An Improved AODV Routing Security Algorithm Based on Blockchain Technology in Ad Hoc Network

Conglin Ran
Jiujiang University
Shuailing Yan (yanshuailing@163.com)
Hengshui University https://orcid.org/0000-0003-4905-1485
Liang Huang
Shangrao Normal University
Lei Zhang
Hengshui University

Research

Keywords: Ad Hoc network, AODV protocol, blockchain, routing security, QoS, smart contract

Posted Date: February 12th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-125899/v2

Version of Record: A version of this preprint was published on March 9th, 2021. See the published version at https://doi.org/10.1186/s13638-021-01938-y.

An Improved AODV Routing Security Algorithm Based on Blockchain Technology in Ad Hoc Network

Conglin Ran[1,4], Shuailing Yan[2,4,*], Liang Huang[3,4], Lei Zhang[2]

[1] Department of Information Technology Center, Jiujiang University, Jiujiang 332005, P.R.China
[2]Department of Mathematics and Computer Science, Hengshui University, Hengshui 053000, P. R. China
[3] School of Mathematics & Computer Science, Shangrao Normal University, Shangrao 334001, P.R. China
[4]Department of Computer and Software Engineering, Wonkwang University, Iksan 54538, Republic of Korea
*Correspondence: yanshuailing@163.com

Abstract: Ad Hoc network is a special network with centerless and dynamic topology. Due to the free mobility of the nodes, routing security has been a bottleneck problem that plagues its development. Therefore, a multi-path QoS (Quality of Service) routing security algorithm based on blockchain by improving the traditional AODV (Ad hoc On-Demand Distance Vector) protocol (AODV-MQS) is proposed. Firstly, a chain of nodes is established in the network and the states of all nodes by making the intermediate nodes on the chain are saved. Secondly, the smart contract in the blockchain is set to filter out the nodes that meet the QoS constraints. Finally, two largest unrelated communication paths are found in the blockchain network through smart contract, one of which is the main path and the other is the standby path. Simulation experiments show that the performance of the proposed algorithm is better than other algorithms, especially in an unsafe environment.

Keywords: Ad Hoc network, AODV protocol, blockchain, routing security, smart contract

1 Introduction

In Ad Hoc networks, because the nodes are exposure to the outside, some problems, for example, the nodes are damaged and the batteries are exhausted and so on, are faced by them [1][2]. At the same time, due to the characteristics of the network, such as inherent defects of the wireless channel itself, dynamic changes of the topology, lack of a centralized control center to protect node information etc. [3][4]. Therefore, the routing security issues of mobile Ad Hoc networks need to be resolved urgently. At present, there have been many attack methods and defense schemes to deal with the problems of protocol vulnerabilities and routing security of Ad Hoc networks [5-7]. In the network a node as an individual may be subjected to malicious attacks, the attack points are not limited to a certain protocol layer, they can harm some layers of the protocol stack at the same time [8][9]. From the perspective of attack mechanism, the attacks can generally be divided into two categories: routing mechanism damage and routing resource consumption [10] [11]. From the perspective of attack methods, the attacks can be classified into four categories: interception, tampering, interruption, and forgery [12].

For security issues, different solutions can be proposed for different environments. In multi task, many methods, such as identifying tasks effectively, protecting access to massive data effectively and so on, are the ways to solve security problems [13][14]. At present, many scholars focus their research on the handling of attacks, but they ignore the QoS, and the actual Ad Hoc network environment often takes notice of service quality seriously. Effective evaluation and comparison are the most powerful basis for comprehensive analysis and accurate judgment of service quality. Many algorithms have introduced this idea [15][16]. Simulation experiments show that the proposed algorithm has obvious advantages over other algorithms in terms of end-to-end time delay, packet delivery rate and control overhead, it can avoid malicious attacks and improve the routing security of Ad Hoc networks.

The rest of this paper is organized as follows. Section 2 discusses the related work of attacks in Ad Hoc network. An improved AODV Multi-path QoS routing security algorithm is designed in Section 3. The simulation experiment and analysis are given in Section 4. In Section 5, the summary and future research are concluded.

2 Related work

So far, many scholars have proposed many solutions to solve black hole attacks in Ad Hoc networks. S. Gupta et al. proposed a method to detect black hole nodes by modifying routing requests and routing reply control packets based on the AODV protocol [17]. Firstly, the count of hops, the destination node, the sequence number and other information in the routing table are counted. Secondly, the trust threshold is set. Finally, the scheme of the optimal route according to the path length in AODV protocol is chosen to be transformed into one that relies on the threshold. The strategy is carried out to ensure that the packet transmission node is the most likely legal node, and the biggest disadvantage is that it depends on the choice of trust threshold. Once the threshold is not set reasonably, it will cause great misjudgment and form a false warning, thus the performance of the whole network is seriously affected. Deng et al. proposed a method to detect the next-hop node of the intermediate node [18]. When the source node receives the package RREP which is sent by the intermediate node, it sends a verification packet to the next-hop node to authenticate. After receiving the verification information, the next-hop node replies to the source node. And the source node will confirm whether the intermediate node is a normal node or not through the message. If it is, the source node sends data through the route. Otherwise, the intermediate node is regarded as a black hole node.

Huang et al. proposed a method to detect the loss packets based on one-way hash chain and one-time hash tag commitment [19]. The implementation of the method mainly depends on the form of forwarding redundant data packets and sharing secret keys among nodes. In addition, the source node also needs to predict the sending status of the next data packet. Therefore, the main disadvantage of the method is that the control overhead is too high, especially when the network scale becomes larger, the shared key cannot be guaranteed to transmit. Papadimitriou et al. used path redundancy and threshold secret sharing technology to achieve the secure transmission of data [20]. The scheme uses an end-to-end authentication method. The packet loss path discovery process does not require intermediate nodes to participate, but it cannot detect the nodes whose loss packages.

Sankara et al. proposed a high-level mechanism against wormhole attacks in the MANET network [21]. The mechanism mainly uses the service quality of the network to detect the attacking nodes, at the same time, it could judge whether the attack is active or passive according to the round-

trip time of the data packet at one node. This method can identify wormhole attacks better, but it does not consider the risk of data being intercepted. Aswale et al. introduced advanced encryption algorithms to detect nodes, and they adopted channel security detection to avoid the traditional secure communication at the cost of energy and extend the life of the network [22]. However, the complexity of the method is too high, which leads to an excessively high control overhead, so it is not suitable for high-speed mobile Ad Hoc networks with limited network bandwidth.

Dr. He et al. proposed a trust mechanism by introducing blockchain technology in distributed peer-to-peer networks [23]. The mechanism can separate the untrusted nodes and create a secure network environment. However, only the untrusted nodes are considered in this mechanism, and there is no reasonable judgment to make the performance of network degrade caused by the nodes' own problems. Therefore, it is easy to cause the problem of node misjudgment. Lazrag et al. proposed a method of data security sharing based on blockchain technology for distributed devices [24]. Although the method solves the problem of data security transmission, it does not make a reasonable evaluation of node security. Goyat et al. proposed a secure location method of wireless nodes based on blockchain technology [25]. The method only considers the security of a single node, but it does not consider the security of association between nodes. Firdaus et al. proposed a scheme to solve the trusted environment of secure data storage and sharing based on blockchain and smart contracts in wireless environment [26]. The scheme effectively uses the characteristics of blockchain technology to solve the problem of data storage and environment detection in an insecure environment, but it does not consider normal failure of nodes in a secure environment.

3 Methods

The accuracy of the model can be effectively controlled by the parameters, and then the expected goal can be achieved [27][28]. Therefore, the flexible parameter information may be used to achieve the path selection.

3.1 Definition of QoS related parameters

(1) Path bandwidth

It refers to the minimum bandwidth of all adjacent nodes in the whole routing path, which is represented by parameter $Bandwidth$.

$$Bandwidth(s,\ d) = min\ \{B(i,j),\ i = 1,2,3\mathrm{L}\ ;\ j = 1,2,3\mathrm{L}\ \} \tag{1}$$

where s indicates the source node, and d indicates the destination node, and $B(i,j)$ indicates the communication link bandwidth between the intermediate node i and node j that can communicate with each other.

