International Journal of Advanced Smart Convergence Vol.8 No.4 169-178 (2019)
http://dx.doi.org/10.7236/IJASC.2019.8.4.169

IJASC 19-4-21

Node-Level Trust Evaluation Model Based on Blockchain in Ad Hoc Network

Shuai-ling Yan[1,2] and Yeongjee Chung[3*]

[1]M.S., Assistant Professor, Department of Mathematics and Computer Science, Hengshui University, Hengshui 053000, China.
E-mail: yanshuailing@163.com
[2]Ph.D., Program, Department of Computer and Software Engineering, Wonkwang University, Iksan 54538, Korea
[3]Ph. D., Professor, Department of Computer and Software Engineering, Wonkwang University, Iksan 54538, Korea
E-mail: yeongjee@gmail.com

Abstract

Due to the characteristics of an ad hoc network without a control center, self-organization, and flexible topology, the trust evaluation of the nodes in the network is extremely difficult. Based on the analysis of ad hoc networks and the blockchain technology, a blockchain-based node-level trust evaluation model is proposed. The concepts of the node trust degree of the HASH list on the blockchain and the perfect reward and punishment mechanism are adopted to construct the node trust evaluation model of the ad hoc network. According to the needs of different applications the network security level can be dynamically adjusted through changes in the trust threshold. The simulation experiments demonstrate that ad-hoc on-demand distance vector(AODV) Routing protocol based on this model of multicast-AODV(MAODV) routing protocol shows a significant improvement in security compared with the traditional AODV and on-demand multipath distance vector(AOMDV) routing protocols.

Keywords: *Ad hoc network, blockchain, node-level trust evaluation, trust degree, reward and punishment mechanism.*

1. Introduction

An ad hoc network is a multi-hop, centerless, self-organizing wireless network, and there is no fixed infrastructure to support it [1, 2]. Each node in such a network is provided with information processing and forwarding functions. The communication is achieved by a direct coverage of the wireless signal or forwarded by other nodes. As shown in Figure 1, the communication can be accomplished directly between the nodes 1 and 3, while nodes 3, 4, and 6 are required to forward the packets when node 1 connects to node 8.

The trust model, which involves finding and traversing the trust path when establishing trust relationships

Manuscript Received: November. 17, 2019 / Revised: November. 24, 2019 / Accepted: November. 29, 2019
*Corresponding Author: yeongjee@gmail.com (Yeongjee Chung)
Tel: +82-63-850-6887, Fax: +82-63-856-8009
Professor, Department of Computer and Software Engineering, Wonkwang University, Iksan 54538, Korea

and verifying certificates, is an important concept in the public key infrastructure(PKI) principle. It originated from the subjective trust model proposed by the author in 1994[2]. Since then, a large number of trust evaluation models have been established by the researchers.

2. Related works

A method is proposed to calculate the local and global reputation ratios by establishing a node confidence factor function [3], which could judge the trust reliability of the nodes. A finite state machine is used to dynamically model the neighbors of evaluated nodes in a P2P network [4]. To solve network interference in an ad hoc network, essentially caused by abnormal behaviors such as selfishness and non-cooperation of nodes, Guidance and incentive measures are applied to handle selfish nodes during the trust evaluation of the nodes [2, 5-7], and the network nodes were divided into trsted and untrusted nodes.

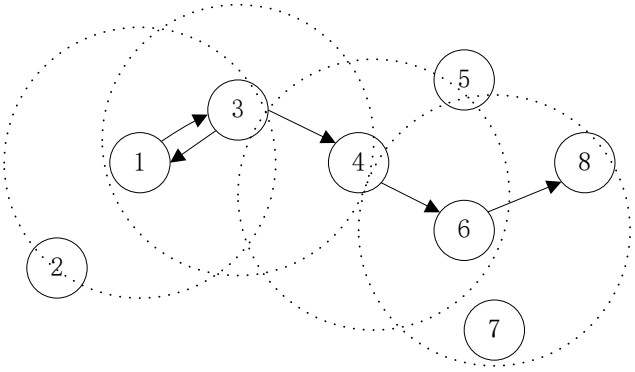

Figure 1. Ad hoc network node communication structure

In summary, numerous node-level trust evaluations have been researched from different aspects till date. However, looking at the comparisons, some problems still exist in some researches, such as, the evaluation parameters are too simple, due to which the degree of discrimination is not obvious; the evaluation algorithms are unsuitable for mobile networks because of the high time complexity; and trust evaluation models are too rigid to be dynamically adjusted. To solve the mentioned problems, a blockchain-based node security trust evaluation model is proposed based on the analysis of an ad hoc network and the blockchain technology. The node trust degree of the HASH list on the blockchain and the perfect reward and punishment mechanism are adopted to construct the node trust evaluation model of the Ad hoc network. According to the requirements of different applications, the network security level can be dynamically adjusted by changing the trust threshold.

