International Journal of Internet, Broadcasting and Communication Vol.12 No.3 46-55 (2020)
http://dx.doi.org/10.7236/IJIBC.2020.12.3.46

IJIBC 20-3-7

Improved Ad Hoc On-demand Distance Vector Routing(AODV) Protocol Based on Blockchain Node Detection in Ad Hoc Networks

Shuailing Yan [1] and Yeongjee Chung[2*]

[1]Ph.D. Program student, Department of Computer and Software Engineering, Wonkwang University, Korea
E-mail: yanshuailing@163.com
[2]Professor, Department of Computer and Software Engineering, Wonkwang University, Korea
E-mail: yeongjee@gmail.com

Abstract

Ad Hoc network is a special wireless network, mainly because the nodes are no control center, the topology is flexible, and the networking could be established quickly, which results the transmission stability is lower than other types of networks. In order to guarantee the transmission of data packets in the network effectively, an improved Queue Ad Hoc On-demand Distance Vector Routing protocol (Q-AODV) for node detection by using blockchain technology is proposed. In the route search process. Firstly, according to the node's daily communication record the cluster is formed by the source node using the smart contract and gradually extends to the path detection. Then the best optional path nodes are chained in the form of Merkle tree. Finally, the best path is chosen on the blockchain. Simulation experiments show that the stability of Q-AODV protocol is higher than the AODV protocol or the Dynamic Source Routing (DSR) protocol.

Keywords: *Ad Hoc network, AODV protocol, node detection, blockchain technology and smart contract.*

1. Introduction

The Ad Hoc network [1] is a special wireless network as shown in Figure 1. It had been popular among many scholars since its appearance, Ad Hoc network is an automated and intelligent network. Its main specialties are that the internal nodes have no control center, the nodes act as routing and communicating functions simultaneously, the operation of the entire network does not require external intervention. These features can effectively complement your existing network. Especially in the case of earthquake relief, construction of temporary Ad Hoc meetings, and operation of individual sites and so on, the ad hoc network seems to be the main network backbone in that case. In-vehicle Internet, Internet of Things, and Wireless Mesh Networks derived from networking have evolved rapidly in recent years [2] [3]. However, the Ad Hoc network is a relatively weak network, the communication mode is wireless, and the nodes can enter and exit

Manuscript Received: May. 21, 2020 / Revised: May. 28, 2020 / Accepted: June. 5, 2020
*Corresponding Author: yeongjee@gmail.com
Tel: +82-63-850-6887, Fax: +82-63-856-8009
Professor, Department of Computer and Software Engineering, Wonkwang University, Korea

the network freely, the data transmission path is often interrupted due to the node's movement or non-cooperation, the malicious nodes irrupt the network and so on. The stability of data transmission is the biggest problem in the current research of Ad Hoc networks, and finding the optimal transmission path through a reasonable evaluation of the internal nodes of the network is undoubtedly the best way to solve this problem.

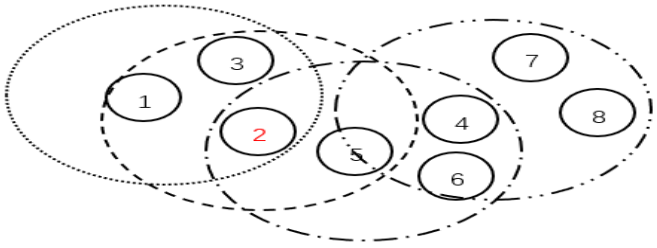

Figure 1. Ad Hoc network data communication

In 2008, Nakamoto presented the concept of blockchain [4]. Originally, the technology was mainly used in the field of economic research. Due to its unique technical advantages such as decentralization, non-repudiation and reversibility, the blockchain have also been developed rapidly in other research areas such as power, logistics, and network security [5]. The characteristics of the blockchain technology coincide with the characteristics of the Ad Hoc network. In this paper, the blockchain technology is introduced in the selection of path nodes. The reliability of the nodes inside the network is verified by means of smart contracts, which ensures the stability of the data transmission path of Ad Hoc network.

