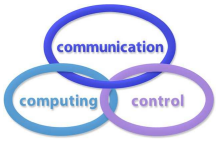
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 18, Issue: 3, Month: June, Year: 2023
Article Number: 5005, https://doi.org/10.15837/ijccc.2023.3.5005



CCC Publications

Invulnerability Improvement of Multipath Protocols in Different Scenarios

Quan-Hai Wang, Shao-feng Lan, Dian Zhang, Yi-Qun Wang, Qunxi Zhu, Wen-bai Chen

Quan-Hai Wang
Northeastern University at Qinhuangdao,
No. 143 Taishan Road, Northeastern University Qinhuangdao Branch, Qinhuangdao, China
276750743@qq.com

Shao-Feng Lan
School of Automation, Beijing Information Science and Technology University,
No.35 North 4th Ring Middle Road, Chaoyang District, Beijing, China
lanshaofeng01@163.com

Dian Zhang
School of Automation, Beijing Information Science and Technology University,
No.35 North 4th Ring Middle Road, Chaoyang District, Beijing, China
iszhangdian@126.com

Yi-Qun Wang
School of Automation, Beijing Information Science and Technology University,
No.35 North 4th Ring Middle Road, Chaoyang District, Beijing, China
wangyiqun@bistu.edu.cn

Qun-Xi Zhu
Northeastern University at Qinhuangdao,
No. 143 Taishan Road, Northeastern University Qinhuangdao Branch, Qinhuangdao, China
qhddjks@qq.com

Wen-Bai Chen
School of Automation, Beijing Information Science and Technology University,
No.35 North 4th Ring Middle Road, Chaoyang District, Beijing, China
*Corresponding author: chenwb@bistu.edu.cn

Abstract

Developments in computer communications and networks enabled the deployment of exciting new areas. Meanwhile, Efficient network and communication technologies also promote the development of routing protocols. AODV(Ad hoc On-Demand Distance Vector Routing, AODV) routing protocol has invulnerability to different mobile attributes of agent nodes and network damage scenarios. However, this invulnerability performance can not meet the needs of mobile multi-agent cooperative communication. Therefore, this paper proposes an improved responsive

multipath routing protocol MD_AODV(Multipath Destroy-resistance AODV, MD_AODV). This routing protocol is based on AODV routing protocol. It is mainly improved in three aspects: multi-channel concurrency mechanism, node load balancing mechanism and shortest path maintenance mechanism. Firstly, in this research, an improved multipath routing protocol is modeled and implemented, which is based on OPNET Network simulation platform. Then, network models with different degrees of impairment are built. Combines the mobile attributes of mobile multi-agent task coordination to carry out invulnerability simulation experiments . These experiments study the invulnerability of the improved multipath routing protocol. Finally, this paper evaluates and compares the routing invulnerability of MD_AODV, AODV and AOMDV(Ad-hoc On-Demand Multipath Distance Vector, AOMDV). The evaluation results show that MD_AODV routing has better invulnerability when the network is severely damaged.

Keywords: AODV protocol, Multipath routing, Network Invulnerability, Opnent simulation.

1 Introduction

Mobile multi-agent system can carry out complex task cooperation and agent mobility, which is carried out under the condition of the integrity of the communication link between the agent nodes[1]. Routing control technology is the key technology of agent cooperative communication. It is also a routing protocol with high reliability and fault tolerance. The routing control technology will ensure that the mobile multi-agent can successfully complete the collaborative task when the network is impairment. Therefore, it is very meaningful to study the invulnerability of mobile multi-agent routing protocols.

At present, there are three routing protocols that can be applied to mobile multi intelligent systems. These three routing protocols are proactive routing protocols, reactive routing protocol and hybrid routing protocol[2]. AODV protocol is a common reactive routing protocol3. It is widely used in different scenarios, but it is a single path protocol. When the link of AODV protocol is disconnected, it is necessary to re initiate the routing request.[4] However, this will increase the route initiation frequency and end-to-end delay. In recent years, researchers have proposed many schemes to improve the performance of AODV protocol. After considering multiple routing information, Zhang et al. [5]proposed a new protocol to improve AODV, called SAODV(Secure AODV,SAODV). In SAODV, improving the selected route needs to combine different routing standards. These include the length of the path and information from network status. Based on these, the new route is optimized for the target application. Alebed et al. [6]proposed a routing protocol called AOMDV. It is an extension of the AODV protocol. This research mainly analyzes and improves AODV in multi-channel concurrency mechanism, node load balancing mechanism and shortest path maintainer. Therefore, an improved responsive multipath routing protocol MD_AODV is proposed.

For the network environment without infrastructure support, especially the invulnerability of routing protocols in mobile multi-agent networks, the research mainly focuses on three aspects. The first is the routing invulnerability of link redundancy. The second is the research of routing invulnerability based on link repair. Thirdly, routing invulnerability research based on high dynamic topology. Although these three aspects are related, their respective characteristics and the application background on which the research is based are not the same. S. J.lee et al. [7]proposed AODV-BR(Ad Hoc on-demand distance vector-backup routing, AODV-BR) on-demand backup routing protocol with link redundancy. On demand backup routing stability's disadvantage is that the backup routes enabled by the network are often not applicable to the current topology[8]. The algorithm is effective when the nodes in the network are relatively fixed. However, when the network nodes move in a large range and at a high speed, the performance is not outstanding. Moreover, this algorithm does not study the invulnerability in the case of network damage. Marina et al. [9]studied AOMDV on-demand multipath routing protocol. It backs up multiple routing sequences from the source node to the destination node to save the cost of route discovery. The research on this protocol shows that the repair ability of this routing protocol is not as good as the traditional AODV on-demand single path routing protocol when the network topology changes dramatically and the network scale is small. Yang et al. [10]considered the link failure caused by the decrease of node communication distance during data transmission. Propose A MANET Routing Strategy with maximum survival path. This strategy can reasonably

select the path to transmit data according to the residual energy value of the node.