3. Basic theory of node trust evaluation in ad hoc network

3.1 P2P-like networking of ad hoc networks

To allow the application of the mature node trust evaluation theories used in P2P networks [8, 9] to our ad hoc network, a P2P-like network is proposed. A P2P-like network is composed of a node j and its neighboring nodes as a module in the ad hoc network; in this module, at least one link ending at the node j is capable of enabling sequential communication. Therefore, the ad hoc network can be seen as a combination of many overlapping P2P-like networks, each comprising a node and its neighbor nodes.

3.2 Blockchain technology in ad hoc network security

Some innovative technologies exist in the blockchain field [10, 11], such as distributed ledger, asymmetric

encryption, authorization technology, consensus mechanism, and smart contract for the trust and security of transactions, and these exactly satisfy the trust system needs between the nodes studied in our ad hoc network. Consequently, a block-architecture-based ad hoc network security architecture is proposed.

In the applied architecture, the characteristics of the mobility, vulnerability, and selfishness of the nodes in the ad hoc network are fully considered; the mutual supervision between the nodes is strengthened; and the anonymity of nodes in the network is ensured through asymmetric encryption, which prevents malicious nodes from intercepting the source and destination information for launching destructive attacks. In addition, time stamps and the Hash function are used to record the transaction information of the nodes in the network, so that tamper-proof transactions and traceability can be ensured. Thereafter, the authenticity of the information stored in the blockchain is proved. The ad hoc network security architecture used in our model is more purposeful and easier to operate than the pure blockchain architecture model.

4. Node-level evaluation model based on blockchain in ad hoc network

4.1 Blockchain table creation and update

A block structure table is stored in each node of the network, which is a feature of the P2P-like network nodes used in our ad hoc network, as described in Section 2.A, and shown in Table 1. The table is dynamically updated as the node moves, and the speed of the table update is determined by the relative movement difference among the nodes. In other words, the nodes in the P2P-like network are relatively static or undergo little change, and the block structure table is stable.

Table 1. Block structure table

Block	Data item	Data item	Size
Block head	Block number	Block unique sign	4
	Previous block record	The hash value of the previous block	8
	Interactive block record	The hash value of the interactive block	8
	Personal assets	Asset ownership value	36
	Time stamp	Block generation time	4
	Merkle tree root hash	Record transaction information of the block	32
Block body	Number of communications	Total number of communications recorded by the current block	4
	Communication activity	Communication information of the current block record	32
	Believability	Trust value of the current block	4

The information in the table will automatically update the chain when the nodes interact, and no changes can be made to the tables by the nodes themselves or other nodes except for queries, which fully guarantees the security of the blockchain and the authenticity of the recorded information.

Each node in the ad hoc network automatically checks its neighbor nodes at intervals (t1) for connection in the P2P-like network. When the connection is first established, it starts from one node and traverses all its neighbor nodes to establish a connection to form a blockchain, and if all the nodes are still unable to connect, the longest connection is chosen to be the primary blockchain. The blockchain is valid for time t1; if the time

exceeds t1, the chain must be traversed again. If the nodes have not changed or the relative position is unchanged or slightly changed, the chain does not undergo any change. Otherwise the chain needs to be updated. The blockchain is shown in Figure 2.

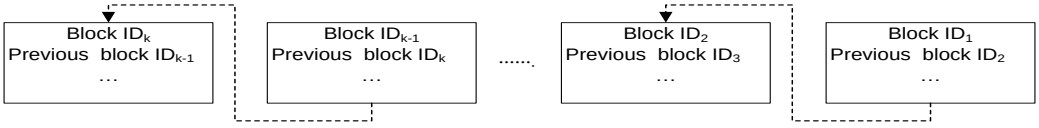

Figure 2. Blockchain diagram

4.2 Node identity and message authentication

An asymmetric key cryptosystem is used to authenticate messages when initializing the nodes. The RSA algorithm is adopted to encrypt the generated random number, and the time stamp, which is needed to decrypt the random number, is set according to the principle of information validity. Then, the decrypted random number is compared with the hash function query result. If the decrypted random number is consistent with the random number obtained from the query, the verification of the node will succeed, otherwise the verification will fail.