2. Related work

In order to solve the data transmission problem in Ad Hoc networks, many algorithms have been proposed. Jabbar WA et al. [6] analyzed the performance characteristics of traditional routing protocols and proposed to use new routing metrics based on multiple link quality indicators to find the best path, which breaking the limit of the number of nodes hops. Pathak G et al. [7] pointed out that multi-path alternative transmission will increase the path load, increase the probability of path congestion, resulting in reduced data transmission capacity, resource consumption, and is not applicable to mobile ad hoc networks with limited bandwidth and power. Chen W et al. [9] consider the energy consumption and movement patterns of nodes. The existence of nodes is based on battery energy, and the links between nodes are based on their speed and direction of movement. Estimate the lifetime of the link during routing. Toh C K et al. [10] proposed a battery cost routing protocol. The protocol uses the remaining energy of the path as a routing metric, and takes the path with the largest remaining energy of the node as the optimal path.

Although the above routing protocols could optimize the network load in one aspect and ensures the stability of data transmission in the Ad Hoc network to a certain extent, there are some problems. The routing protocol proposed in [6] only considers the load parameters of the route, and does not consider the node mobility problem. The routing protocol proposed in [7] considers the node mobility mode, but the mobile mode metric lacks the location information of the neighbor nodes. The routing protocol proposed in [9] does not consider the impact of node mobility on the network load, and does not reflect the link changes well. The routing protocol proposed in [10] only considers the battery cost of the node, and ignores the influence of other factors on the node. How to evaluate the nodes comprehensively and maximize the stability of the data transmission requires further research.

3. Research on AODV Protocol

AODV was first proposed by Charles E. Perkin and Elizabeth M. Belding-Royer in 1999 [15]. It is based on the traditional distance vector algorithm, which avoids the occurrence of loops and the generation of obsolete routes by using sequence numbers. The protocol includes two processes of route establishment and maintenance.

When the source node sends a data packet to the destination node, it first checks whether the path to the destination node is stored in the routing table of the source node, and if so, sends the data packets according to the path. Otherwise, the route establishment process will be initiated. First, the source node generates an RREQ (Route Request) packet and broadcasts it to neighboring nodes. After the RREQ packet arrives at the intermediate node, it is checked whether the same EERQ (EERQ packet with the same ID number and source node identifier) has passed, and if so, the packet is discarded, and if not, the reverse route is established or updated. At the same time, check whether the node is the destination node, and if so, end it, otherwise query its routing table to see if there is a route to the destination node and the route is new enough (that is, the sequence number in its routing table is greater than or equal to the destination sequence in RREQ) No.) If present, send a RREP (Routing Answer) packet to the source node. Otherwise, modify the routing table to broadcast the RREQ packet. Thus, the search is continuously progressed until the destination node is found, and the destination node returns the route reply packet RREP immediately after receiving the RREQ packet. The RREQ packet is broadcast in a flooded manner, and the RREP packet is unicast back to the source node using the established reverse path, and the intermediate node receiving the RREP establishes or updates the corresponding forward route. Reverse routes established by intermediate nodes that have established reverse routes and have not received RREP will automatically become invalid after a certain period. After the source node receives the RREP packet, a shortest path from the source node to the destination node is established.

4. Improved AODV protocol based on blockchain node detection

4.1 Nodes detection model based on blockchain in Ad Hoc network

In the Ad Hoc network, the nodes in the network can be divided into three parts according to the transmission of the data packet. The first part is the source node, which is responsible for transmitting the data packet; the second part is the intermediate node, which is responsible for forwarding the data packet; the third part is the destination node, which is responsible for receiving data packets. The three parts of the data packet transmission in the Ad Hoc network are mapped into the relationship of the blockchain, and the nodes in the blockchain mainly have three functions to be implemented, which are the contract sending node, the CA node and the verification node. The contract sending node can issue the smart contract, it is the initiator of the activity; the CA node mainly provides the identity information of the digital certificate, it can cancel or pass the node; the verification node mainly runs the contract to check the legality of the transaction data, updates and maintains the blockchain, node data or status information, etc.

The nodes detection mathematical model (AHM) definition in the Ad Hoc network is as follows.

$$AHM = (Node_s,\ Node_m,\ Node_d,\ Blockchain,\ IC,\ RS,\ Fuction,\ Connectivity)$$

where,

1. $Node_x = \{node\text{-}i \mid i \in N^+\},\ x \in \{s,m,d\}$, a finite set of source nodes $Node_s$, intermediate nodes $Node_m$, and destination nodes $Node_d$ in the network.

2. *Blockchain* is the blockchain which can detect nodes in the Ad Hoc network.
3. *IC* is smart contract in *Blockchain* .
4. $RS = \{g_k \mid g_k \in Node_i \times Node_j,\ k \in N^+,\ i \in N^+,\ j \in N^+\}$, a finite set of node-node trading relationships in the network
5. *Function* is a defined function that calculates whether a node meets the threshold requirements.
6. *Connectivity* is the connectivity of the nodes in the network, that is, the number of nodes one node can communicate with directly.