These studies are basically to improve the original network routing protocol, and to some extent increase the robustness of the original routing strategy. However, the above research did not study and analyze the invulnerability of network routing protocols based on network damage and task cooperative mobility attributes of mobile Multi-Agent. This paper proposes an improved responsive multipath routing protocol called MD_AODV. In addition, this paper also studies the invulnerability of MD_AODV by combining the mobile attributes of mobile multi-agent and the degree of network damage.

Based on MD_AODV, this paper improves the multi-channel concurrency mechanism, node load balancing mechanism and shortest path maintenance mechanism. In view of the different requirements of the damage degree of the network on the Invulnerability, a network model with different damage degree is constructed. This paper combines the mobile attributes of mobile multi-agent task coordination, and carries out the Invulnerability Simulation Experiment of the improved multipath routing protocol under the scenarios of different degrees of network damage. This paper evaluates the Invulnerability of the above experiments and compares them with AODV[11] and AOMDV routing protocols.

2 Modeling process of mobile multi-agent network

2.1 Invulnerability of mobile multi-agent network

From the way of network impairment, the factors affecting the invulnerability of mobile multi-agent can be divided into four aspects. These four aspects are the agent's own factors, the wireless communication mode, the agent's mobility and the continuous change of network scale.[12]

Similarly, there are four strategies to improve the invulnerability of multi-agent networks. These four aspects are communication link hardware protection, topology evolution, network reconfiguration and routing control. Among them, hardware protection, network reconfiguration and topology evolution of communication links are all invulnerability optimization strategies in hardware. Enhancing the invulnerability of network reconfiguration and topology evolution is achieved by optimizing network heterogeneity or coverage. Routing control is a necessary software optimization technology in network communication. It can improve the invulnerability of mobile multi-agent based on the original hardware and topology of the system. Figure 1 shows a strategy to improve the invulnerability of mobile multi-agent systems.(Figure1)

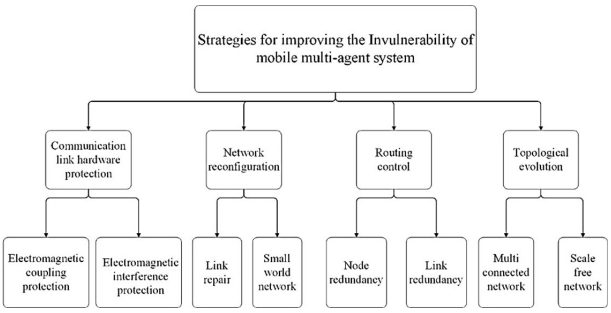


Figure 1: strategies for improving the Invulnerability of mobile multi-agent system

2.2 Mobile multi-agent Invulnerability Simulation Platform

OPNET simulation platform[13] has excellent communication networks, facilities, protocols, simulation algorithms and modeling mechanisms. It has also been unanimously recognized by the professional field and research field of network communication. In order to better simulate the real network, the network model of OPNET is usually composed of process model, node model and network model. Among them, the process model regulates, makes decisions and implements algorithms for the behaviors of nodes in the system. The node model is used to standardize the functions of applications,

processes, queues and communication interfaces to nodes. The network model is used to standardize the system from high-level devices (i.e. nodes and communication links).

The modeling steps of mobile multi-agent network are divided into three layers. [14]The first layer is mainly the description of network topology, network scope and subnet, that is, network domain modeling. The second layer refers to the description of various node models that make up the network topology. The interior of the network node is generally established according to the OSI (open system interconnection) model[15]. Each layer is similar to a process, and different threads can be run in the process according to different protocol mechanisms; Between processes, that is, between layers, variables can be transferred by setting pipelines or promoting variable attributes, that is, node domain modeling. The third layer is process domain modeling. Process domain modeling describes the processes that make up the node model through c/c++ language, OPNET's own API and finite state machine mechanism.[16]

The process model is the main body of generating and processing events in OPNET. This is the key to the invulnerability simulation of mobile multi-agent. Similar to the circular data scheduling mechanism of single core processor, it enters different sub functions through flag bits and processes the data. There are four main process models involved in mobile multi-agent network modeling and simulation. The four models are network / routing layer model, MAC model, communication related physical layer model and node mobility model.

3 Network impairment model

3.1 Impairment model design

For the research on the Invulnerability of mobile multi-agent network, the typical analysis method is to compare the network characteristics under different damage conditions. Mobile multi-agent network can cause node failure to varying degrees due to its characteristics of node mobility, wireless communication, limited energy and network vulnerability.[17] Generally, electromagnetic interference, communication distance limitation, network attack and other scenarios can be summarized as recoverable network impairment caused by node failure, that is, slight impairment.[18] Generally, the node recovers its connection with the network through watchdog reset, adjusting node position and waiting for the end of the attack in about 10 100s. Sometimes, the network suffers from malicious attacks, and the energy of nodes is exhausted. Mechanical failure or interference of nodes due to their own and environmental reasons. All of these will cause the node to be disconnected from the network continuously, which can be summarized as the irrecoverable network damage caused by node failure, that is, severe damage.

Based on the typical task scenario of mobile multi-agent, 10 mobile nodes in the network are selected for different degrees of failure to simulate two different degrees of network damage. The number of mobile multi-agent nodes in the network is 50. After investigation, each mobile node and the network start to connect to the whole network and run stably, usually taking less than 10 minutes.[19] Therefore, the network damage time is set after 10 minutes, and the network simulation time is set to 20 minutes. The node model created in this paper does not support the global configuration of network failure by the failure recovery module of OPNET. The way to configure node invalidation under the node model established in this paper is to select break down time and break hold time parameters in the node attribute attribute to realize node invalidation and recovery. The node is only enabled outside the failure time.

Table1 describes the parameters of the network impairment model under the scenario of recoverable node impairment, and table 2 describes the parameters of the network impairment model under the scenario of unrecoverable node impairment.

- The network is slightly damaged, that is, after the node is damaged at a certain time, it can return to normal within the set time interval (see Table 1).

- The network is severely impairment, that is, the node will permanently fail after being damaged

Table 1: Network impairment model parameters of node impairment recoverable scenario

Serial number	Failed node ID	Impairment moment/s	Network impairment duration /s
1	2	600	100
2	7	610	90
3	10	620	80
4	14	630	70
5	26	640	60
6	29	650	50
7	31	660	40
8	35	670	30
9	44	680	20
10	47	690	10

at a certain time (see Table 2).