4.3 Reward and punishment mechanism

To fully mobilize the enthusiasm of the nodes in the network, individual asset value (δ) is used to reward and punish nodes according to their performance in the transaction. The individual asset value of the node is an important reference value to detect a suspicious node in the network, because the abnormal behavior of the node in the network directly affects its individual asset value. The individual asset double threshold (ω_s, ω_d) is set as the basis for determining the nature of the node as (1).

$$\text{node} = \begin{cases} \textit{normal} \text{ node} & \delta < \omega_s \\ \textit{suspicious node} & \omega_s \le \delta \le \omega_d \\ \textit{malicious node} & \delta > \omega_d \end{cases} \tag{1}$$

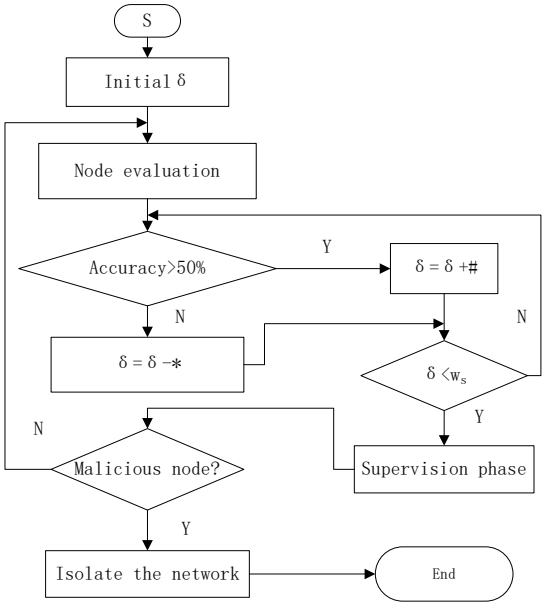

Figure 3. Reward and punishment mechanism workflow

During the network operation, a node obtains reward or punishment on its individual assets by providing an accurate evaluation of other nodes. When the accuracy of the given node is high, its individual asset value will be rewarded, and vice versa. Participation in each evaluation of the node will bring about a change in individual asset value. To avoid misjudgment of the node, a node verification mechanism is introduced, i.e., when the individual asset value is less than ω_s, a supervision of the node will be initiated; if the inner node shows no abnormal behavior, the initial value of its individual assets will be restored, otherwise it will directly set its individual asset value to zero. To quickly punish malicious behavior, the number of nodes that are punished will be recorded, and the penalty strength will be increased with the increasing number of iteration times. For example, the first penalty is 10, the second penalty is 20, the third penalty is 40, and this continues by analogy until the node enters the supervisory program. The workflow of the reward and punishment mechanism is shown in Figure 3.

4.4 Reward and punishment mechanism

The supervision and evaluation of node behavior relies on the blockchain implementation in P2P-like networks. A node on the blockchain is overseen by all the neighbor nodes from its chain, and its behavior is decided by the communication among the nodes in the most recent time. According to the evaluation criteria, the trust evaluation of the nodes is divided as follows: source node evaluation and other neighbor node evaluation. This is different from the direct and recommendation evaluations in the traditional theory, because the source node and other neighbor node evaluations are performed from different angles and are not supplementary to each other.

The source node is evaluated by the transaction node, i.e., node i evaluates node j (the source node) and the evaluation is represented by R_{ij}. R_{ij} is the ratio of the distance between the two nodes and the transmission bidirectional time. The bidirectional transmission time is the average of the time difference between the receiving of the response packets and the corresponding transmission of the request packets in the most recent time t0.

$$R_{\mathrm{ij}} = \frac{d_{ij}}{t_{\Delta}} \tag{2}$$

And

$$t_{\Delta} = \sum_{m=1}^{k} \frac{t_{me} - t_{ms}}{k} \tag{3}$$

d_{ij} represents the actual distance between node i and node j, t_{me} represents the corresponding time of the arbitrary probe packet in the most recent time, and t_{ms} represents the packet transmission time corresponding to t_{me}.