(2) Time delay

It refers to the time of a packet transmission from source node to destination node, which is represented by the parameter T. Assuming that all nodes in the network have the same processing capacity and channel bandwidth, and the wireless channel is symmetric. At the same time, the size of the route request probe packet, the response packets of the nodes, and the data packets are equal. In the network the data packets transmission time is divided into two parts, namely the processing time $\mathrm{Pr}o$ and the transmission time Tra in the communication. The processing time $\mathrm{Pr}o$ is divided into the waiting processing time T_w in the queue and the real actual processing time T_e.

$$T = \sum_{k=1}^{n} \mathrm{Pr}o_k + \sum_{m=1}^{n} Tra_{m(m-1)}, k \geq 2,\ k \in N,\ m = k-1 \tag{2}$$

$$\Pr o = T_w + T_e \tag{3}$$

where $\Pr o_k$ represents the time when the node k forwards the information packets in the data transmission, and $Tra_{m(m-1)}$ represents the time taken by the data packet to pass between the intermediate node m and node $m-1$. Assume that the number of nodes in the network is bigger than 1, $k \geq 2$ can be set. The maximum value of k is the total number of nodes in the network. Combining Eq. (2) and Eq. (3), it can be seen that the time delay T of data transmission is,

$$T = \sum (T_w + T_e)_k + \sum Tra_{m(m-1)}, k \geq 2, k \in N, m = k-1 \tag{4}$$

Compared with the transmission time of the data packet in the path and the actual execution time of the data packet, the waiting time of the data packet in the queue is short enough, so the waiting time of the data packet could be ignored, and Eq. (4) can be transformed into,

$$T = \sum (T_e)_k + \sum Tra_{m(m-1)}, k \geq 2, k \in N, m = k-1 \tag{5}$$

(3) Path survival vitality

The viability of the node is the continuous working time of the node under normal conditions, which is represented by E_{id}. It is obtained by the calculation through the smallest degree of the node's connectivity ω and the remaining battery consumption θ, which can be expressed by Eq. (6),

$$E_{id} = \frac{\theta}{\omega + 1} + \alpha \tag{6}$$

where α indicates a balance factor, it can be set freely according to the required path survival expectation, and we add 1 to the denominator to prevent the invalidity of the Eq. (6) caused by ω being 0. The value of ω is the number of nodes under the energy coverage of the node. As shown in Fig. 1. It can be seen that the connectivity of node *C* is 2, because there are the two nodes (node *A* and node *B*) under the energy coverage of node *C*. θ indicates the original full energy of the node. As time goes by, the energy value of node will decrease, and the covered communication radius may be also shrinking, so the number of covered nodes will decrease, the value of $\frac{\theta}{\omega + 1}$ cannot change much. The value can reflect the sustainable working time of the node to a certain extent, and the viability of the entire path can be inferred.

The viability of the path is the reference value *E* for the path existing the longest time. *E* is the minimum node viability in the path.

$$E = \min \{E_{id}\}, id = 1, 2, 3\mathrm{L}\ n \tag{7}$$

(4) Comprehensive measurement of QoS parameters

The survivability of the path reflects the usable performance of the path. It mainly be determined by time delay, available bandwidth and path viability. *M* is set to the survivability of the path, then it can be expressed as the Eq. (8),

$$\begin{cases} M = \lambda \dfrac{Bandwidth}{Bandwith\_B} + \chi \dfrac{T}{T\_B} + \delta \dfrac{E}{E\_B} + \zeta \\ \lambda + \chi + \delta = 1 \\ 0 \le \lambda \le 1 \\ 0 \le \chi \le 1 \\ 0 \le \delta \le 1 \end{cases} \tag{8}$$

where λ, χ, δ are the coordination coefficients, and ζ is the balance factor of routing survivability, it can be set according to the detection of data packets in the path. *Bandwidth* represents the bandwidth, T represents time delay and E represents path viability of the path respectively, $Bandwith\_B$ indicates the estimated standard value of the path bandwidth, T_B indicates the estimated standard value of time delay, E_B indicates the estimated standard value of path viability.

When the network environment is secure except for some malicious nodes, the coefficient λ is set to be larger and other coefficients are set to be smaller. When the network environment is secure with no malicious nodes, the coefficient ζ is set to be larger and other coefficients are set to be smaller. When the network environment is insecure and exists malicious nodes, the three coefficients are set to be larger. The parameter M is a comprehensive parameter, it can be adjusted according to different coefficients set by the environment.

3.2 Route establishment

The process of route establishment is a process initiated by the source node to establish a blockchain in which the available nodes in the network are continuously connected to the chain by means of request/response. The ultimate goal of the process is to find two short and most irrelevant chains ending with the destination node. When the source node needs to send data to the destination node and the source node does not have a route to the destination node, it will create a genesis block to find the lists to the destination node. As shown in Fig. 2. Then the source node sends the detection packets (EERQ) to its neighbor nodes according to its Merkle tree, the process of finding the destination node is started.

In Fig. 2, Merkle tree is composed of the neighboring nodes of the node, and Pre-point is the address of the previous node. Since the node is a creator node, there is no previous node, its value is null. ID represents the address of this node.

Step 1. The source node sends EERQ packets to its neighboring nodes, and the time timer is started and valid time domain τ is set.

Step 2. When the delay field ς in the EERQ is bigger than valid time domain τ during transmission, the EERQ packet become invalid because it exceeds the maximum time delay in finding a path.

Step 3. According to the storage capacity flag (isfull) in the node memory routing table, when its value is 0, go to Step10. When the value is 1, the timer for processing packets of the node is started.

Step 4. After the neighboring node receives the EERQ packet, it will be judged that it is first time or not. If so, the EERQ packet will be received. Otherwise, the EERQ packet is discarded and transferred to (5).

Step 5. If the conditions are satisfied, the node is agreed to connect to the blockchain. Otherwise, it will be rejected and detected regularly. Node 1 and node 3 are connected to the source node because they meet the requirements, as shown in Fig. 3.

Step 6. Compared with the survivability domain E of the path in the detection packet EERQ. If it is less, the domain value will be updated, otherwise the survivability domain value E of the path in EERQ will remain unchanged.

Step 7. Check whether the processing packet timer of the node is off, and if so, go to Step10. Otherwise, the RREQ forwarding data counter is started and the counter value is set according to the viability of the node. The value of the path viability e is calculated by Eq. (7). The specific method to determine the node timer is as follows,

①The counter is set to maximum value, that is, regardless of the viability of the node, the counter value cannot be set to exceed the maximum value. The maximum value is determined according to the specific communication time delay. Set the maximum value as MAX and the communication time delay as T then,

$$MAX = \frac{1}{2}T \tag{9}$$

②The corresponding counter value Dt is set according to the node's vitality E, its connectivity ω, and the number of hops H_d in EERQ.

$$W = \omega - \left\lceil \frac{\omega}{H_d + 1} \right\rceil \tag{10}$$

$$D_t = (1 - \frac{1}{W + 1})MAX \tag{11}$$

When the connectivity ω of the node's vitality E is 0, then D_t is 0. Because when the connectivity ω of node vitality E is 0, the node has no forwarding ability and conditions. From the Eq. (11), it can be concluded that only the greater the connectivity of the node and the smaller hop number in EERQ, the closer the counter of the node is set to the max value.

Step 8. Judge whether the node is the destination node or not. If so, go to Step10. Otherwise, go to Step 9.

Step 9. The node forwards the EERQ request packet, Step4 must be gone, and the forwarding of the request packets is repeated.

Step 10. If the destination node is found, the public key information of the destination node is transmitted to the source node according to the blockchain path. Otherwise, terminate this search.

The Ad Hoc network is shown in Fig. 4. In Fig. 4, node 2 and node 6 are malicious nodes, and node 4, node 8 and node 11 are the nodes that do not meet the constraints. The source node is S and the destination node is D.

After the algorithm, the block of the source node saves all the retrieval results from the source node to the destination node, as shown in Fig. 5.

It can be seen from Fig. 5 that the path detection is no longer performed at malicious nodes and the nodes that do not meet the constraint conditions. In the figure, the connecting lines at node 2, node 4, node 6 and node 8 lose the arrow, it indicates that the blockchain connection has been lost in this part. It can be seen that the network finally formed three paths: R1: S-1-7-11-D, R2: S-1-7-12-13-D and R3: S-3-9-14- D. The three paths are recorded in the memory routing table of the source node in the order of arrival time, and the intermediate nodes on each path enter the table in order of increasing repetition rate, and the initial value is 0. The three available paths in Fig. 5 enter

the memory table, the memory table as shown in the Tab. 1.

Table 1. Path memory routing table

Path name	The values (Σ) of intermediate nodes			
S1	0	0	0	
S2	1	1	0	0
S3	0	0	0	

In Tab. 1, the minimum sum of Σ is taken as the first criterion, because the larger value of Σ, the greater the correlation between the path and the previously reached path. In order to find the largest irrelevant path, it can be obtained by simple accumulation of the value Σ. When the value Σ of the path is the same, the length of the path is taken as the second selection criterion, because in the same correlation, the shorter the path is, the more stable the link is, and the smaller the control cost of the network is. When the length is the same, the order in which the source node receives the public key returned by the destination node according to the corresponding path is taken as the selection standard, because the faster the data packets of the first arrival path are transmitted, the less the end-to-end delay is, and the network data transmission efficiency can be greatly improved.

3.3 Route Maintenance

In the Ad Hoc network, although there are multiple paths to ensure the transmission of information, it is still possible that the link connection fails due to the movement of nodes, and the occurrence of congestion leads to insufficient bandwidth, transmission timeout, and other path damage. Therefore, the repair of the path cannot be ignored. Three methods are used to resolve these problems, as shown in Tab. 2.

Table 2. Experimental parameters and their configuration

Environment / conditions	Strategy adopted	Failure situation
The environment is good and malicious nodes exist	Two paths	Uneven distribution of nodes
The environment is good and malicious nodes do not exist	Rerouting from breakpoint	Uneven distribution of nodes
The environment is bad and malicious nodes exist	Rerouting from the source node	Uneven distribution of nodes

Three routing maintenance strategies are listed in Tab.2, and specific environment and conditions are defined for each routing maintenance strategy. Only when the environment and conditions are met and the main path fails, the corresponding routing maintenance strategy will be started.