Table 2: Network impairment model parameters of node impairment irrecoverable scenario

Serial number	Failed node ID	Impairment moment/s	Network impairment duration /s
1	2	600	600
2	7	610	590
3	10	620	580
4	14	630	570
5	26	640	560
6	29	650	550
7	31	660	540
8	35	670	530
9	44	680	520
10	47	690	510

3.2 Construction of network damage model based on OPNET

In this paper, the degree of network damage is simulated by configuring failure parameters for the specified nodes in the same network scenario. The node failure and failure holding functions are realized in the MAC process model, specifically for the IDEL state machine in the 802_11_CSMA/CA_mac processor module to import Break Down Time and Break Hold Time variables. The function of IDEL state machine is to wait for packets from MAC layer and put them into wlan_interrupts_process() interrupt function for processing. The parameters related to the failure time are input from the node application layer to the MAC layer. So the node failure parameters will finally take effect in the wlan_higher_layer_data_arrival(void) function. If the application layer data packet is received and there is enough space in the upper layer data buffer, the data packet is queued for MAC layer processing. When the node is within the set Break Hold Time time, the node MAC layer will refuse to transmit data, so as to simulate the process of node failure.

4 Improved MD_ AODV multipath routing protocol

4.1 Improvement of routing protocol

There may be four reasons for the low Invulnerability of the network.[20] The first is that the AODV routing protocol fails to transmit network information due to the damage of the communication link in the node failure scenario. Second, the existing AODV multipath routing protocol node load balancing mechanism is not perfect. Third, the routing update of multipath single sending routing protocol is not timely. Fourth, it is difficult to adapt to the application scenario of dynamic change of mobile multi-agent network topology. In order to improve the problem of low network Invulnerability , this paper designs an improved multipath routing protocol based on the following three improvement ideas.

1) Multiple concurrency mechanism

When the source node needs to send data to the destination node, the source node will send application layer data in parallel from multiple routes found each time. MD_ AODV adopts this link

redundancy mechanism. When the mobile multi-agent network is disturbed and some nodes fail, the probability of data transmission failure will be inversely proportional to the number of effective paths. However, this situation is related to the transmission reliability of the same application layer data. This mechanism can effectively improve the data transmission success rate of the network.[21]

2) Node load balancing mechanism

When the network is establishing a route, when the node receives RREQ, it will first judge whether the node is already an intermediate route of the same type of RREQ. If so, it will discard the RREQ data to avoid forming a route intersected by nodes. If it is not the same type of RREQ, judge whether the number of local effective routing tables of the node reaches the maximum threshold. If it reaches the maximum threshold, discard the RREQ to avoid the load of the node exceeding the upper limit of the node itself.[20] The final network is a network system with node load balancing and disjoint nodes in the same type of routing.

3) Shortest path maintenance mechanism

In the process of route repair, AODV adopts the mechanism of local repair, while MD_ AODV routing adopts the mechanism of source node repair. MD_ AODV always selects the route with the least hops as the available route when discovering routes. After the route is disconnected, the repair from the source node can make the effective path from the source node to the destination node update a current best route in time, that is, the route with the smallest number of hops. For the network with node failure, from the probability event analysis, the fewer nodes in the network link, that is, the smaller the number of hops, the lower the probability of link damage. The smaller the number of routing hops, the lower the network transmission delay, and the overall link quality of the network will be improved.

4.2 Improved routing protocol design process

The overall process of MD_AODV routing protocol implementation is described as follows:

Step 1: initialize the status variable of the routing protocol. It mainly includes obtaining the internal relevant ID and node address of the node, obtaining the data cache queue memory area of the MD_AODV sub process, obtaining the number of nodes, initializing the serial number of this node, initializing RREQ_ID , initializing RREQ retransmission times, initializing RREP sending handle, creating multi-path cache queue, initializing the RREQ serial number received by the node, initializing the routing table and neighbor node table, initializing the RREQ request queue Set the maximum number of paths and set the maximum threshold of node load.

Step 2: wait and process the data from the upper and lower Mac. It mainly includes determining the node corresponding to the destination address of the packet, setting the packet domain and size of the data packet, counting the packets to be transmitted, refreshing the routing table entry, packet transmission and lower layer data packet processing. Step 3: data and network maintenance. It mainly includes RREQ retransmission after RREP timeout, periodic HELLO packet transmission, RRER processing and route repair after link disconnection.

The main implementation process of the improved multipath routing protocol is route discovery and route maintenance.

1) Route discovery

The source node needs to send data to the destination node. When the source node has multiple paths cached to the destination node, data will be sent from multiple paths in parallel. When there is no valid path to the destination node, the source node will broadcast RREQ. When the node receives the RREQ packet, it judges whether the number of effective paths loaded by the node reaches the set threshold, whether the RREQ packet reaches the maximum number of broadcast hops, and whether it has received the repeated RREQ message. If the above conditions are not met, the RREQ packet will be processed in the next step. Record the packet sequence number (RREQ_ID) and set the address of the First_Hop to update the route from this node to the source node. If the node is the destination node, feed back the RREP response packet. If it is not the destination node and does not reach the maximum broadcast range, continue to forward the RREQ message. The flow of updating the routing algorithm from the local node to the source node is shown in algorithm1. Based on the multiple effective paths from the source node to the destination node cached during route discovery,

Algorithm 1 Update the routing algorithm from the local node to the source node in RREQ

Input: input:the RREQ data received by the node and the routing list of the source node in the RREQ data

