac{Q_i}{R_{ij}}, \tag{4}$$

subject to

$$\sum_{j=\tilde{i},1}^{M} x_{ij} = 1, \sum_{i=1}^{N} x_{ij} = 1, \qquad (5)$$
$$x_{ij} \in \{0,1\}, \forall s_i \in S, r_j \in R, d_{\tilde{i}} \in D,$$

where x_{ij} represents the factor of transmission mode selection and relay node allocation, defined as

$$x_{ij} = \begin{cases} 1, \text{if } s_i \text{ choose } r_j \text{ or single-hop}(j = \tilde{i}) \\ 0, \text{otherwise} \end{cases} . \qquad (6)$$

In addition to the transmission delay, another kind of delay is the process delay, defined as the delay of processing access requests for the destination node. Because the size of access requests is small, the difference of the transmitting access delays between various nodes can be ignored, thus, the process delay is given by

$$T_i^{\text{proc}} = (t_{\text{Tr}} + t_{\text{Proc}})N_i^{\text{relay}}, \forall s_i \in S, \qquad (7)$$

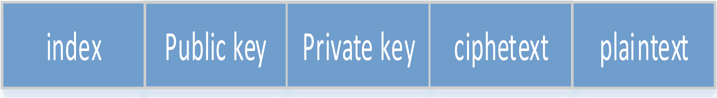
where the constant $t_{\text{Tr}} + t_{\text{Proc}}$ represents the sum of the transmission delay and the process delay of each access request, N_i^{relay} is the number of alternative relay nodes for s_i, ranging from 1 to $M + 1$ (include the single-hop mode). Although the relay node with the best channel condition may be found, when $d_{\tilde{i}}$ receives the access signals from all the relay nodes, the process delay will increase upon the increase of N_i^{relay}.

Due to the randomness of the channel and the mobility of nodes, the system state is not stationary. Thus, the source nodes need to choose and update the transmission modes and relay nodes dynamically, according to the self-demands and system states.

2.2 Blockchain-Aided Access Control

Ad hoc networks without the authentication center are inclined to secure risks, e.g., being eavesdropped, being tampered and malicious access of unauthorized nodes. Thus, for the sake of security performance, effective distributed protocols are needed for secure communications in ad hoc networks. Blockchain as a novel P2P-based decentralized protocol that integrates the specialized storage structure, advanced encryption algorithms and consensus mechanisms, can guarantee reliable, secure information transmissions and records in a distributed network. However, high delay imposed by generating and verifying blocks restricts the applications of blockchain technology in practical communications.

To weaken the influence of blockchain technology on the communication delay, only the part of the access request contracts and the executive results are included into blocks, excluding the transmission data Q out of blocks considering the timeliness of data. A transaction consists of the node states (location,



index	Public key	Private key	ciphetext	plaintext

Fig. 1. The general structure of a transaction in the blockchain.

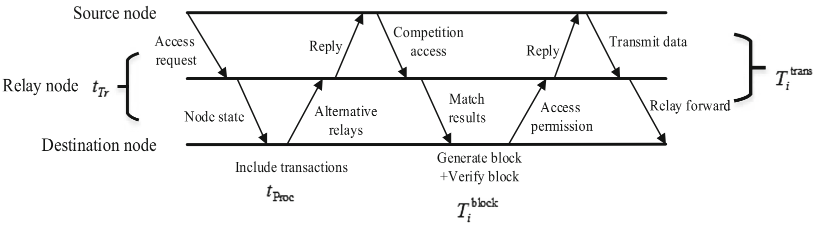


Fig. 2. The general process of the blockchain-aided access control.

achievable rate, power..), the results of multi-hop routings, etc., and its general structure is as shown in Fig. 1.

Such reduction of transaction data contributes to the decrease of the delay and the required storage resources. Moreover, another kind of delay imposed by generating and verifying blocks can be given by

$$T_i^{\text{block}} = t_{\text{generate}} N_i^{\text{verify}}, \forall s_i \in S, \tag{8}$$

where t_{generate} represents the delay of generating a block, N_i^{verify} is the required number of the verified block. To guarantee the security of the storage information in the blockchain, the delay of verifying blocks T_i^{block} needs to be waited before forwarding data Q_i and more verified blocks lead to the higher security but the higher delay. Thus, the size of N_i^{verify} is a key parameter to balance the security and the delay in the blockchain-aided ad hoc networks.