4 Results and Discussion

4.1 Simulation environment and parameter setting

In this paper, NS3.29 software is used as the simulation platform [29]. Network topology is a network model with nodes randomly distributed in a plane rectangular area of 1000 m×1000 m. The range of mobile nodes speed is from 5m/s to 50m/s. IEEE 802.11 and constant bit rate (CBR) data stream are adopted in the MAC layer. The simulation time is 900s, and the maximum residence time

of nodes is set to 0s, 5s, 10s, 20s, 30s. The abnormal nodes are added during the experiment, they include a random number of energy-constrained nodes, black hole nodes, wormhole nodes, and sybil nodes [30][31]. During the simulation, the following performance parameters are mainly considered: data packet delivery rate, data end to end delay and control overhead. The main performance parameters are shown in Tab. 3.

Table 3. 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
Vmax/Vmin	50/5(m/s)	Maximum and minimum node speed
Tmax/Tmin	40/0	Time interval for sending packets
Time	900s	Simulation time

4.2 Data Analysis

Fig. 6 is comparison of end-to-end delay of four routing algorithms in a safe environment. It can be seen that the AODV-MQS algorithm proposed in this paper performs a lower time delay than the other two algorithms when the node moving speed is low. Because the method of maximum irrelevant multipath is adopted in proposed algorithm, it ensures that when one path becomes invalid, the other alternative path can be used directly without rerouting and searching. However, when the nodes move faster, the multi-path proposed in this paper may also break at the same time, which will inevitably lead to time delay similar to the other three algorithms. Therefore, when the node speed increases, the advantages of the proposed algorithm in this paper are not obvious. At the same time, due to the interrupt path repair method, the faster node movement will not lead to the continuous deterioration of the time delay. Therefore, the time delay of the other three kinds of algorithms shows a continuous increase in this respect, while the algorithm proposed in this paper shows a gentle rise.

Fig. 7 is comparison of end-to-end delay of four routing algorithms in an unsafe environment. It can be seen that the proposed algorithm performs obvious advantages in end-to-end delay. Although the delay deteriorates with the increase of node speed, the change is slow and tends to be peaceful, which greatly guarantees the end-to-end delay time. And the other three algorithms, compared with the algorithm in this paper, is not good in the performance of end-to-end time delay, and with the growth of node speed, their time delay becomes more worse.

Fig. 8 is comparison of delivery radio of four routing algorithms in a safe environment. It can be seen that the algorithm proposed in this paper performs worse than the algorithm proposed in reference [10] within a certain range of node moving speed. The reason may be that the two paths of AODV-MQS algorithm simultaneously broke during this interval, which caused more data packets to loss. After that, it can be recovered quickly with the acceleration of the node movement speed, because two paths to the destination node are restored in the blockchain. As a whole, the algorithm proposed in this paper can control the packet rate at about 90%, which effectively ensures the smooth operation of the network.

Fig. 9 is comparison of delivery radio of four routing algorithms in an unsafe environment. It can be seen that the algorithm proposed in this paper is obviously better than the other three types of algorithms. With the increase of nodes moving speed, the packet delivery rate decreases to a

certain extent, but when the speed increases again, the packet delivery rate rises, the main reason is that this paper adopts the blockchain technology to screen the nodes entering the blockchain network, which ensures the reliability of the nodes on the data transmission path. In addition, the algorithm proposed in this paper adopts alternative paths and constraints to ensure the safety of path transmission as much as possible.

Fig. 10 is comparison of overhead of four routing algorithms in a safe environment. It can be seen that the algorithm proposed in this paper performs better performance than the other three types of algorithms. But the blockchain technology used in this paper requires repeated inspections of nodes one by one in the construction of the blockchain network. A lot of control packages must be wasted. The experiment adjusted the QoS parameters and removed the consideration of risk factors. Therefore, the proposed algorithm can effectively adapt to changes in the communication environment by adjusting QoS parameters.

Fig. 11 is comparison of overhead of four routing algorithms in an unsafe environment. It can be seen that the proposed algorithm in this paper performs the best effect, because the use of blockchain technology only needs to waste some control packets when the route is established, which ensures the safety of the data in the transmission process. The other three algorithms are more likely to be broken in the process of data transmission than the proposed algorithm in this paper, and because of the existence of abnormal nodes, the reconstruction of routing will inevitably cause a lot of control overhead. Therefore, the control overhead of the other three algorithms is larger than proposed algorithm in this paper.

Simulation results show the superiority of the proposed algorithm. It can be seen from the simulation experiments that the algorithm proposed in this paper performs better network performance than the other algorithms, at the same time, the increase of control overhead and end-to-end delay are controlled effectively. The conclusion also further confirms that the use of blockchain technology in dealing with packages delivery equips with obvious effect, which can greatly improve the routing security problems.

5 Conclusion

A multipath QoS routing security algorithm based on blockchain is proposed in this paper. AODV-MQS is an on-demand QoS routing security algorithm based on the improved AODV protocol using the technology of blockchain. Firstly, the abnormal nodes are avoided effectively by using path survivability constraints and blockchain technology. Secondly, two optimized paths are chosen. Finally, routing security of Ad Hoc network is increased greatly. The application of blockchain technology in Ad Hoc networks routing security is a new method, there are many aspects that need further study, such as data transmission encryption, consensus algorithm, energy distribution, etc.

List of Abbreviations

QoS：Quality of Service.

AODV：Ad hoc On-Demand Distance Vector.

AODV-MQS ： A multi-path QoS routing security algorithm based on blockchain by improving the traditional AODV protocol.

EERQ: The detection packets.

Eq.: Equation.

R-P: Proportion of control overhead.

Acknowledgements

The authors acknowledged the anonymous reviewers and editors for their efforts in valuable comments and suggestions. And thanked the Hengshui University and Wonkwang University for the use of their equipment.

Funding

This work was supported by the Project of Hebei Province for Department of Education Youth Fund (Grant No. QN2020520), and Hebei Province for Science and Technology Department Science Popularization (Grant No. 20550301K), and the Teaching Reform Project of Jiangxi Provincial Department of Education (Grant No. JXJG-17-17-15), and the National Social Science Foundation of China (Grant No. 18XXW011).

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions

Shuailing Yan proposes the innovation ideas, and Conglin Ran does the theoretical analysis, Liang Huang carries out experiments and data analysis. Lei Zhang participated in its design and coordination and helped to draft the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1] Department of Information Technology Center, Jiujiang University, Jiujiang ,332005, P.R.China

[2]Department of Mathematics and Computer Science, Hengshui University, Hengshui, 053000, P. R. China

[3] School of Mathematics & Computer Science, Shangrao Normal University, Shangrao, 334001, P.R. China

[4]Department of Computer and Software Engineering, Wonkwang University, Iksan, 54538, Republic of Korea

Reference

[1] Pal, A., Dutta, P., Chakrabarti, An efficient load balanced stable multi-path routing for mobile ad-hoc network. Microsyst Technol. 2020(1), 101-112(2020).

[2] A. M. Shantaf, S. Kurnaz and A. H. Mohammed, Performance Evaluation of Three Mobile Ad-hoc Network Routing Protocols in Different Environments. 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 1-6(2020).

[3] K. Lei, Q. Zhang, J. Lou, B. Bai and K. Xu, Securing ICN-Based UAV Ad Hoc Networks with Blockchain. IEEE Communications Magazine 57(6), 26-32(2019).

[4] A. S. Al Hasan, M. S. Hossain and M. Atiquzzaman, Security threats in vehicular ad hoc networks. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 404-411(2016).

[5] N. Nishanth and A. Mujeeb, Modeling and Detection of Flooding-Based Denial-of-Service Attack in Wireless Ad Hoc Network Using Bayesian Inference. IEEE Systems Journal 2020(3),1-10(2020).

[6] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs.2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). 28-33(2019).

[7] W. Wei, H. Song, H. Wang and X. Fan, Research and Simulation of Queue Management Algorithms in Ad Hoc Networks Under DDoS Attack. IEEE Access 5(1), 27810-27817(2017).

[8] M. Karthigha, L. Latha and K. Sripriyan, A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks. 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 396-402(2020).