Output:

```
if Source node serial number in RREQ > The serial number of the destination node in the routing table corresponding to the source node address in RREQ then
    Clear the routing sequence information corresponding to the source node address in RREQ;
Write the latest next address, the next hop address after the group, the number of hops and the lifetime to the routing sequence;
Add the updated route sequence to the route list corresponding to the source node address in RREQ;
else if Source node serial number in RREQ == The serial number of the destination node in the routing table corresponding to the source node address in RREQ then
    if Number of routes corresponding to the source node address in RREQ > Maximum number of unicast paths (Path_num) then
        Discard RREQ message
        for j=0; j < The number of paths to the destination node corresponding to the source node in RREQ (Path_size) do
            if There is no node intersecting link between the local path and the original link of the routing table then
                for j=0; j < Path_size; j++ do
                    if Number of routing hops in RREQ (HopCount) < The number of hops in the routing sequence corresponding to the destination node address in RREQ then
                        Update routing sequence;Add the updated route sequence to the route list corresponding to the source node address in RREQ
                    end if
                end for
            elseDiscard RREQ message
            end if
        end for
    end if
elseDiscard RREQ message; // Expired RREQ information
end if
```

the destination node sends packet data immediately after receiving RREP. If multiple RREPs are received, multiple packet data will be sent accordingly, MD_ The AODV route discovery mechanism is shown in Figure2. In the process of route discovery, the mechanism of node load balancing is selected by judging the number of effective paths loaded by nodes and the disjoint links of nodes during route update.[22]

2) Route maintenance

The initial stage of route maintenance is similar to the AODV mechanism. It judges whether to send RRER message by periodically broadcasting Hello message. When the node receives RRER, it notifies its neighbor node and the previous hop node. Delete the route with this node as the next hop, and establish the route when the data application layer sends data again.[23] The processing flow of RRER packet information is shown in algorithm2. Local route repair and destination node route repair are not performed at this time. The reason is that in the scenario of node failure and frequent changes in mobile multi-agent network topology, the locally repaired route is often not the shortest route from the current destination node to the source node. Based on the basic characteristics of passive routing, the source node repair is not carried out at this time, but when the source node resends RREQ, in order to maintain the path from the source node to the destination node. The MD_AODV route maintenance process is shown in Figure3.

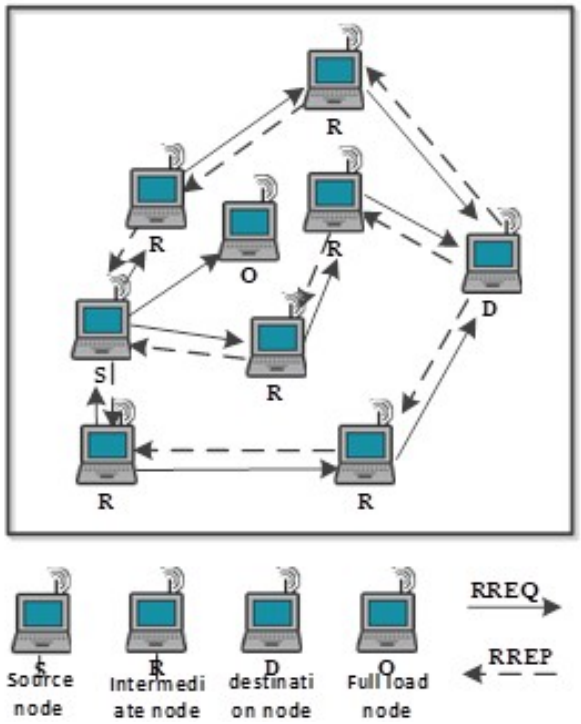


Figure 2: MD_ AODV route discovery process diagram

5 Analysis on Invulnerability of multipath routing protocol

5.1 Node damage recovers Invulnerability in network scenarios

5.1.1 Network scenario settings

The network scenario parameters of the mobile multi-agent node damage recoverable scenario are shown in Table 5. The node moving speed and moving path correspond to the moving speed and moving path in different collaborative mobile task models.

Table 3: Network impairment model parameters of node impairment irrecoverable scenario

parameter	Set value
Scene range	50km×50km
Number of nodes	50
Failed node item	10
Simulation time	20 min
Network damage moment	After 10 minutes of network operation
Network impairment type	Node damage recoverable model
Mobile scene	Random, formation maintenance, aggregation
Maximum communication distance of node	3000 m
Data transmission rate	1 Mbps

5.1.2 Evaluation of Invulnerability

1) Evaluation measure

Referring to the evaluation index of network topology Invulnerability[24] and the definition of network robustness, this paper proposes an index suitable for the Invulnerability evaluation of mobile multi-agent routing protocol, that is, network reliability. Considering that the probability of node failure in the actual network scenario is basically the same, the fewer nodes required for routing and forwarding, the lower the probability of the link being hit. Therefore, the average number of routing hops is used to evaluate the Invulnerability of routing protocols. In this paper, the Invulnerability of mobile multi-agent network routing protocol will be evaluated in combination with network throughput, reliability and average routing hops.

Algorithm 2 RREP packet data processing algorithm

Input: input:RREP data received by the node, source node data and destination node data in RREP data

Output:

if Node receives RRER packet data **then**
  Obtain the source node address (Source_addrr) and destination node address (Dest_addr) in RRER;Destroy the RRER packet data;
  if Number of broadcast hops corresponding to the destination node address in RRER (Broadcast_HopCount) < Total number of nodes in the network +1 **then**
    Path_size = Number of paths corresponding to the destination node address in RRER (Dest_addr.path);
    for j = Path_size-1; j ≥ 0; j– **do**
      Get route sequence information in the path (Path_info)
      if Next hop address in Path_info (Next_addr) == Source_addr **then**
        Delete the routing information corresponding to Dest_addr in Path_info;// The path corresponding to the destination node address in RRER has been updated
      end if
    end for
    if Number of paths corresponding to the destination node address in RRER (Dest_addr.path) == 0 && Path_size > 0 **then**
      while The forward address corresponding to the destination node address in RREQ (Dest_addr.Precursor_addrlist) > 0 **do**
        Clear the predecessor node (Pre_node_addr) corresponding to the Dest_addr.
      end while
      Source node address in RRER (Source_addr) = Local node address (My_node_addr); Number of repackaging RRER; Send RRER packet information to MAC for processing;
    end if
  end if
end if