The process of the blockchain-aided secure access control is described as Fig. 2. Firstly, the source nodes transmit the access requests with state information. Next, the relay nodes that receive request signals decide whether to provide relay services and forward the signals to the destination nodes attached with itself information (power, location, trajectory, etc.). Then, the destination node $d_{\tilde{i}}$ chooses N_i^{relay} alternative nodes and founds an appropriate routing path for the corresponding source node, according to the proposed match scheme. Afterwards, the match results as a part of transactions are included into blocks and are broadcasted to the whole network. Finally, after the delay of verifying blocks, the source nodes set up the single-hop or multi-hop routing path with the destination nodes according to the match results and start to forward data.

3 Problem Formulation

Considering the mobility of nodes and the randomness of the channel, the performance of the long-term dynamic system is investigated by introducing the definition of frame. A frame τ of s_i is from the beginning of sending access requests to the ending of the $Q_i[\tau]$ data transmission, the length of frame is given by

$$T_i[\tau] = T_i^{\mathrm{trans}} + T_i^{\mathrm{proc}} + T_i^{\mathrm{block}}, \forall s_i \in S. \tag{9}$$

To deal with security threatens imposed by the unauthorized or dishonest nodes, the credibility of nodes is defined as the measure of the reliability, which is given by

$$c_j = \frac{1}{r}\sum_{\tau=1}^{r} w_j[\tau], \forall r_j \in R, \tag{10}$$

where $w_j[\tau]$ represents the comparison between the contracts recorded in the block and the executive results, which are both recorded in the blockchain and can not be modified. Thus, the destination nodes can verify the consistency of the provided request contracts and the real results, such as rate, power, etc., $w_j[\tau]$ is defined by

$$w_j[\tau] = \begin{cases} 1, \text{if contracts match executive results} \\ 0, \text{otherwise}, \forall r_j \in R \end{cases}. \tag{11}$$

Based on the credibility of nodes, the punishment mechanism for the dishonest or malicious behaviours is represented by

$$\tilde{p}_j^r[\tau] = c_j p_j^r[\tau], \forall r_j \in R, \tag{12}$$

where $\tilde{p}_j^r[\tau]$ is the destination nodes estimation of r_j power, i.e., if the dishonest nodes break the contract time after time, it will lose the competitiveness of relay access services due to the decrease of relay rate in (1), thereby, the security of the long-term system can be enhanced further.

The system utility function is given by

$$\begin{aligned} &\min_{x_{ij}[\tau]}\max \ \{T_i[\tau], \forall s_i \in S\}, && (13.a) \\ s.t. &\sum_{j=\tilde{i},1}^{M} x_{ij}[\tau] = 1, \sum_{i=1}^{N} x_{ij}[\tau] = 1, && (13.b) \\ &x_{ij}[\tau] \in \{0,1\}, \forall s_i \in S, r_j \in \tilde{R}_i, d_{\tilde{i}} \in D. && (13.c) \end{aligned} \tag{13}$$

Such optimization model is an integer programming problem, where $\tilde{R}_i$ is a subset of R, whose element includes the N_i^{relay} alternative relay nodes for the source node s_i. The constraints guarantee the one-on-one match between the source nodes and relay nodes.

4 Proposed Algorithm

The above integer programming is an NP-hard problem with complexity $O(M!)$. On the other hand, the optimization model can be considered as a node matching problem and the match priority function is defined as $T_i[\tau]$, i.e., the nodes with the lower delay have the higher priority. To simplify the notation, the sing-hop mode is seen as the special relay node, whose node number is denoted as 0. Thereby, the priority list of the source node s_i consists of $N_i^{\text{relay}} + 1$ node number, the elements of which are arranged from high to low priority. Assuming all of the source nodes have the same number of alternative relay nodes $N_i^{\text{relay}} = N_{\text{relay}}, \forall s_i \in S$, and the $N \times (N_{\text{relay}} + 1)$ priority matrix is consisted of the preference profile of each source node.