[9] J. Tang,A. Liu,Z. Jian,N. Xiong,Z. Zeng,W. Tian, A Trust-Based Secure Routing Scheme Using the Traceback Approach for Energy-Harvesting Wireless Sensor Networks. Sensors, 18(3),751(2018).
[10] T. Poongodi, M. S. Khan, R. Patan, A. H. Gandomi and B. Balusamy, Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks. IEEE Access 7(1), 18409-18419(2019).
[11] H. Moudni, M. Er-Rouidi, H. Mouncif and B. El Hadadi, Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks. 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV). 385-389(2016).
[12] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). 28-33(2019).
[13] W. Guo, N. Xiong, H. Chao, S. Hussain, G. Chen, Design and analysis of self-adapted task scheduling strategies in wireless sensor networks, Sensors 11 (7), 6533-6554(2011).
[14] X. Wu, Y. Zhang, A. Ming, et al, "MNSSp3: Medical big data privacy protection platform based on Internet of things", Neural Computing & Application, 2020. https://doi.org/10.1007/s00521-020-04873-z.
[15] H. Liang, D. Zou, Z. Li, K. Muhammad Junaid, Y. Lu, Dynamic evaluation of drilling leakage risk based on fuzzy theory and PSO-SVR algorithm. Future Generation Computer Systems 95, 454-466(2019).
[16] X. Wu, H. Wang, D. Wei, M. Shi, ANFIS with natural language processing and gray relational analysis based cloud computing framework for real time energy efficient resource allocation. Computer Communications. 150, 122-130(2020).
[17] S. Gupta, S. Kar and S. Dharmaraja, BAAP: Blackhole attack avoidance protocol for wireless network. 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011). 468-473(2011).
[18] Hongmei Deng, Wei Li and D. P. Agrawal, Routing security in wireless ad hoc networks. IEEE Communications Magazine 40(10), 70-75(2002).
[19] C. Jiang, R. Li, T. Chen, C. Xu, L. Li, S. Li, A two-lane mixed traffic flow model with drivers' intention to change lane based on cellular automata. International Journal of Bio-Inspired Computation 6(4),229-240(2020).
[20] P Papadimitratos, Z Haas, Secure message transmission in mobile ad hoc networks. Elsevier Ad Hoc Networks Journal 1(1), 193-209(2003).
[16] ELSEMARY A M, DIAB H, BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. IEEE Access, 95197-95211(2019).
[21] Sankara Narayanan S, Murugaboopathi G, Modified secure AODV protocol to prevent wormhole attack in MANET. Concurrency and Computation: Practice and Experience 32(4), 112-1232019.
[22] Aswale A.B., Joshi R.D, Security Enhancement by Preventing Wormhole Attack in MANET. Innovations in Electronics and Communication Engineering 107(1), 225-237(2020).
[23] 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 6(1), 27324-27335(2018).
[24] Lazrag H , Chehri A , Saadane R , Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. Concurrency and Computation: Practice and Experience.10(2),6-15(2020).
[25]Goyat R , Kumar G , Rai M K , Blockchain Powered Secure Range-Free Localization in

Wireless Sensor Networks. ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING, 18(3),6(2020).
[26] Firdaus M , Rhee K H , On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. Applied Sciences, 11(1),4-14(2021).
[27] H. Liang, J. Zou, K. Zuo, K. Muhammad Junaid, An improved genetic algorithm optimization fuzzy controller applied to the wellhead back pressure control system. Mechanical Systems and Signal Processing 142, 106708(2020).
[28] X. Wu, Y. Wei, Y. Mao, L. Wang, A differential privacy DNA motif finding method based on closed frequent patterns. Cluster Computing. 21, 1-13(2018).
[29] M. Karthigha, L. Latha and K. Sripriyan, A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks. 2020 International Conference on Inventive Computation Technologies (ICICT), 396-402(2020).
[30] H. Zheng, W. Guo, N. Xiong, A kernel-based compressive sensing approach for mobile data gathering in wireless sensor network systems, IEEE Transactions on Systems, Man, and Cybernetics: Systems 48 (12), 2315-2327(2017).
[31] N. Xiong, W. Han, A. Vandenberg, Green cloud computing schemes based on networks: a survey IET Communications, 6(18), 3294-3300(2012).