The evaluation of other neighbor nodes means that a node is evaluated by all other nodes except the source node on the blockchain, and this evaluation is expressed in the form of an evaluation degree, which is determined by the combination rate ρ and the reliability π of other neighbor nodes. The receiving rate ρ refers to the ratio of the data packets received by the node to those transmitted by the node in the most recent time t0; i.e., $\rho_k = \frac{D_{kr}}{D_{ks}}$, where ρ_k is the receiving rate of the kth node, D_{kr} is the total number of packets received by the node, and D_{ks} is the total number of packets sent by the node. The confidence π is the product of the individual property value of the node and its chain weight coefficient. The individual property value

vector $W = |\delta_1, \delta_2, ..., \delta_k|$, where δ_k represents the personal property value of the node k, the chain weight coefficient vector $F = |f_1, f_2, ..., f_k|$, where $f_k = \frac{\delta_k}{\sum_1^k \delta_k}$, and the reliability of the node k is;

$$\pi = \delta_k . f_k = \frac{\delta_k . \delta_k}{\sum_1^k \delta_k} \quad \text{and} \quad R_{kj} = \begin{cases} 0 & k = 0 \\ \frac{1}{k} . \sum_1^k (\frac{D_{kr}}{D_{ks}} . \delta_k . \frac{\delta_k}{\sum_1^k \delta_k}) & k > 0 \end{cases} \tag{4}$$

R_{kj} in (4) is the evaluation of other neighbor nodes with K other neighbor nodes in the blockchain.

For comprehensive node evaluation in (5);

$$R_j = \alpha . R_{ij} + \beta . R_{kj} \tag{5}$$

Here, α and β are adjustment coefficients, and $\alpha + \beta = 1$. An adjustable index threshold θ is set for the comprehensive evaluation of nodes to determine whether the node is a trusted node by comparing it with the threshold of the index as (6);

$$\text{node} = \begin{cases} \textit{Trusted} \text{ node} & R_j > \theta \\ \textit{Under} \min \textit{ed node} & \frac{1}{2}\theta \le R_j \le \theta \\ \textit{Dangerous node} & R_j < \frac{1}{2}\theta \end{cases} \tag{6}$$

4.5 Model analysis

Due to its combination with the blockchain, and being bound to a P2P-like network , the behavior of the node will be supervised and evaluated by all the nodes in the network. Simultaneously, the node, subject to its individual property, is also bound to be responsible for its own evaluation behavior. The evaluation of the nodes using this model is undoubtedly credible in decentralized and mobile ad hoc networks, because of the following major reasons:

(1) Node evaluation is accomplished by double equivalent evaluations by the source node and the neighbor nodes. The trust evaluation of the nodes is evaluated through communication between the nodes and involves the analysis of the nearest connection status of the neighbor nodes. The evaluation weights of the two nodes can be flexibly adjusted according to different situations so that the model can be applied to different network environments.

(2) Reward and punishment mechanism: To stimulate the supervision of nodes over the whole network, the incentive mechanism of the blockchain technology is adopted. This measure can effectively guide the correct monitoring of other nodes by quantifying the behavior of nodes and can also detect selfish nodes. This method solves the problem of hindrance in effective path selection caused by the inaction of hidden nodes in the network.

5. Simulation experiment

5.1 Experimental environment

To analyze the performance of the node trust evaluation model is proposed, a simulation platform is built

by using NS-3.29 software [12]. The network simulation parameters are shown in Table 2.

In the simulation, the mobile node moves in a 300 × 1100 m area, and each node moves according to the Random Way Point model, that is, the node randomly moves to one location, and then moves to another destination after a period of time until the simulation time ends. The movement parameters are shown in Table 3.

Table 2. Network simulation parameters

Simulation parameters	Value
Radio propagation model	Nagakami m=3
MAC	IEEE 802.11
Antenna type	Omni antenna
Transport layer protocol	UDP protocol
Packet type	CBR
Packet size	512 bytes

Table 3. Mobile parameters table

Simulation parameters	Value
Movement time	500 s
Node number	30
Number of malicious nodes	0～4
Mobile area	300 × 1100 m
Pause time	30 s
Node moving speed	0～5 m/s
Mobility model	Random way point
Node transmission range	250 m

5.2 Numerical analysis

For numerical analysis, an AODV protocol based on the blockchain-based node trust evaluation model which is proposed (MAODV protocol) is tested. The classical AODV and AOMDV protocols are selected as the references, and the packet loss rate and end-to-end transmission delay performance are compared. To analyze the model objectively and reduce the experimental error, several different attack methods (blackhole attack, DoS Attack, etc.) are used for 10 repetitions in every experiment, and the average value is accepted as the final data.