After converting the integer programming into the node matching problem, the problem is not still solved due to the required central structure and the $O(M!)$ complexity when implementing the optimal match algorithm. To solve the above problem in a distributed ad hoc network and at a lower complexity, a suboptimal match algorithm based on competition access (MCA) is proposed. Its main idea is that the source nodes choose the preferred node number according to the priority firstly, which will lead to node collision, when different source nodes choose the same relay node. Then, to avoid the collisions, the relay nodes employ the competition access scheme, where the relay node choose to forward data of the source node having the higher delay based on the consideration of the min -max system utility function. In priority matrix operations, that is, corresponding row of the source node having lower delay rotates left. The details of the MCA algorithm is shown in Algorithm 1.

Note that, MCA does not require the global information, thus, it can be applied to the distributed systems. Moreover, because the node collision will not happen when the different source nodes choose the same number of the node 0 (the single-hop mode), the complexity of the MCA is controlled in $O(N_{\text{relay}}N^2)$. With the number of alternative relay nodes increases, the probability of node collision decreases, thereby the performance of the proposed algorithm can be improved further.

5 Numerical Results

To investigate the performance of the proposed blockchain enabled structure in ad hoc networks, we simulate the system utility value under different parameter settings. And to verify the validity and the advantages of the proposed scheme, the MCA algorithm is compared with the other three schemes: the traditional access scheme (TA), the random access scheme (RA), the only single-hop scheme (SH). More specifically, the TA scheme adopts the rule of first come, first serve, that is, the source node with the higher instantaneous rate can obtain the prior access to the required relay node. And the SH scheme ignores the block delay T_i^{block} due to that the lack of information interactions can avoid certain security threats.

Algorithm 1. The proposed match algorithm based on competition access

```
Input:
  $T_i, N_{\text{relay}}, N$
Output:
  the match results $x_{ij}$
  for each source node $s_i$ do
    Choose $N_{\text{relay}}$ relay nodes and sort the priority according to $T_i$;
  end for
  Construct the priority matrix, the first column as the initial match results;
  for $t = 1$; $t < N_{\text{relay}}$;$t++$ do
    for $i = 1$; $t < N$;$i++$ do
      Compare with other node selection;
      if $x_{ij} == x_{i' j}$&&$j \neq 0$ then
        node collision happens, then
        if $T_i > T_{i'}$ then
          Rotate left the row corresponding to $i$;
        else
          Rotate left the row corresponding to $i^{'}$;
        end if
      end if
    end for
  end for
  return the first column as the final match results.
```

In the simulation environment setting, the node mobile model adopts Gaussian-Markov Mobile Model (GMMM) [10], with log-normal shadowing and Rayleigh fading. Without loss of generality, all of the source nodes have the same number of the alternative relay nodes, the required verified blocks and the transmit power, denoted as $N_i^{\text{relay}} = N_{\text{relay}}, N_i^{\text{verify}} = N_{\text{verify}}, p_i^s = P_{\max}^s, \forall s_i \in S$, and all of the relay nodes have the same maximum transmit power $P_{\max}^r$. If not specifically indicated, other parameter settings are as follows: the carrier frequency $f_0 = 2.3\,\text{GHz}$, $B = 0.18\,\text{MHz}$, $P_{\max}^s = 23\,\text{dBm}$, the data size of each frame $Q_i[\tau]$ is subjected to poisson distribution with the mean 1000 kbps, the power spectral density of background noise N_0 is $-174\,\text{dBm/Hz}$, $t_{\text{Tr}} + t_{\text{Proc}} = 0.01\,\text{s}$, $t_{\text{generate}} = 0.5\,\text{s}$.