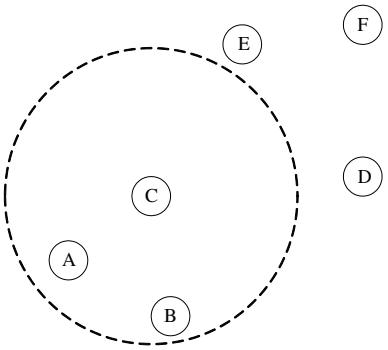

Figure 1. Connectivity of the node C

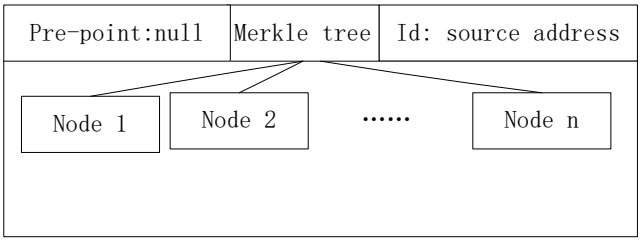

Figure 2. Genesis block

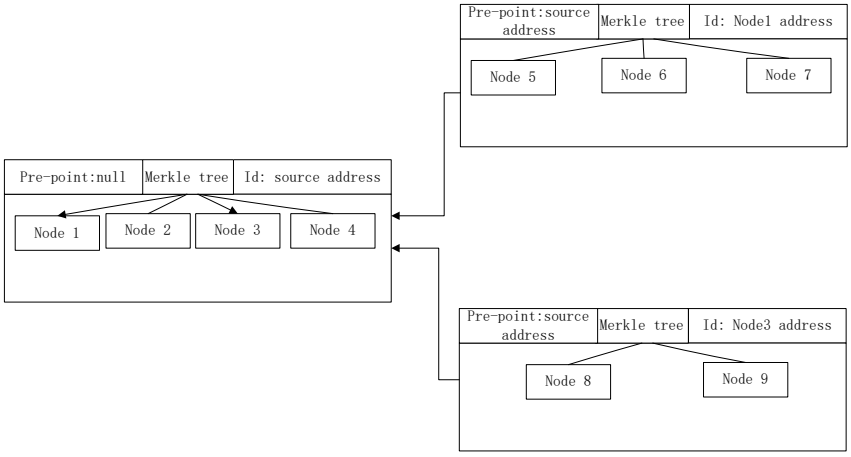

Figure 3. Nodes connection

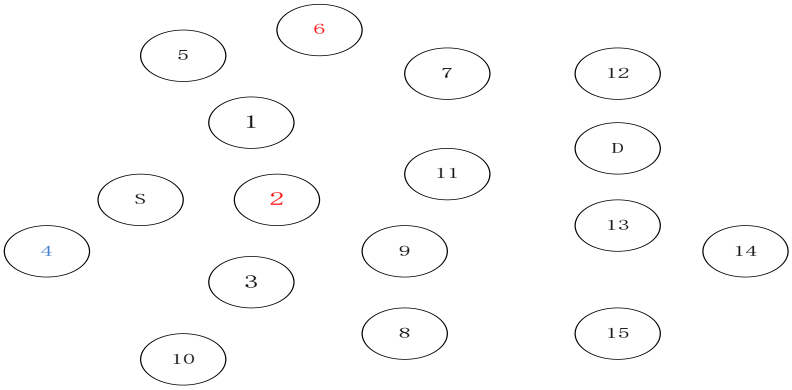

Figure 4. Ad Hoc network

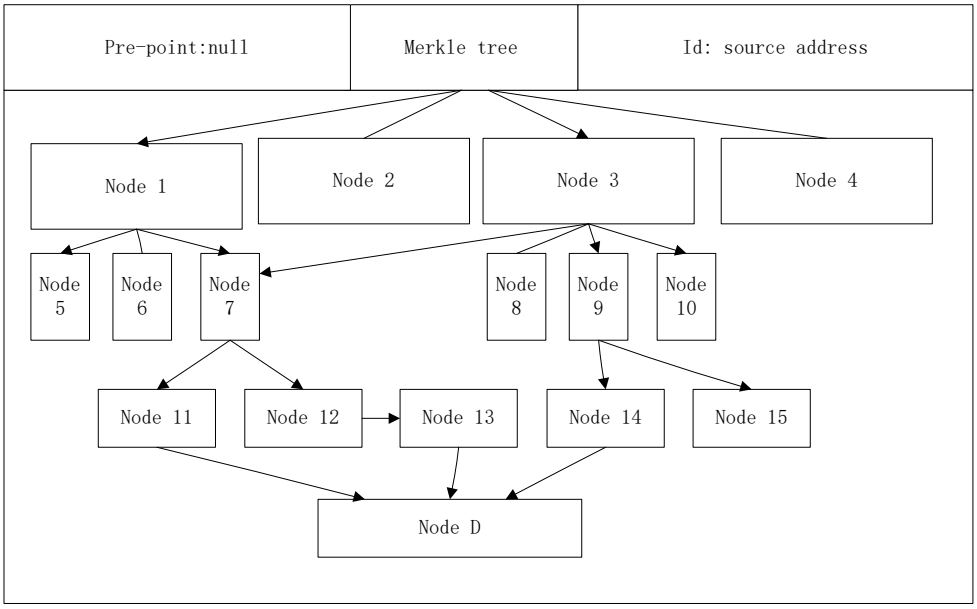

Figure 5. Source node result block

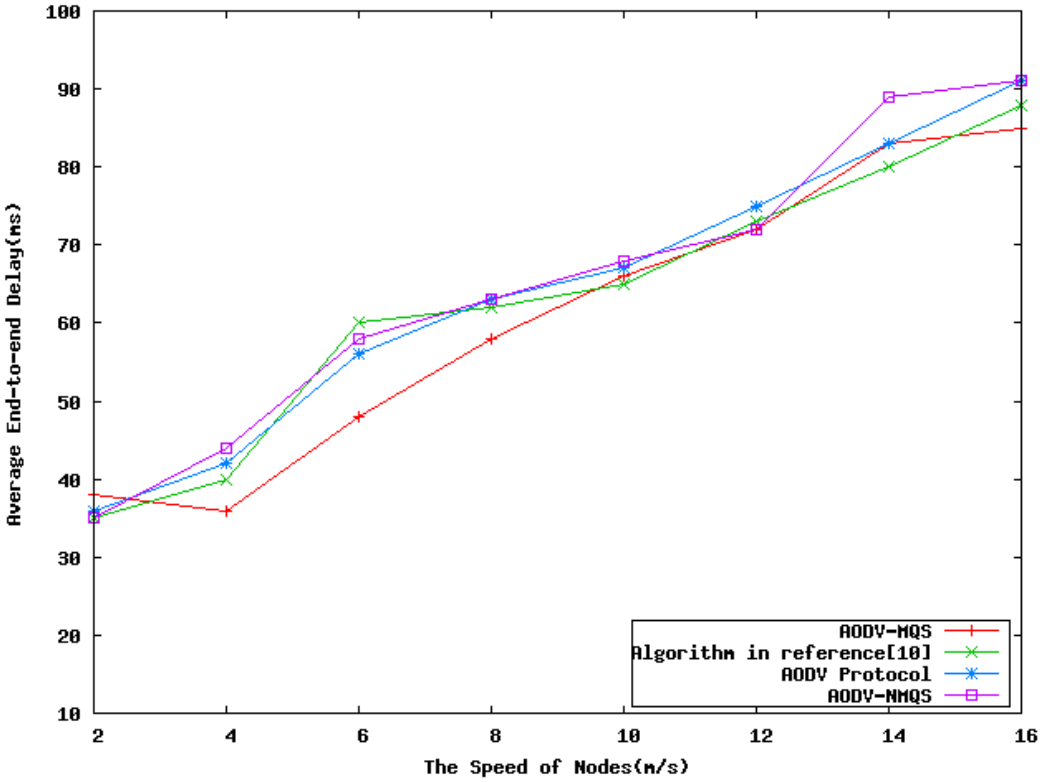

Figure 6. Comparison of end-to-end delay of four routing algorithms in a safe environment

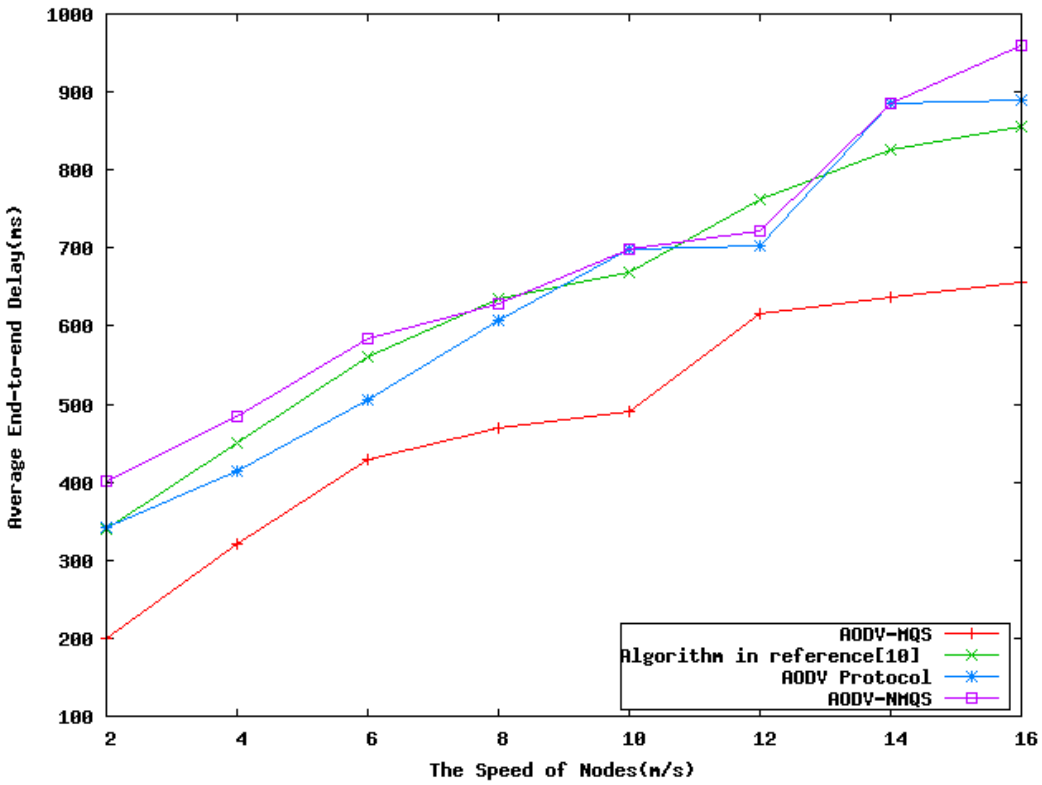

Figure 7. Comparison of end-to-end delay of four routing algorithms in an unsafe environment

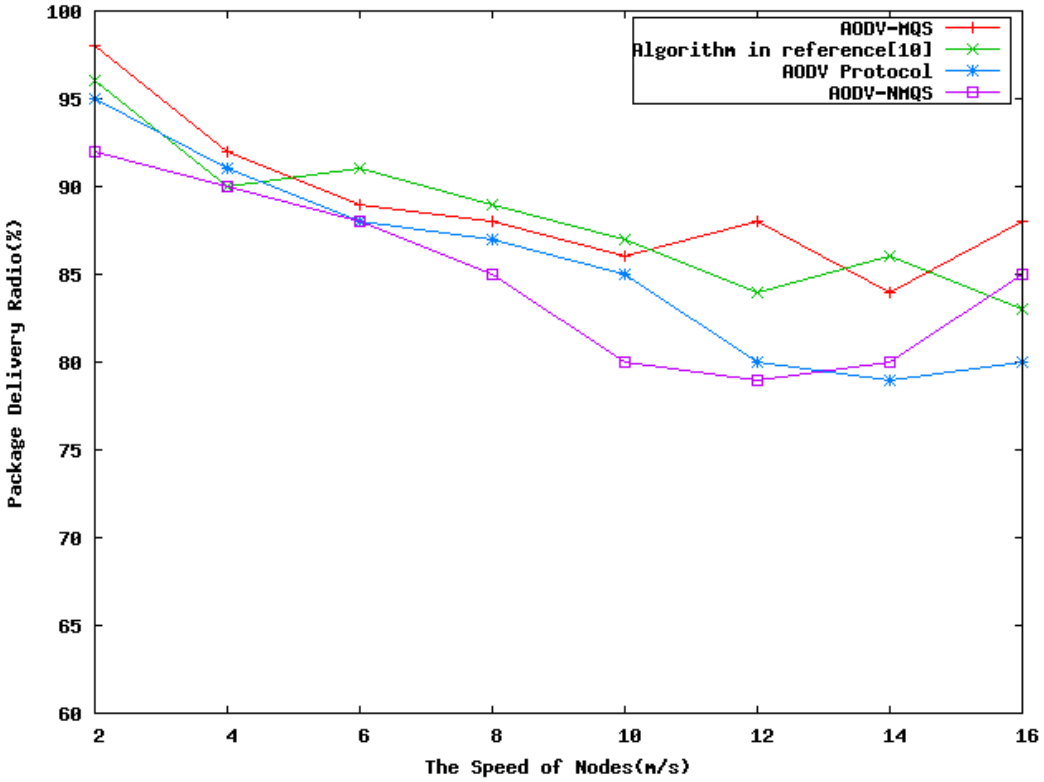

Figure 8. Comparison of delivery radio of four routing algorithms in a safe environment

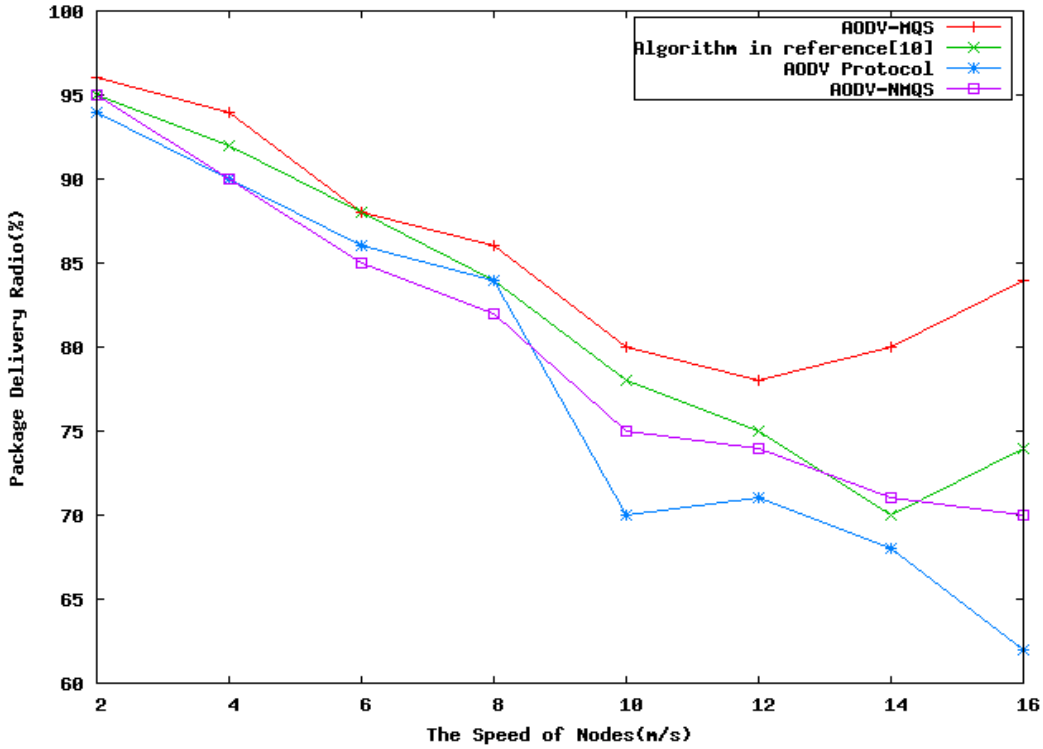

Figure 9. Comparison of delivery ratio of four routing algorithms in an unsafe environment