(1) Network reliability

Network reliability refers to the characteristics of the system to complete the specified functions under limited conditions. After the available nodes fail, the number of effective links currently available in the network (in which the number of unicast multipath effective links ≤ 1) is consistent with the ratio of the number of links between all nodes in the network. Suppose a node in the network fails. The remaining node set is G_p. Where n represents the total number of network nodes, l_{ij} represents the number of nodes corresponding to the effective link in the current network. If there is an effective link between nodes i and j, then $l_{ij} = 1$, otherwise l_{ij}=0. The network reliability is shown in Formula5.1.2.

$$m_p = \frac{\sum_{i \in G_p} \sum_{j>i} l_{ij}}{n(n-1)}$$

(2) Average routing hops

In ad hoc networks, the data transmission from the source node to the destination node often needs to be forwarded by the intermediate node. The more nodes an effective path passes through in the network, the greater the possibility of the path being damaged. Set the effective route in the network as $L_{|S \sim D|_i}$, where S represents the source node, D represents the destination node. $S \sim D$ represents the node sequence passed by the route, and the length of the node sequence is expressed in $|S \sim D|_i$. i refers to the sequence number of effective routes in the network, which increases with the number of effective routes. The average number of routing hops is shown in formula 5.1.2.

$$H_p = \frac{\sum |S \sim D|_i}{i}$$

2) Evaluation results

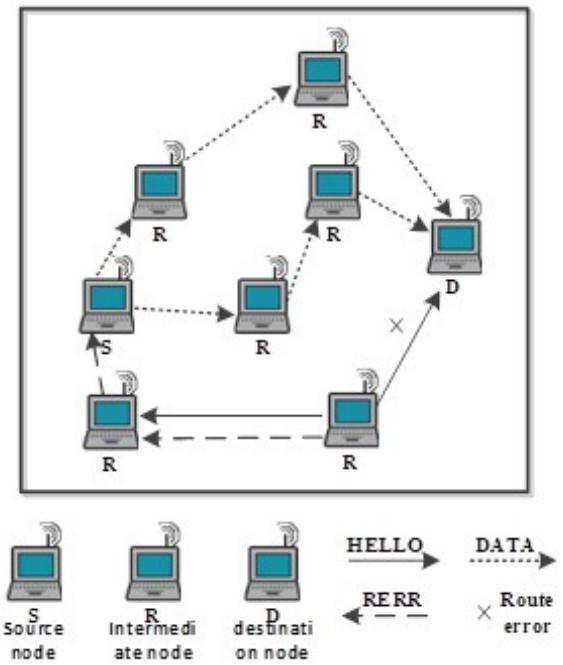


Figure 3: MD_ AODV route maintenance process diagram

(1) Random moving scene

As shown in Figure4, it is the network performance curve when nodes move randomly in the scenario of node damage recoverable. It can be seen from the figure that the throughput and reliability indexes of MD_AODV are better than those of AODV and AOMDV routing protocols. The average number of routing hops is close to that of AOMDV. But in the end, the average number of routing hops of MD_AODV drops to the optimal state.

(2) Formation keeping moving scene

As shown in Figure5, it is the network performance curve when the node formation remains moving in the scenario of node damage recoverable. From the results of throughput and average routing hops, it can be seen that the routing performance of MD_AODV is better than AODV. However, in terms of reliability index, AOMDV index is slightly better than MD_AODV . It can be seen that when the network is damaged, the reliability index of AOMDV shows a downward trend, while MD_AODV shows a steady increasing trend.

(3) Aggregate mobile scenes

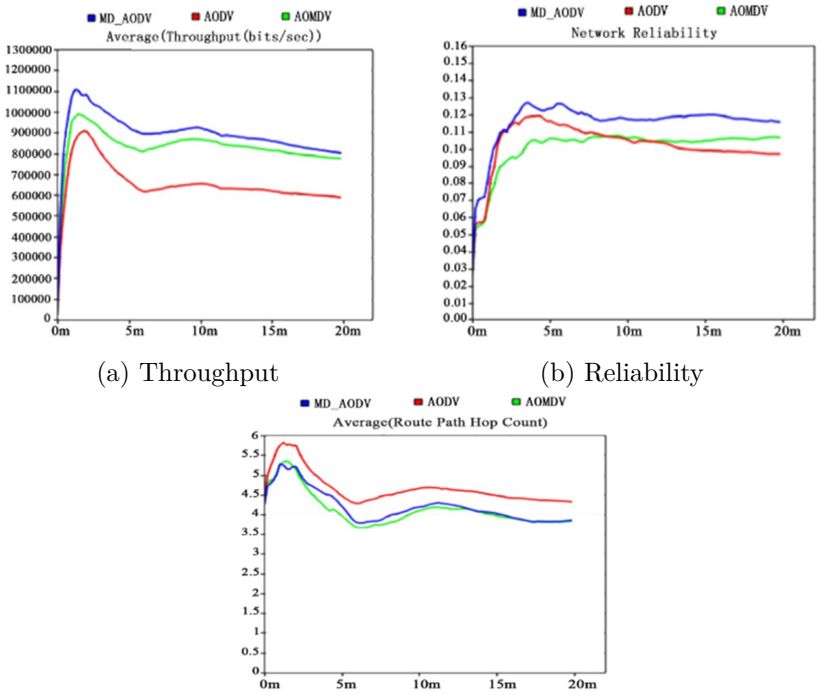
Figure6 is the network performance curve of node aggregation and movement in the scenario of node damage recoverable. It can be seen that the reliability and average routing hops of MD_AODV are better than AODV and AOMDV routing protocols. Although the network throughput of MD_AODV is better than AODV routing protocol, it is not significantly better than AOMDV routing protocol.

To sum up, when the network is slightly damaged, combined with the overall evaluation of network performance indicators in three mobile scenarios. It can be concluded that the survivability of MD_AODV is better than that of AODV and AOMDV routing protocols. However, the single network performance of MD_AODV and AOMDV in different mobile scenarios needs to be further explored.