4.2 Blockchain model of Ad Hoc network

The blockchain contains two parts: the block header and the block body. The block header contains the HASH value of the block, the timestamp, the difficulty, the HASH value of the previous block, and the HASH value of the Merkle-root. The block body contains the information detection value of the nodes during the creation and verification process as shown in Figure 2.

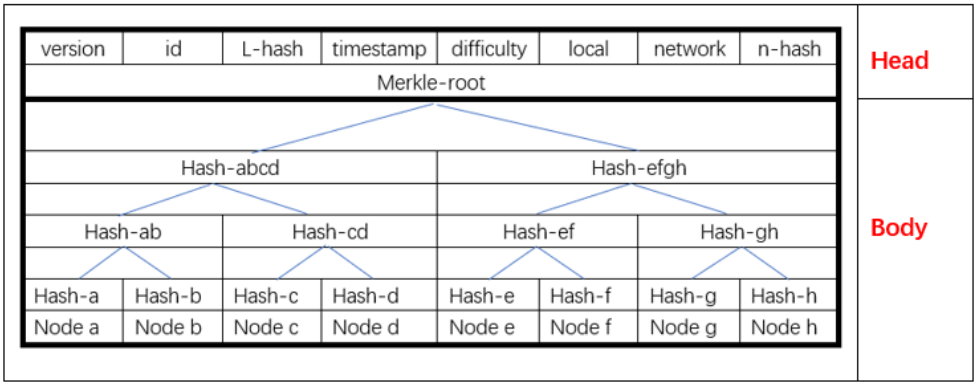

Figure 2. Blockchain model of Ad Hoc network

The model assumes that there is a total of eight nodes, which are a, b, c, d, e, f, g, h in the network. The nodes a, b can form a first-level blockchain, the nodes c, d can form a first-level blockchain; and the nodes a, b, c, d can form a secondary blockchain, nodes a, b , c, d, e, f, g, h can form a three-level blockchain. When there are many nodes in the network, a higher level of blockchain can be obtained. The blockchain of the higher level is composed of the blockchain of the lower level. In an Ad Hoc network, each primary blockchain is composed of any two nodes that can communicate with each other. The lower-level blockchains are connected to a higher-level blockchain, requiring inter-node mutual authentication for reliability, and the reliability primarily relies on smart contracts to evaluate latency and response timeliness of the node.

(1) Processing delay (DH)

The processing delay calculation is used to solve the problem that the node receives the data packet in time. The ratio of the two items is calculated as the basis for determining the processing delay from the time when the node accepts the data packet to the time when the node transmits the data packet within a certain time interval.

$$DH=\begin{cases}\dfrac{headle\_i}{\text{Interval}} & 0<\dfrac{headle\_i}{\text{Interval}}<1\\ 1 & \dfrac{headle\_i}{\text{Interval}}\geq 1\end{cases} \tag{1}$$

where $headle\_i$ is the processing delay of the node i during the time interval, which is a fixed time interval.

(2) Response timeliness (FRT)

The response timeliness mainly depends on the forwarding rate and response time of the data packet. Whether a node can forward the data packet to the destination node within the maximum tolerance time is of concern in the Ad Hoc network, which is also an important factor in identifying one node is stable or not. Therefore, the response timeliness can be expressed as:

$$FRT=\frac{sd_i}{td_i}(1-\frac{T_{next}-T_{prior}}{T_{fix}}) \tag{2}$$

where, sd_i indicates the total number of packets sent by the node, td_i indicating the total number of packets received by the node i. T_{next} indicates the time when the next node receives the packet and T_{prior} could be seen the time when the node receives the packet, T_{fix} indicating a fixed time interval.

Therefore, the detection results (DRT) of a single node are summarized as follows:

$$DRT=\begin{cases}0 & life=0\\ \alpha\times HD+\beta\times FRT & life=1\end{cases} \tag{3}$$

where, α , β is the proportion of processing delay and response timeliness respectively, which can be adjusted according to different network environments. At the same time, we set the node reliability threshold interval as follows:

$$\text{node}=\begin{cases}\text{Reliable node} & DRT>\max(\omega)\\ \text{Undetermined node} & DRT\in\omega\\ \textit{Un}\text{reliable node} & DRT<\min(\omega)\end{cases} \tag{4}$$

When the detection result of the node is greater than the maximum value of the threshold interval, the reliability of the node is strong. When the node is lower than the minimum value of the threshold interval, the reliability of the node is weak. When the node happens to be in the threshold interval, it cannot be determined that the reliability of the node needs further detection.