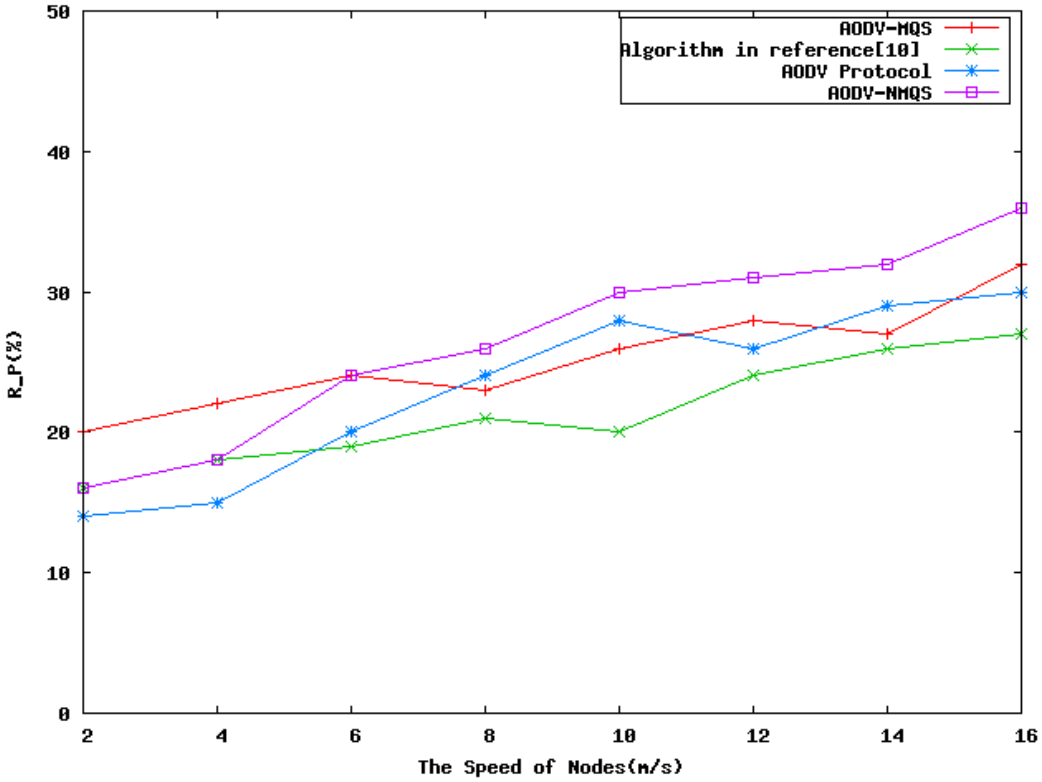

Figure 10. Comparison of overhead of four routing algorithms in a safe environment

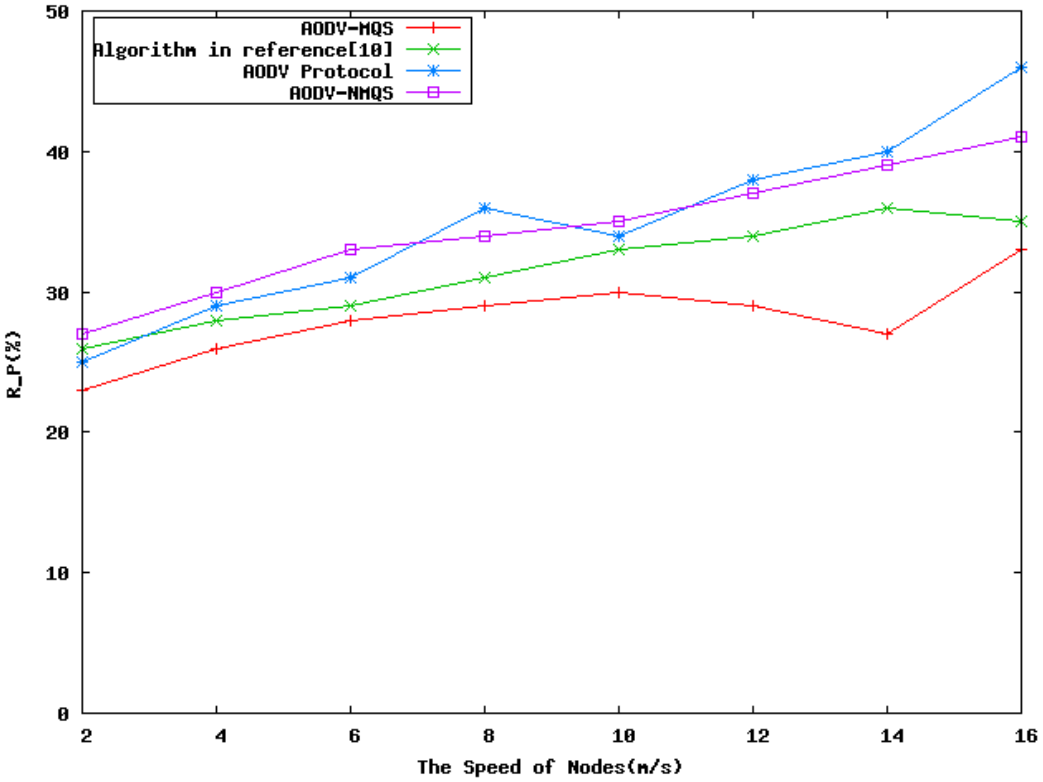

Figure 11. Comparison of overhead of four routing algorithms in an unsafe environment