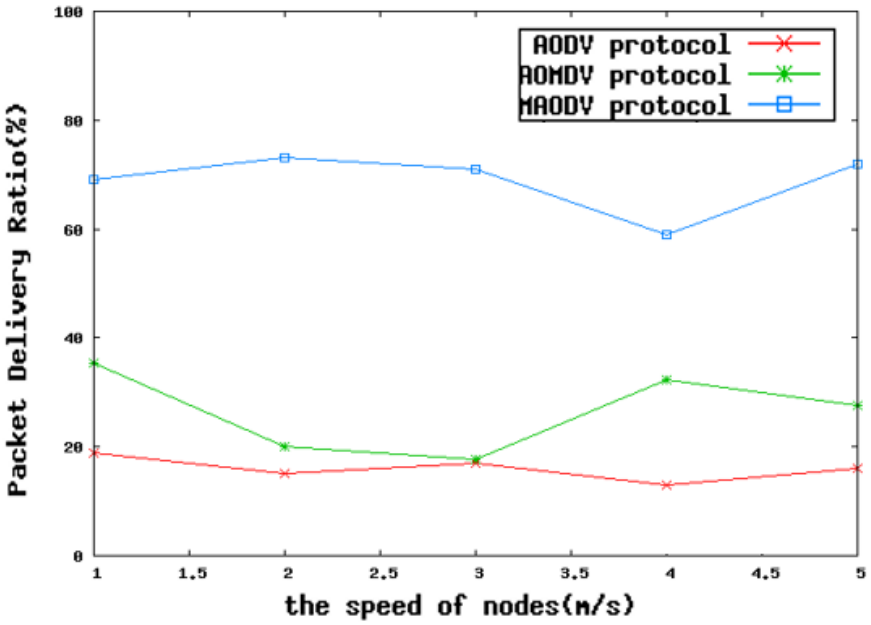

Figure 4. Comparison of successful packet delivery rates with variable speeds

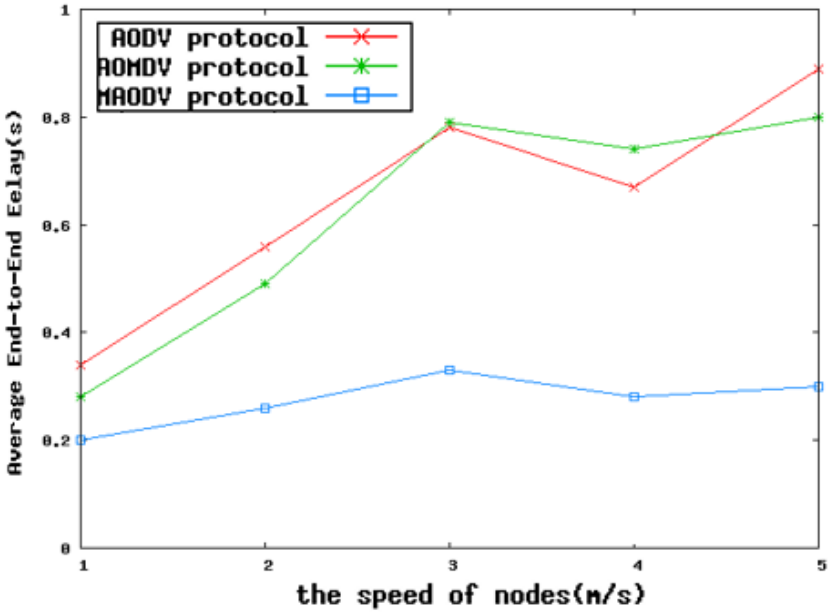

Figure 5. Comparison of average end-to-end delays with variable speeds

Figures 4 and 5 show the effective packet rate and end-to-end delay measured by running the three protocols at variable speeds from 1 m/s to 5 m/s in the presence of four malicious nodes. The packet rate of the MAODV protocol which is proposed is significantly higher than that of the AODV and the AOMDV protocols, because both these protocols cause repeated pathfinding due to malicious nodes, whereas the MAODV protocol avoids

the malicious nodes during the pathfinding process. Similarly, the end-to-end delay of the AODV and AOMDV protocols without any guard detection is higher than the MAODV protocol at different moving speeds, and the difference is more obvious as the speed increases. The faster the nodes move the greater damage is wrought by malicious nodes, and the superior model can be identified more clearly.