Figure 3 shows the combined influence of the number of alternative relay nodes and the required verified blocks on the performance of average system delay. It can be observed that as the number of alternative relay nodes N_{relay} increases, the average system delay firstly decreases and then increases slightly, which is attributed to that the smaller number of alternative relay nodes leads to the higher probability of node collision. Thereby, when the number of alternative relay nodes is lower than the number of source nodes ($N_{\text{relay}} < 5$), more source nodes will choose the single-hop mode based on MCA, which results in the higher average system delay. For the sake of the slight increase of the system delay, the increase of the process delay T_i^{proc} with N_{relay} can explain such trend. In addition, more verified blocks can improve the security but incur significant

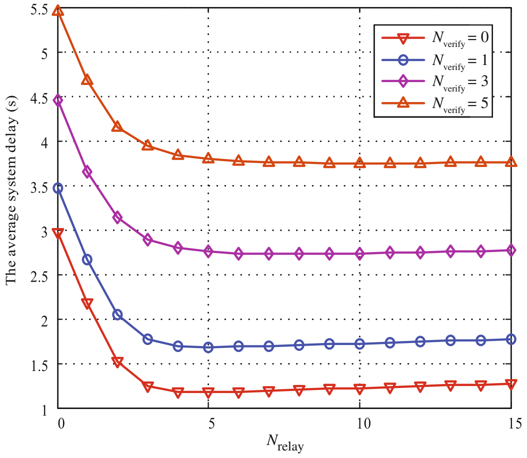


Fig. 3. The average system delay versus N_{relay} under different N_{verify}.

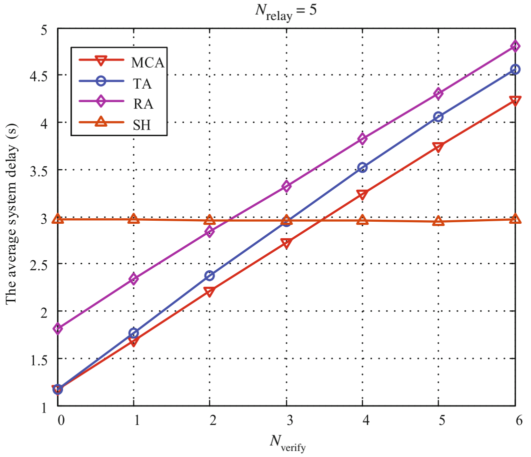


Fig. 4. The comparison of the average system delay of different schemes versus N_{verify}.

delay increase. The number of the verified blocks has important effects on the balance between the security and the delay due to the considerable block delay T_i^{block}, which needs further researches.

Figure 4 compares the delay performance of different schemes versus the number of verified blocks. In general, the SH scheme has the higher delay compared to other three schemes when N_{verify} is small. Then, with the N_{verify} continuing to increase, the delay performance of the SH exceeds other three schemes because of the lack of the block delay. However, it should be pointed out that the impact of block delay on the system delay will be weaken as the data size $Q_i[\tau]$ increases, which can be observed in the following simulations. Besides, the difference of the

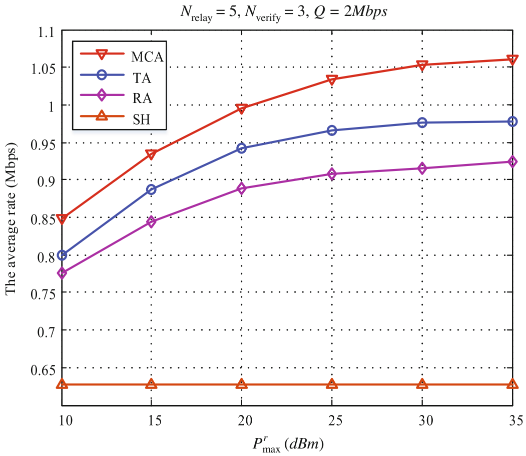


Fig. 5. The comparison of the rate performance of different schemes versus the maximum relay power.