5.2 Invulnerability under the scenario of irrecoverable network with node damage

5.2.1 Network scenario settings

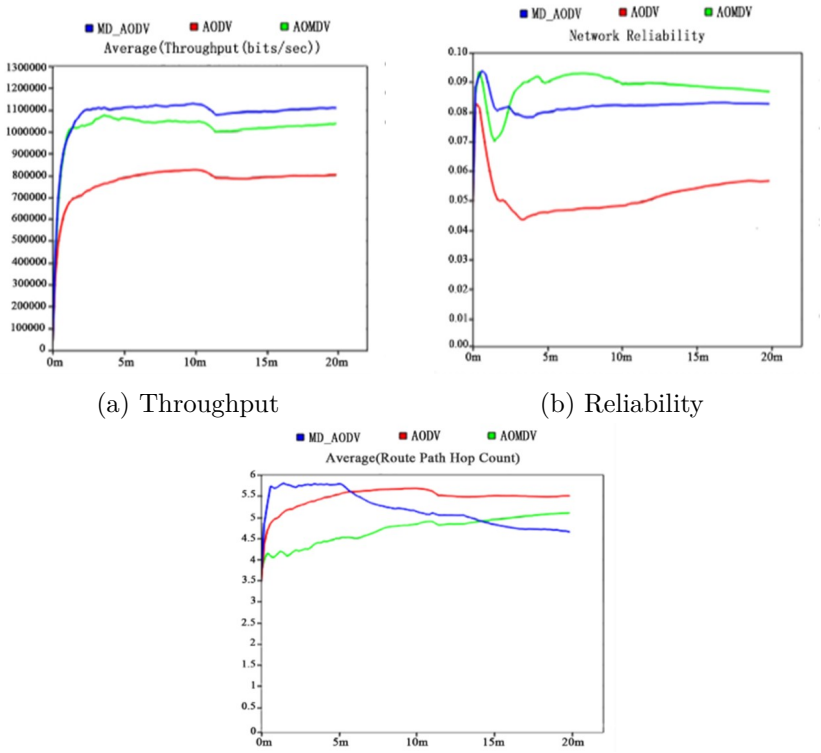
The network scenario parameters of the mobile multi-agent node damage recoverable scenario are shown in Table4. The moving speed and moving path of nodes correspond to the moving speed and moving path in different cooperative mobile task models.



(a) Throughput (b) Reliability

(c) Average routing hops

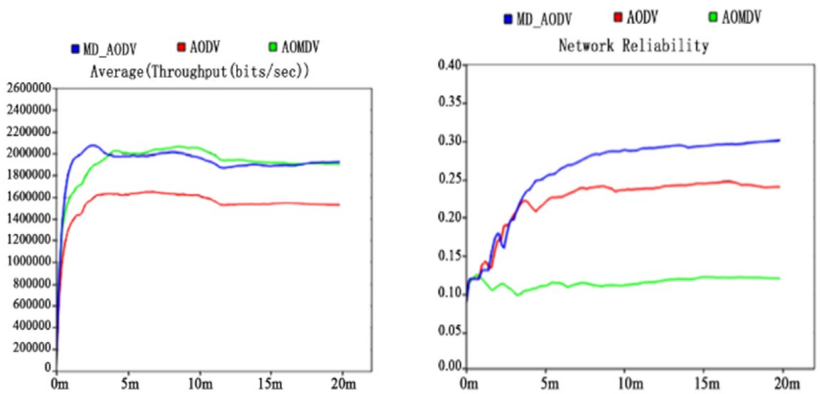
Figure 4: Invulnerability in random moving scenario



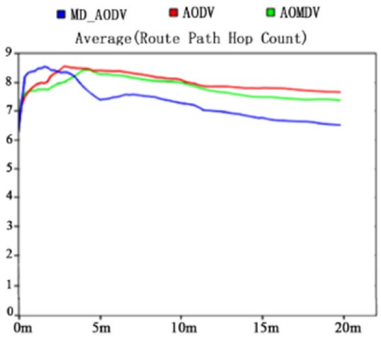
(a) Throughput (b) Reliability

(c) Average routing hops

Figure 5: Invulnerability performance in formation keeping moving scene



(a) Throughput (b) Reliability



(c) Average routing hops

Figure 6: Invulnerability in aggregated mobile scenarios

Table 4: simulation scenario parameters

parameter	Set value
Scene range	50km×50km
Number of nodes	50
Number of failed nodes	10
Simulation time	20 min
Network damage time	After 10 minutes of network operation
Network damage model	Node damage irrecoverable model
Mobile scene	Random, formation maintenance, aggregation
Maximum communication distance of node	3000 m
Data transmission rate	1 Mbps

5.2.2 Evaluation of Invulnerability

In the case of unrecoverable network with node damage, the Invulnerability of the routing protocol is evaluated through the indicators of network throughput, reliability and average routing hops. The evaluation results are as follows:

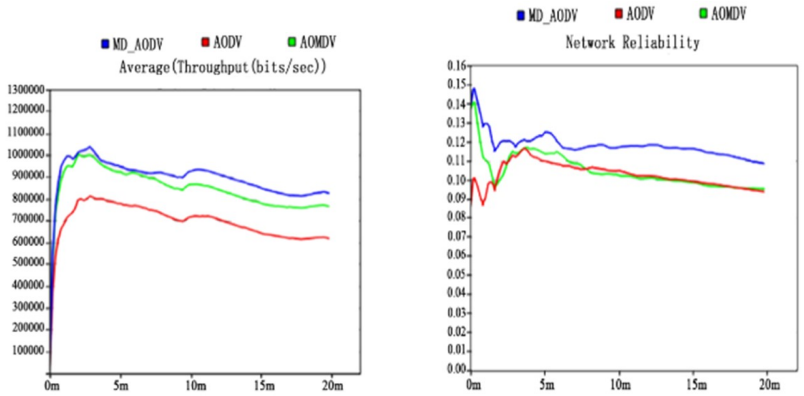
(1) Random moving scene

Figure 7 is the network performance curve when nodes move randomly in the scenario of irrecoverable node damage. In terms of reliability, MD_AODV routing is better than AODV and AOMDV routing. The average number of routing hops of MD_AODV decreases continuously after the network is damaged. The throughput of MD_AODV is similar to that of AOMDV.