4.3 Route Establishment

The route establishment is mainly a valid path established by the source node to find the destination node by broadcasting the probe packet, and then the destination node returns the response packet. Each node within the network periodically probes neighbor nodes and records probe information. First, the network can be divided into several clusters, where there is only one common node between two adjacent clusters, and the common node is the node through which the packet transmission must pass. Each node forms a cluster with adjacent, communicable nodes. Within the cluster, the information sending node begins to form a blockchain, in which the packet processing delay, packet forwarding rate, and response time of the node are passed

through the node chain. And the node that does not satisfy a condition of the reliability of the detection node such as the data packet request frequency of communication, is isolated and will be broadcasted to the entire network. The route establishment process is as follows:

(1) The node sends a probe packet to the network. Check whether there is a destination node in the communication coverage of the node. If it exists, send the probe packet directly to the destination node and end. If it does not exist, go to (2).

(2) Within the communication coverage of the node, a first level blockchain is established, and the first level blockchain is connected to the secondary blockchain to obtain a reliability node and is stored to the path chain.

(3) Establish a new first-level blockchain within the communication range of the highest reliability node and connect the first level blockchain with the first level blockchain of the previous level containing the node for the secondary blockchain connection. Obtain a new reliability node and store the class nodes in the path chain.

(4) Repeat the process of (3) until the destination node is found and connected to the path chain.

(5) The destination node sends a response packet to the source node according to the path chain and confirms the optimal path of the packet transmission.

The route lookup algorithm is as the follow Table 1.

Table 1. Routing lookup algorithm based on blockchain detection

	Input source node, destination node Output routing from source node to destination node
1.	Initialize Ad Hoc network
2.	If finding (destination node) and life=1
3.	{End
4.	return true}
5.	Else if finding (destination node) and life=0
6.	{End
7.	Return false}
8.	Else
9.	Finding(node)
10.	{If node==destination
11.	end
12.	{ for(node-id=1, i<=count(node), node-id++){
13.	$DRT = \alpha \times HD + \beta \times FRT$
14.	Define load threshold α =0.6 β =0.4
15.	DRT compare ω
16.	Comfortable(node-id) belong to blockchain
17.	Finding(node-id)
Print(blockchain)	

5. Experimental simulation

5.1 Network Simulation Environment Settings

In this paper, NS3.29 software is used as the simulation platform [10]. The network topology is a network model with nodes randomly distributed in a plane rectangular area of 1000 m×1000 m. The velocity of mobile nodes is 5m/s to 50m/s. The MAC layer adopts IEEE 802.11 and adopts constant bit rate (CBR) data

stream. The simulation time is 900s, and the maximum residence time of nodes is 0s, 5s, 10s, 20s, 30s. In the stability simulation evaluation of Q-AODV, DSR and AODV, the following performance parameters are mainly considered: data packet delivery rate and data end to end delay. The main performance parameters are shown in Table 2.

Table 2. Experimental parameters and their configuration

Parameters	value	Explanation
N	10-80	Number of network nodes
DOM	1000 m×1000 m	Area size
B_W	10Mps	bandwidth
V_{max}/V_{min}	50/5(m/s)	Maximum and minimum node speed
T_{max}/T_{min}	40/0	Time interval for sending packets

5.2 Definition of simulation parameters

(1) Packet Group Delivery Rate (PDF)

The packet group delivery rate is the ratio of the number of group packets successfully received by the destination node to the number of group packets generated by the source node. This indicator reflects the performance of the algorithm to adapt to network changes and the maximum throughput that the network can support. It is an indicator of the completeness and correctness of the routing algorithm. The larger the packet delivery rate, the less group packets are lost during transmission and the better the network performance.

$$PDF = \frac{Send_{sourse}}{\mathrm{Re}ceive_{destination}} \tag{5}$$

where, $Send_{sourse}$ indicates the data packet generated by the source node, $\mathrm{Re}ceive_{destination}$ indicates the number of packet packets successfully received by the destination node.