Figures

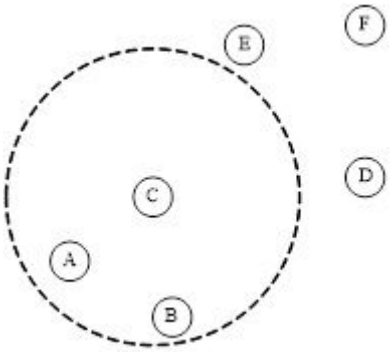

Figure 1

Connectivity of the node C

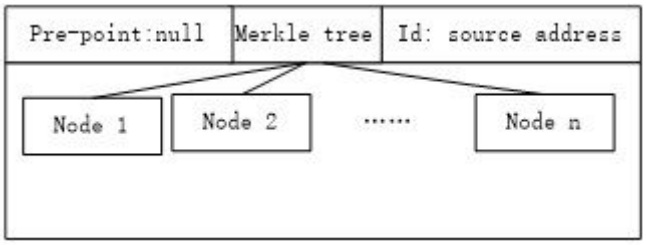

Figure 2

Genesis block

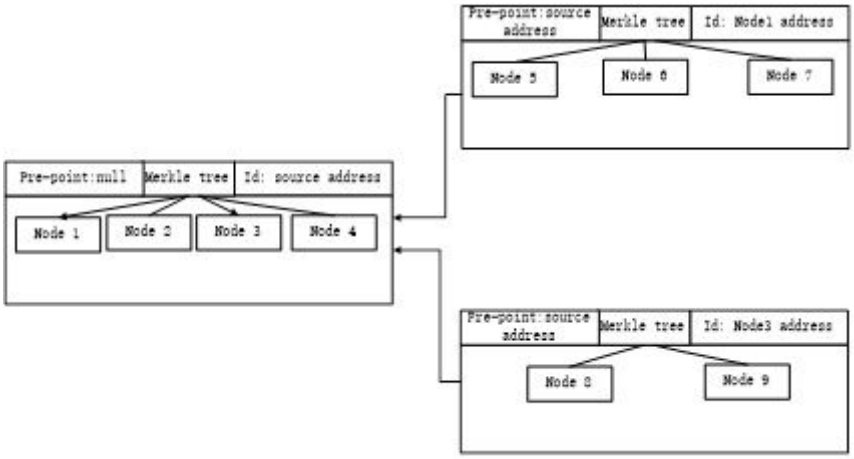

Figure 3

Nodes connection

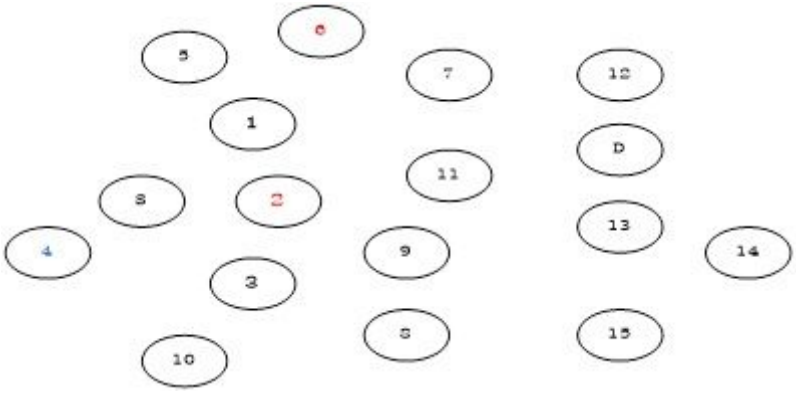

Figure 4

Ad Hoc network

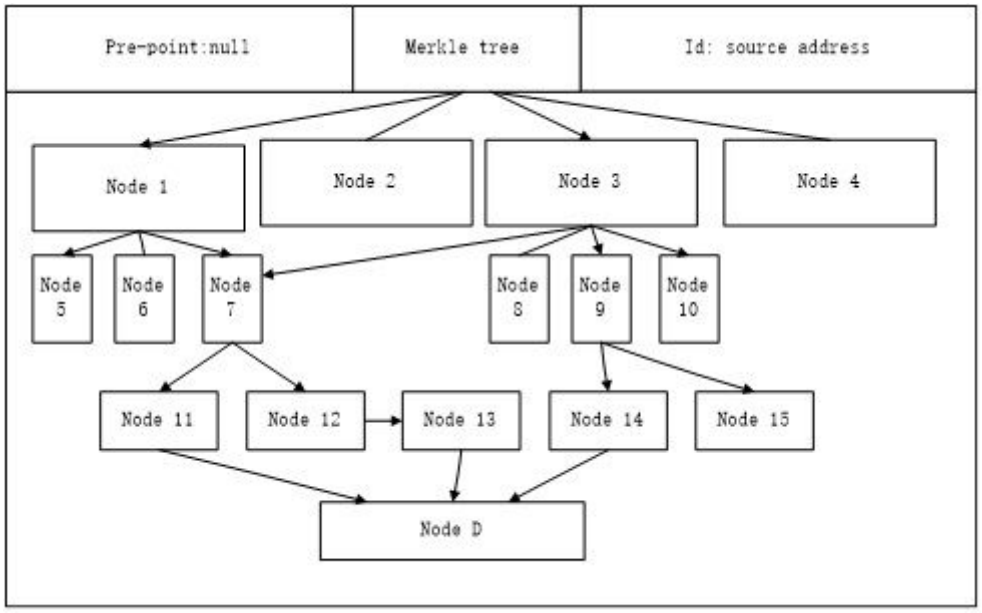

Figure 5

Source node result block

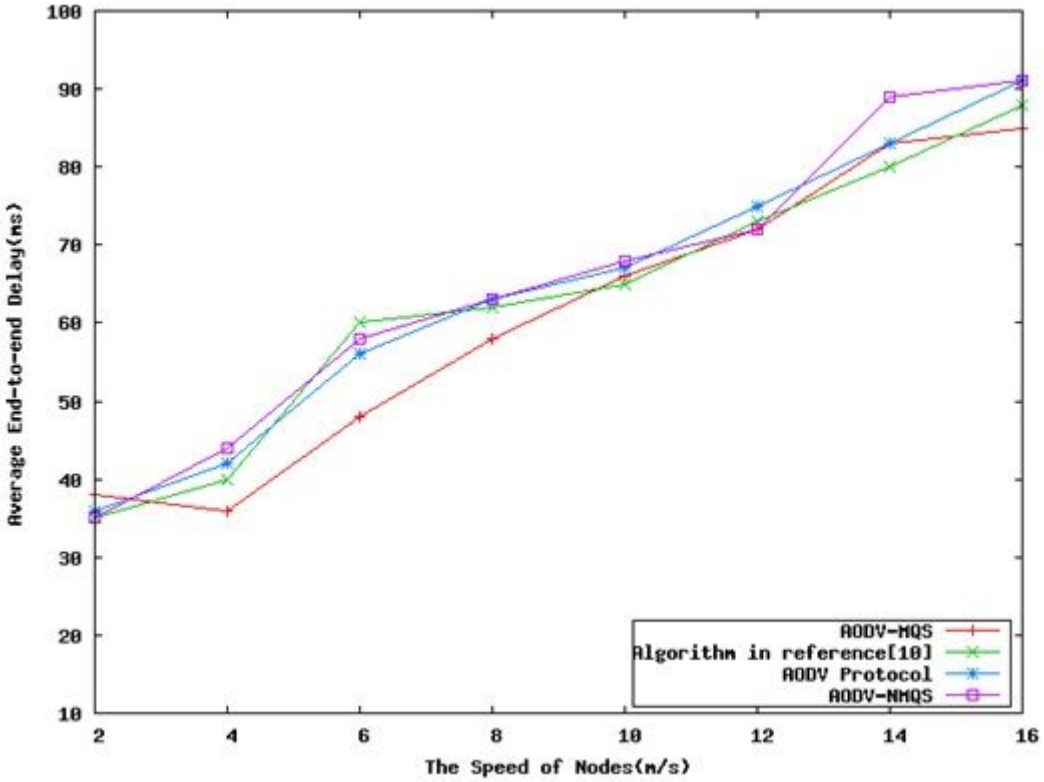

Figure 6

Comparison of end-to-end delay of four routing algorithms in a safe environment

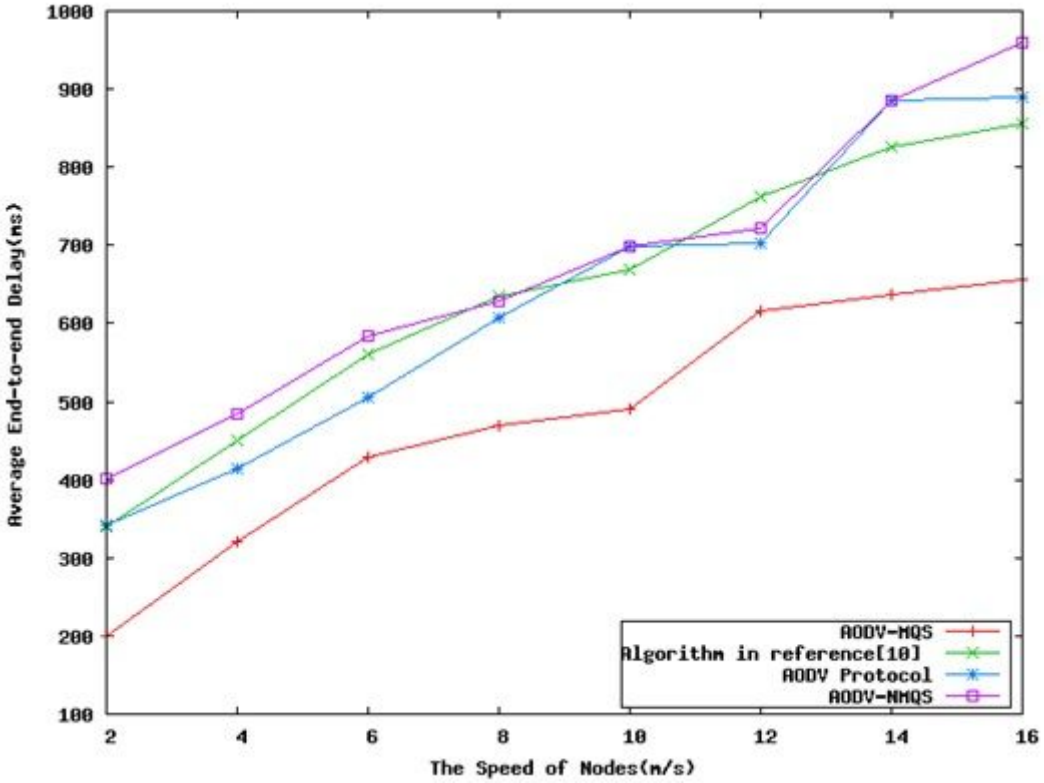

Figure 7

Comparison of end-to-end delay of four routing algorithms in an unsafe environment