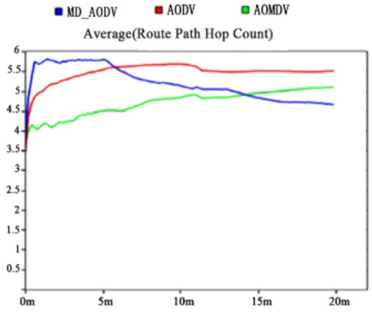
(2) Formation keeping moving scene

Figure8 is the network performance curve when the node formation keeps moving in the scenario of unrecoverable node damage. In terms of reliability and average routing hops, the performance of MD_AODV is better than AODV and AOMDV routing protocols before and after network damage. In terms of throughput, the performance of MD_AODV is close to that of AOMDV.

(3) Aggregate mobile scenes Figure9 is the network performance curve of node aggregation and

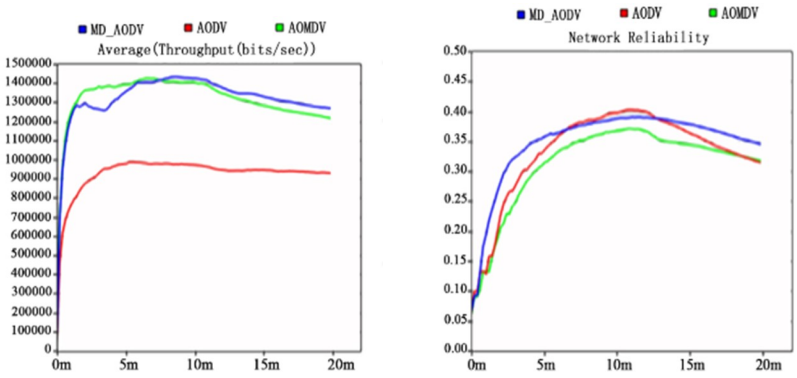


(a) Throughput (b) Reliability

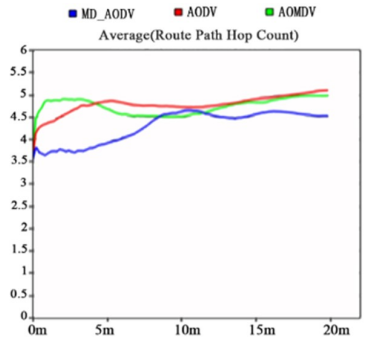


(c) Average routing hops

Figure 7: Network performance in random mobile scenario

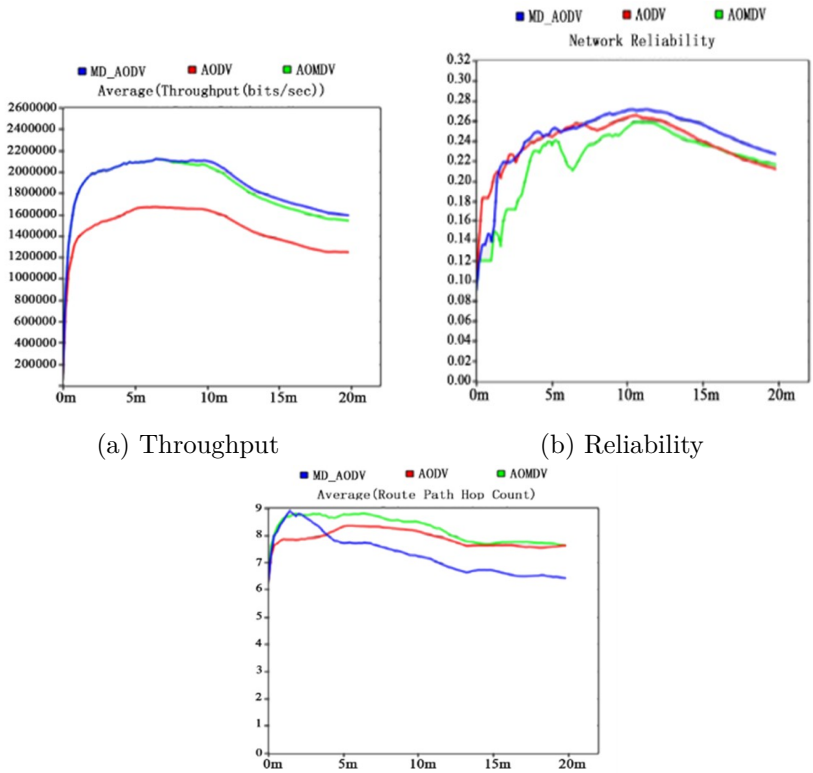


(a) Throughput (b) Reliability



(c) Average routing hops

Figure 8: Network performance in formation keeping mobile scenario



(a) Throughput (b) Reliability

(c) Average routing hops

Figure 9: Network performance in aggregated mobile scenario

movement in the scenario of irrecoverable node damage. It can be seen from the throughput that the performance of MD_AODV and AOMDV is almost the same before the network is damaged. When the network is damaged, the performance of MD_AODV is better than that of AOMDV routing. It can be seen from the reliability that the routing performance of MD_AODV and AODV is similar before the network is damaged. After the network is damaged, the decline of AODV reliability is greater than that of MD_AODV and AOMDV. The average number of routing hops of MD_AODV routing decreases as time goes by.

To sum up, when the network is severely damaged, it can be seen that the network damage reduces the network throughput and reliability corresponding to the three routing protocols. MD_AODV and AOMDV have similar performance in network throughput. After the network is damaged, the average number of routing hops of MD_AODV routing is less, and the reliability is better than that of AODV and AOMDV routing protocols. The overall evaluation shows that the Invulnerability of MD_AODV is better than AOMDV and AODV routing protocols. Because both MD_AODV and AOMDV have the characteristics of multipath backup, their network throughput is high. However, in terms of the number of currently available effective links of the network after serious network damage, MD_AODV routing is dominant. And the average number of routing hops of MD_AODV after network damage is less, which will also help it to continue to deal with more serious network damage.