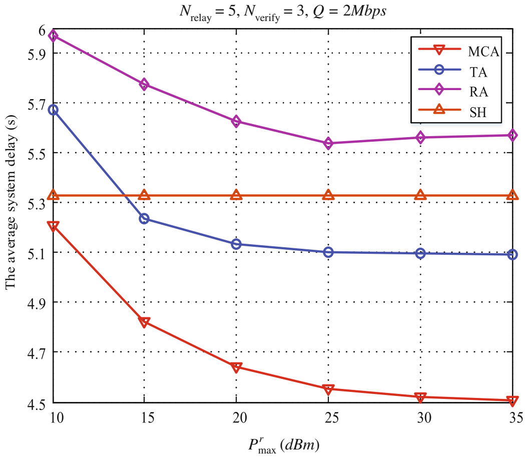


Fig. 6. The comparison of the delay performance of different schemes versus the maximum relay power.

delay between the MCA and the TA scheme gradually grows with the increasing N_{verify}. The reason is that the TA based on the access rule of first come, first serve, only considers the instantaneous rate and ignore the influence of dynamics introduced by the channel randomness, terminal mobility and the data fluctuation, etc., which can be included into the transactions in the MCA scheme. Thus, with the higher waiting time of the block delay, the performance of the TA deteriorates gradually, ultimately close to the RA scheme.

To investigate the rate performance and the delay performance of the different schemes versus the relay node power, the results are shown in Figs. 5 and 6, respectively. Note that, different from the $Q_i[\tau]$ setting in Figs. 3 and 4, the data size in Figs. 5 and 6 is double to show its weakening effect on the role of the block delay in the system delay. We can observe that the rate performance of the multi-hop scheme is superior to the SH scheme and the proposed MCA scheme has the best rate performance. In addition, the TA scheme has the better rate performance than the RA scheme. Although the SH has the worst rate performance, its system delay performance is better than the TA and the RA scheme when the relay power is lower or the data size is smaller, due to the lack of the block delay. Combined Fig. 4 with Fig. 6, it can be observed that with the higher relay power or larger data size, the role of block delay in the system delay is weaken gradually. Consequently, the delay performance of the TA scheme and the MCA scheme exceeds the SH scheme. In general, the proposed MCA scheme has better performance in both delay and rate compared with other schemes, particularly beneficial for larger data and higher relay power scenario.

6 Conclusions

For secure communications in ad hoc networks, we proposed a novel blockchain-aided access control protocol, which integrates the blockchain technology into the multi-hop access process. And the related punishment mechanism was introduced to prevent the access to the dishonest or malicious nodes. Meanwhile, the influences of the number of alternative nodes and the required verified blocks on the system performance were investigated to balance the security and the delay. Furthermore, a low-complexity match scheme based on competition access was proposed to design reasonable routing paths for different source nodes, which minimizes the maximum delay. Numerical results demonstrated that the proposed scheme has significant advantages in the delay performance compared to other conventional access schemes, while improving the security performance in ad hoc networks.

Acknowledgements. This work was supported in part by the National Science Foundation of China under Grant number 61671131, the Fundamental Research Funds for the Central Universities (No. ZYGX2018J092), and Sichuan Science and Technology Program (2018HH0138).

References

1. Chen, S., Zhao, J.: The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication. IEEE Commun. Mag. **52**(5), 36–43 (2014)
2. Royer, E.M., Toh, C.-K.: A review of current routing protocols for ad hoc mobile wireless networks. IEEE Pers. Commun. **6**(2), 46–55 (1999)
3. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)

4. Hartenstein, H., Laberteaux, L.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
5. Akyildiz, I.F., Wang, X.: A survey on wireless mesh networks. IEEE Commun. Mag. **43**(9), S23–S30 (2005)
6. Borgia, E.: The internet of things vision: key features, applications and open issues. Comput. Commun. **54**, 1–31 (2014)
7. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Netw. **13**(6), 24–30 (1999)
8. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
9. Bagaria, V., Kannan, S., Tse, E.A.D.: Deconstructing the blockchain to approach physical limits (2018). https://arxiv.org/abs/1810.08092v1
10. Gao, Y., Xiao, Y., Wu, M., Xiao, M., Shao, J.: Dynamic social-aware peer selection for cooperative relay management with D2D communications. IEEE Trans. Commun. **67**(5), 3124–3139 (2019)