(2) End-to-end average delay Ta

This includes all possible delays caused during buffering, which are route discovery latency, queuing time in the interface queue, transit delay at the MAC layer, and broadcast and transmission delays. The smaller the delay, the faster the response and the more satisfactory the network quality.

$$T_a = \frac{Delay_{nodes}}{Tnumber_{nodes}} \tag{6}$$

where, $Delay_{nodes}$ represents the sum of the delay times of all the packets arriving at the destination node, $Tnumber_{nodes}$ indicates the number of packets successfully received by the destination node.

5.3 Network Simulation and Data Analysis

As can be seen from the figure 3, the Q-AODV algorithm proposed in this paper has a better advantage in the packet rate than the traditional AODV algorithm and DSR algorithm, and the advantage is greater as the number of nodes increases. This is mainly because the Q-AODV algorithm selects a relatively reliable

node as an intermediate node in the initial route search, so that the probability of route interruption in the transmission process of the data packet is lower than other algorithms, so the packet rate is naturally high. While the AODV algorithm and the DSR algorithm are in the process of establishing the path, the selection of the nodes is completely random. When some vulnerable nodes are selected, the routing will be interrupted quickly, and the routing query process must be initiated again.

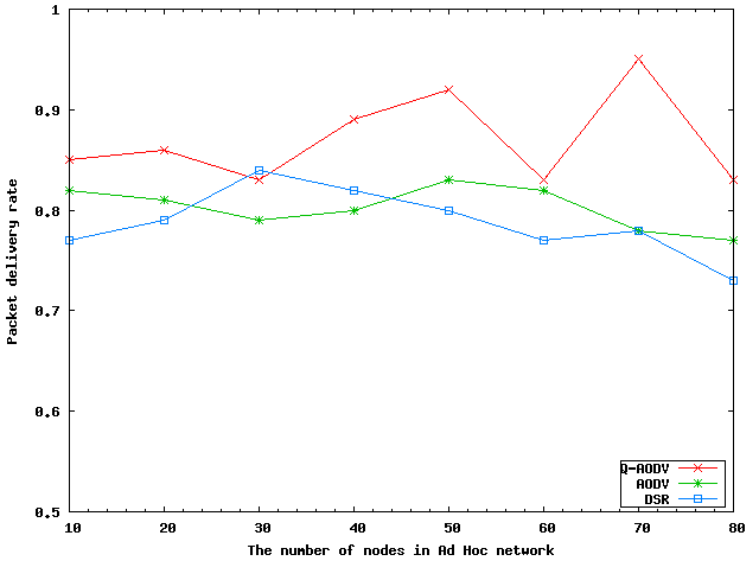

Figure 3. Comparison of package delivery rate for nodes Change

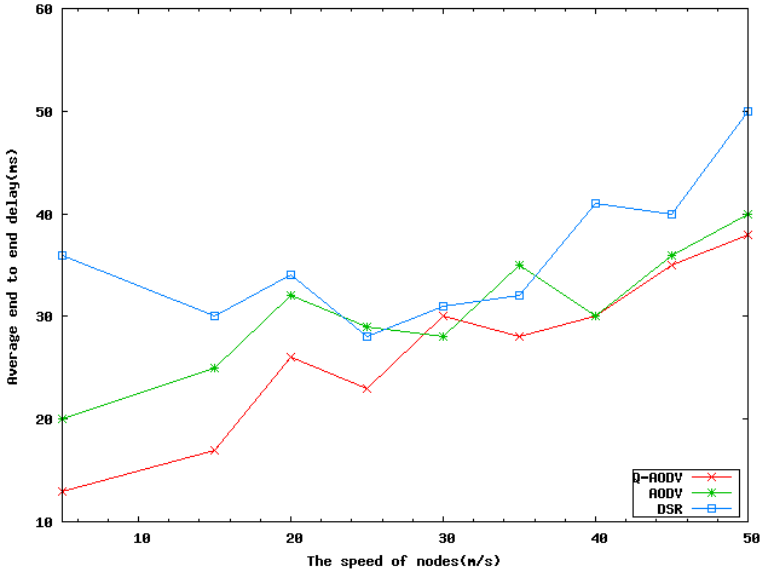

Figure 4. Comparison of average end to end delays for Speed Change

As shown from the figure 4, the Q-AODV algorithm proposed in this paper has better end-to-end time delay than the AODV algorithm and the DSR algorithm, but as the node moving speed increases, its time delay also increases significantly, which is mainly due to reliable nodes. Due to the movement, continuous updates from the blockchain make the route establishment process frequent. The algorithm is more suitable

for low moving speeds than moving speed. However, compared with the traditional AODV algorithm and DSR algorithm, the Q-AODV algorithm has also improved the end-to-end time delay, especially in the case of malicious node attacks, because the algorithm can eliminate malicious nodes early. Making route reconstruction is much faster than the other two algorithms.