6. Conclusion

The application of blockchain technology in ad hoc networks is extremely challenging, because nodes in the network move continuously, and their linked list connections increase rapidly. The HASH function form of Merkle tree is adopted, which makes information search more convenient and feasible. Additionally, a node security trust evaluation model based on the blockchain technology is proposed. The trust degree is introduced as the criterion for evaluating the security of the node. Following a reward and punishment mechanism for the evaluation node, the rationality of the evaluation of the node is standardized, and finally the mobile node can be judged in real time. Results of the simulation experiments and routing protocol using the node trust evaluation model which is proposed shows great advantages in ensuring the security of networks.

Acknowledgement

This work was supported by Wonkwang University in 2019, Korea and teaching reform research project of Hengshui University (jg2018007) in 2018, China.

References

[1] L. Hanzo and R. Tafazolli, "A survey of QoS routing solutions for mobile ad-hoc network," *Journal of IEEE Communications Surveys & Tutorials, vol. 9, no. 2*, pp. 50-70, July 2007. DOI: 10.1109/ COMST.2007.382407.

[2] Y. Xu, J. Liu, O. Takahashi, N. Shiratori, and X. Jiang, "SOQR: Secure optimal QoS routing in wireless ad hoc networks," in *Proc. 2017 IEEE Wireless Communications and Networking Conference (WCNC),* San Francisco, CA pp. 1-6, Mar.19-22, 2017. DOI: 10.1109/WCNC.2017.7925687

[3] Z. Liang and W. Shi, "Enforcing cooperation resource sharing in untrusted P2P computing environment*," Journal of Mobile Networks and Applications, vol. 10, no. 6,* pp. 971-983, October 2005. DOI:10.1007/s11036-005-4453-5.

[4] A. Hakansson, R. Hartung and N. T. Nguyyen, "Service Oriented Architecture and Agents: Parallels and Opportunities," in *Agent and multi-agent technology for internet and enterprise systems,* Springer, Berlin, Heidelberg, pp. 25-48, 2010. DOI: https://doi.org/10.1007/978-3-642-13526-2_2

[5] D. J. Persis and T. P. Robert, "Review of ad-hoc on-demand distance vector protocol and its swarm intelligent variants for mobile ad-hoc network," *Journal of IET Networks Journal, vol. 6, no. 5,* pp. 87-93, September 2017. DOI: 10.1049/iet-net.2017.0015.

[6] S. Buchegger and J.-Y. L. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," in *Proc. 10th Euromicro Workshop on Parallel, Distributed and Network based Processing,* Canary Islands, Spain, pp. 403-410, Jan.9-11, 2002. DOI: 10.1109/EMPDP.2002.994204

[7] A.A. Pirzada, A. Datta, and C. McDonald, "Trust based routing for ad hoc wireless networks," *in Proc. 12th IEEE International Conference on Networks (ICON 2004),* Singapore, pp. 326-330, Nov.19-19,2004. DOI: 10.1109/ICON.2004.1409063

[8] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications," *Journal of IEEE Access, vol. 6,* pp. 27324–27335, April 2018. DOI: 10.1109/ACCESS.2018.2821705.

[9] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in internet of things systems" *Journal of Computer Communications, vol. 97, no. 1,* pp. 1-14, October 2017.
DOI: 10.1016/j.comcom.2016.10.012.

[10] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, *https://bitcoin.org/bitcoin.pdf.*

[11] D. W. Kravitz and J. Cooper, "Securing User Identity and Transactions Symbiotically: IoT Meets Blockchain," in *Proc. 2017 Global Internet of Things Summit (GIoTS),* Geneva, Switzerland, pp. 1-6, Jun.6-9,2017.
DOI: 10.1109/GIOTS.2017.8016280

[12] The Institute of Internet, ns-3 project, ns-3 manual, *https://www. nsnam.org/docs/manual/html/index.html.*

[13] W. W. Kim, "Improved Paired Cluster-Based Routing Protocol in Vehicular Ad Hoc Networks," *International journal of advanced smart convergence, vol. 7, no. 2,* pp. 22–32, Jun. 2018.
DOI: 10.7236/IJASC.2018.7.2.22.

[14] K. C. H. Kim, "The Impact of Blockchain Technology on the Music Industry," *International journal of advanced smart convergence, vol. 8, no. 1,* pp. 196–203, 2019.
DOI: 10.7236/IJASC.2019.8.1.196.