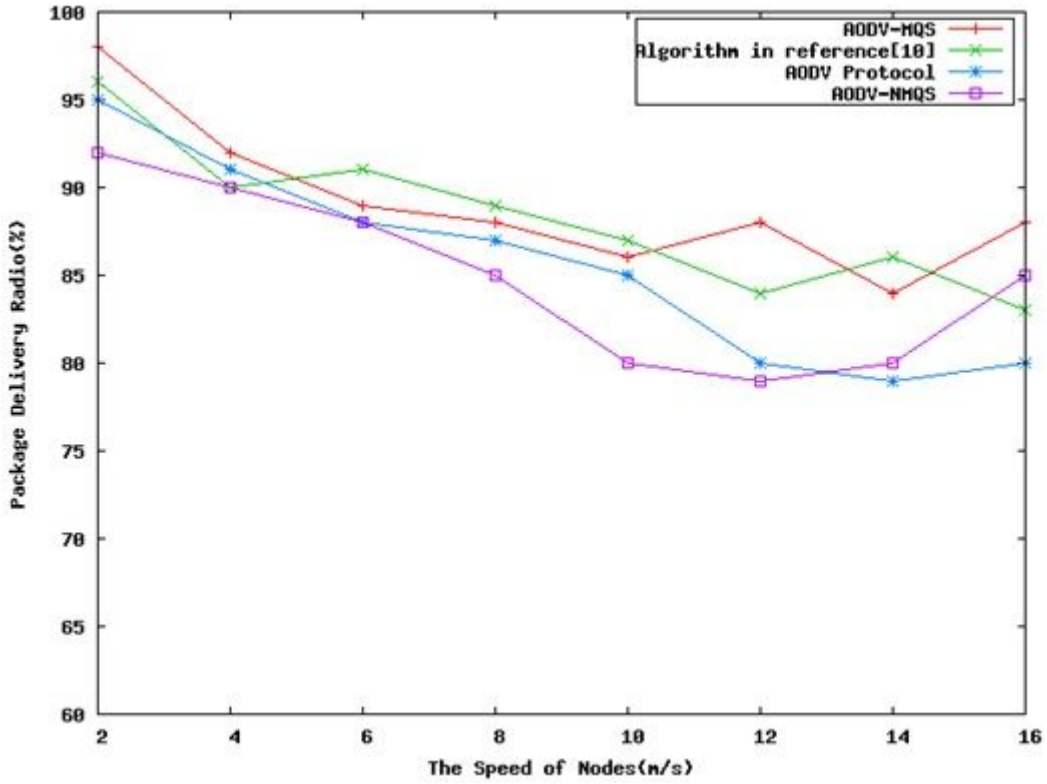

Figure 8

Comparison of delivery radio of four routing algorithms in a safe environment

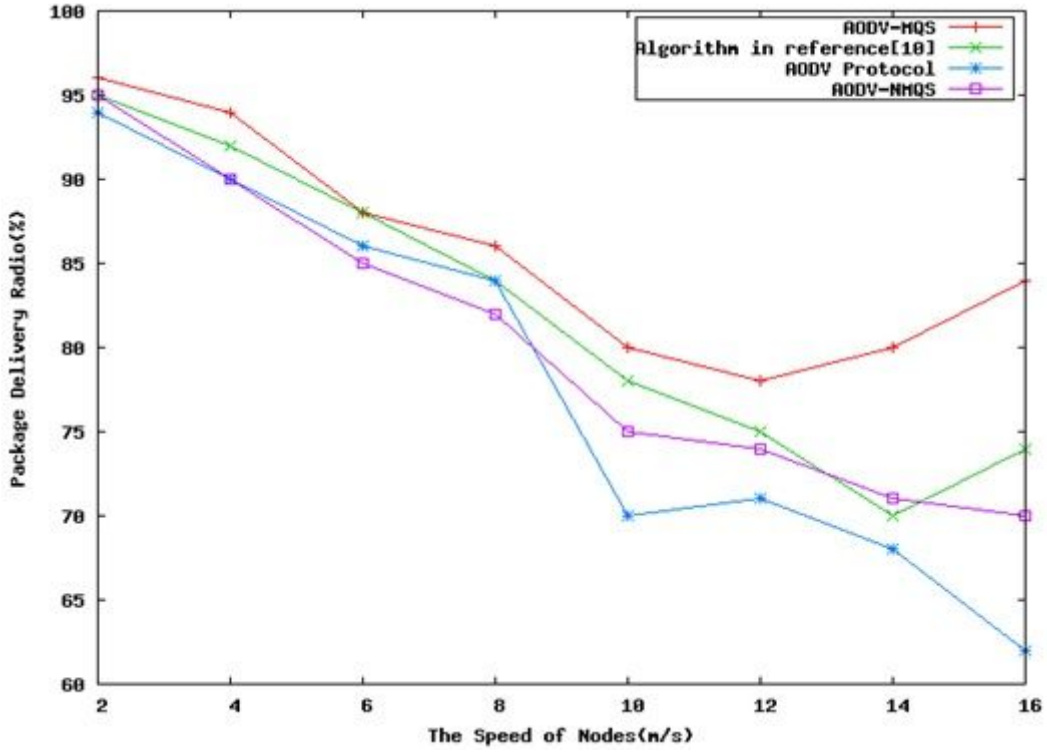

Figure 9

Comparison of delivery ratio of four routing algorithms in an unsafe environment

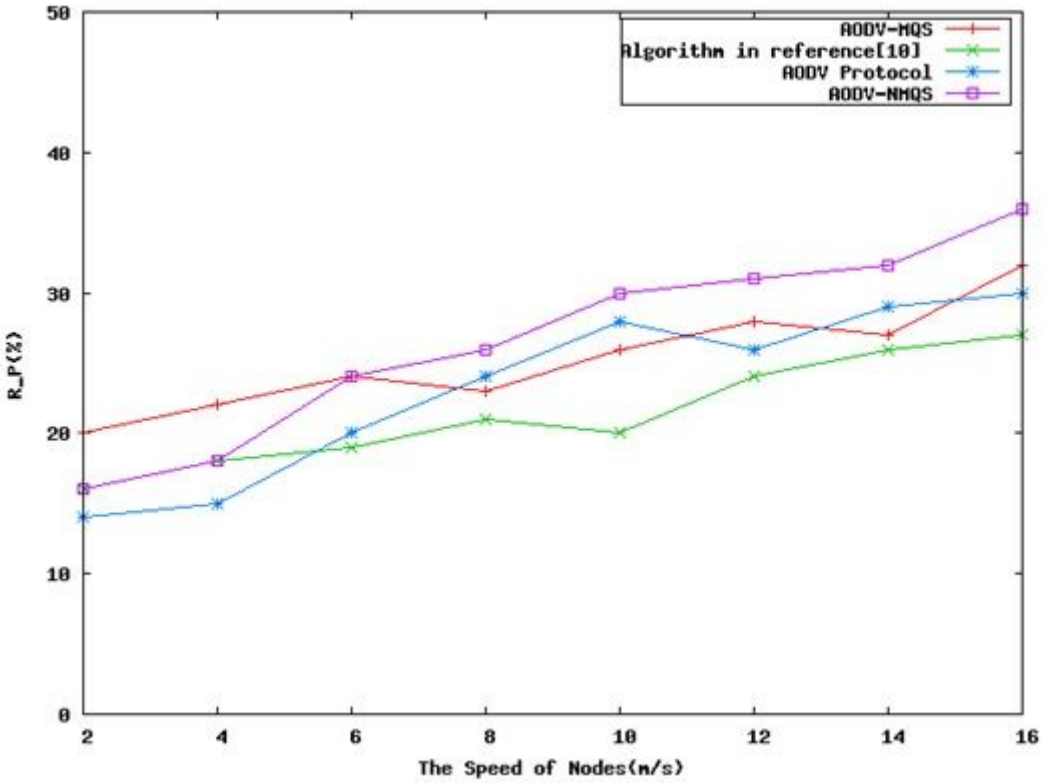

Figure 10

Comparison of overhead of four routing algorithms in a safe environment

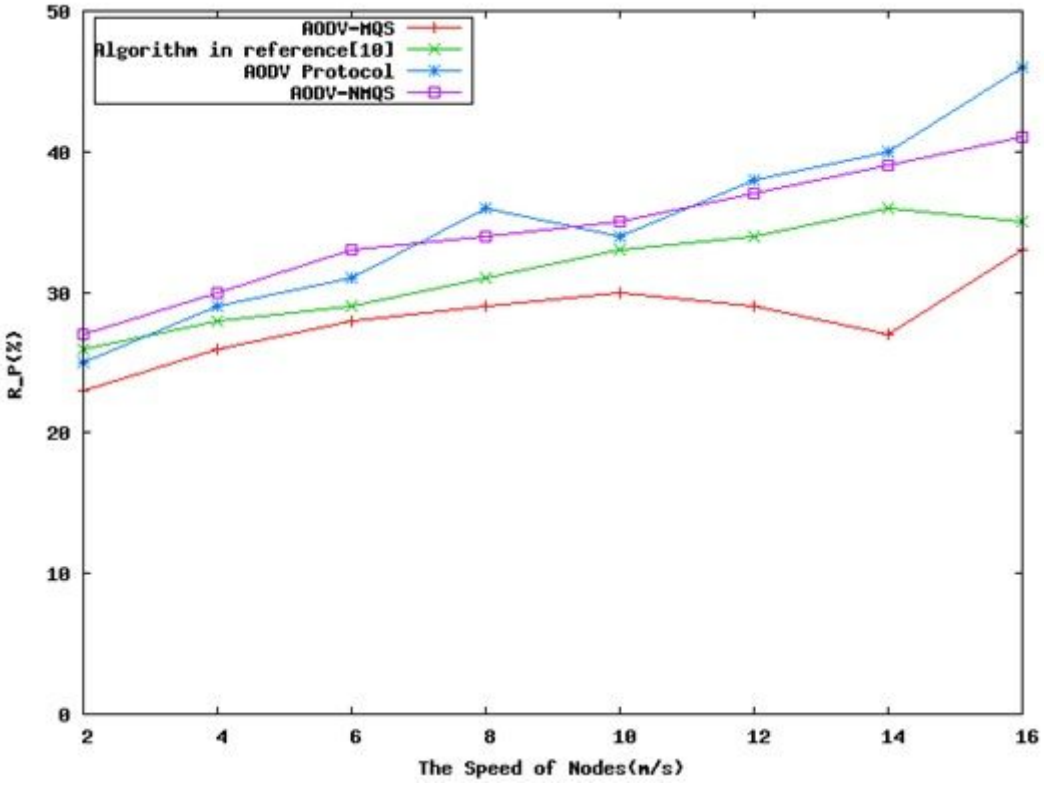

Figure 11

Comparison of overhead of four routing algorithms in an unsafe environment