6. Summary

The Q-AODV algorithm proposed in this paper finds an optimal data transmission path by gradually detecting the node using blockchain technology in the route establishment process. Through simulation experiments, the algorithm shows great advantages in the delivery rate of data packets and the end-to-end delay of data packets, which can well guarantee the stability of network data transmission. However, it is also found that the end-to-end delay of the algorithm also rises significantly when the node moves faster. This is mainly because the node moves quickly away from the path chain and must be searched for again. This situation may be improved by establishing a multipath approach.

Acknowledgement

This paper was supported by Wonkwang University, Iksan Korea in 2020.

References

[1] Islabudeen, M., and Kavitha Devi, M.K. ,"A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks," *Wireless Personal Communications*, Vol.112, No.02, pp:193-224, January 2020.
DOI: https://doi.org/10.1007/s11277-019-07022-5.

[2] Liu F., and Heijenk G., *Wired/Wireless Internet Communications.* Lecture Notes in Computer Science, pp.13, 2006.

[3] Das, S.K., Yadav A.K., and Tripathi, S., "IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network," *Peer-to-Peer Networking and Applications*, Vol.10, No.03, pp: 670–687, November 2016.
DOI: https://doi.org/10.1007/s12083-016-0532-6.

[4] The Institute of Internet, Bitcoin: A peer-to-peer electronic cash system, S. Nakamoto. *https://bitco.in/pdf/bitcoin.pdf.*

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using Blockchain for Medical Data Access and Permission Management," in *Pro. 2nd International Conference on Open and Big Data (OBD)*, pp.25-30, Aug. 22-24, 2016.

[6] Waheb A. Jabbar, Mahamod Ismail, and Rosdiadee Nordin, "Multi-criteria based multipath OLSR for battery and queue-aware routing in multi-hop ad hoc wireless networks," *Wireless Networks*, Vol.21, No.22, pp: 1309–1326, November 2014.
DOI: https://doi.org/10.1007/s11276-014-0857-0.

[7] Gaurav Pathak, and Krishan Kumar, "Traffic aware load balancing in AOMDV for mobile Ad-hoc networks," *Journal of Communications & Information Networks*, Vol.2, No.28, pp:123-130, June 2017.
DOI: https://doi.org/10.1007/s41650-017-0012-z.

[8] K.Rama Abirami, and M.G.Sumithra, "Evaluation of neighbor credit value based AODV routing algorithms for selfish node behavior detection," *Cluster Computing*, Vol.22, No.13, pp: 13307–13316, January 2018.
DOI: https://doi.org/10.1007/s10586-018-1851-6.

[9] Wai Chen, Ratul K.Guha, Taek Jin Kwon, Jone Lee , and Yuanying Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Wireless Communications & Mobile Computing*, Vol.11, No.7, pp:787-795, July 2011.
DOI: https://doi.org/10.1002/wcm.862.

[10] C.-K. TOH, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall PTR, pp.192,2002.

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

[12] N. S. Nizamkari, "A graph-based trust-enhanced recommender system for service selection in IOT," in *Pro International Conference on Inventive Systems and Control (ICISC)*, pp. 1-5, Jan.19-20, 2017.

[13] H. Sukhwani ,J. M. Martínez , X. Chang, K. S. Trivedi , and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)," in *Pro 36th Symposium on Reliable Distributed Systems (SRDS)*, pp. 1-3, Sept.26-29, 2017.

[14] S. Kadam, D. Prabhu, N. Rathi, P. Chaki, and G. S. Kasbekar, "Exploiting group structure in MAC protocol design for multichannel Ad Hoc cognitive radio networks," *IEEE Transactions on Vehicular Technology*, Vol.68, No.1, pp:893-907, Jan. 2019.
DOI: https://doi.org/10.1109/TVT.2018.2883392.

[15] P. Charles, B. Elizabeth, "Ad-hoc On-Demand Distance Vector Routing*," Proc. 2nd IEEE Workshop on Mobile Computing Syst. and Applications (WMCSA '99), February 25-26, 1999, New Orleans, LA, USA*, Vol. 25, No.1, pp:90-100, Feb., 1999.
DOI: 10.1109/MCSA.1999.749281