6 Conclusion

In order to simulate the damage of mobile multi-agent system in real environment, this paper designs two kinds of network models of damage degree, and simulates and analyzes the invulnerability performance of the proposed improved multi-path routing protocol. The results show that the improved multipath routing protocol has different Invulnerability under different network damage scenarios. When the network is slightly damaged, the routing performance of MD_AODV is close to that of AOMDV. When the network is severely impairment, the throughput performance of the two systems is close. However, from the perspective of network stability and the potential to cope with

the continuous deterioration of network damage, MD_AODV routing has better invulnerability.

Funding

All authors have read and agreed to the published version of the manuscript. This work was supported by R&D Program of Beijing Municipal Education Commission (KM202011232023), and supported by Instructional Reform Item of 2018GJJG423.

Author contributions

The authors contributed equally to this work.

Conflict of interest

The authors declare no conflict of interest.

References

[1] Dorri A, Kanhere SS, Jurdak R. Multi-Agent Systems: A Survey. *IEEE Access* 2018;6:28573–93. https://doi.org/10.1109/ACCESS.2018.2831228.

[2] Wang J, Liu C, Li W, Li K. Heterogeneous multi-mode access in smart grid using BeiDou communication. *Microprocess Microsyst* 2016;47:244–9. https://doi.org/10.1016/j.micpro.2016.02.017.

[3] Moudni, Houda, et al. Performance analysis of AODV routing protocol in MANET under the influence of routing attacks. *2016 International Conference on Electrical and Information Technologies (ICEIT).* IEEE, 2016.

[4] Fu X, Fortino G, Pace P, Aloi G, Li W. Environment-fusion multipath routing protocol for wireless sensor networks. *Inf Fusion* 2020;53:4–19. https://doi.org/10.1016/j.inffus.2019.06.001.

[5] Zhang, Wanbin, et al. An improved AODV routing protocol based on social relationship mining for VANET. *Proceedings of the 4th International Conference on Communication and Information Processing.* 2018.

[6] Alebeed, Hani. *A Spectrum Decision Scheme for Cognitive Radio Ad Hoc Networks.* MS thesis. Eastern Mediterranean University (EMU)-Doğu Akdeniz Üniversitesi (DAÜ), 2016.

[7] Lee, S. J., and M. Gerla. AODV-BR: Backup routing in Ad Hoc networks, 2000. *Proceedings of IEEE WCNC.*

[8] Zhang F, Yang G. A Stable Backup Routing Protocol for Wireless Ad Hoc Networks. *Sensors 2020*;20:6743. https://doi.org/10.3390/s20236743.

[9] Matre, Versha, and Reena Karandikar. Multipath routing protocol for mobile adhoc networks. *2016 Symposium on Colossal Data Analysis and Networking (CDAN).* IEEE, 2016.

[10] Yang, Wenjing, et al. Improving Route Stability in Mobile Ad hoc Networks Based on Link Lifetime. *J. Commun.* 6.3 (2011): 205-214.

[11] Yuanyuan, An, et al. Network Equilibrium Optimization of AODV Protocol in Ad Hoc Network. *2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control.* IEEE, 2014.

[12] Qadori, Huthiafa Q., et al. Multi-mobile agent itinerary planning algorithms for data gathering in wireless sensor networks: A review paper. *International Journal of Distributed Sensor Networks* 13.1 (2017): 1550147716684841.

[13] Liu, Qiang, et al. A Multi-UAVs communication network simulation platform using OPNET modeler. *ICC 2020-2020 IEEE International Conference on Communications (ICC).* IEEE, 2020.

[14] Chen, Bo, Harry H. Cheng, and Joe Palen. Integrating mobile agent technology with multi-agent systems for distributed traffic detection and management systems. *Transportation Research Part C: Emerging Technologies* 17.1 (2009): 1-10.

[15] Mehta, Rishabh, et al. Studying the Open System Interconnection Model and Proposing the Concept of Layer Zero [J]. *Indian Journal of Science & Technology* 9.21 (2016).

[16] Hu, Chun Chao, et al. Modeling and Simulation for Quantitative Assessment of Process Level Networks in Substation Based on OPNET. *Advanced Materials Research.* Vol. 805. Trans Tech Publications Ltd, 2013.

[17] Venkatasubramanian, S., A. Suhasini, and C. Vennila. An energy efficient clustering algorithm in mobile Adhoc network using ticket Id based clustering manager. *International Journal of Computer Science & Network Security* 21.7 (2021): 341-349.

[18] Zhang, Zeyu, et al. A survey on fault diagnosis in wireless sensor networks. *IEEE Access* 6 (2018): 11349-11364.

[19] Zhang, Zhenyu, et al. Analyzing the coevolution of mobile application diffusion and social network: a multi-agent model. *Entropy* 23.5 (2021): 521.

[20] Abu Zant, Mahmoud, and Adwan Yasin. Avoiding and isolating flooding attack by enhancing AODV MANET protocol (AIF_AODV). *Security and Communication Networks* 2019 (2019).

[21] Basak, Surajit, and Tamaghna Acharya. Route selection for interference minimization to primary users in cognitive radio ad hoc networks: A cross layer approach. *Physical Communication* 19 (2016): 118-132.

[22] Li, Peng, Lu Guo, and Fang Wang. A multipath routing protocol with load balancing and energy constraining based on AOMDV in ad hoc network. *Mobile Networks and Applications* (2019): 1-10.

[23] Abdelgader, Abdeldime Mohamed Salih, Lenan Wu, and Mohammed Mohsen Mohammed Nasr. A simplified mobile ad hoc network structure for helicopter communication. *International Journal of Aerospace Engineering* 2016 (2016).

[24] Yang, Songtao, and Zongli Zhang. "Entropy weight method for evaluation of invulnerability in instant messaging network. *2009 Fourth International Conference on Internet Computing for Science and Engineering.* IEEE, 2009.

Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:
Wang, Q.-H; Lan, S.-f.; Zhang, D.; Wang, Y.-Q.; Zhu, Q.; Chen, W.-b. (2023). Invulnerability Improvement of Multipath Protocols in Different Scenarios, *International Journal of Computers Communications & Control*, 18(3), 5005, 2023.
https://doi.org/10.15837/ijccc.2023.3.5005