J Inf Process Syst, Vol.16, No.5, pp.1113~1128, October 2020
https://doi.org/10.3745/JIPS.03.0149

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Intelligent On-demand Routing Protocol for Ad Hoc Network

Yongfei Ye*, Xinghua Sun*,**, Minghe Liu***, Jing Mi*, Ting Yan*, and Lihua Ding*

Abstract

Ad hoc networks play an important role in mobile communications, and the performance of nodes has a significant impact on the choice of communication links. To ensure efficient and secure data forwarding and delivery, an intelligent routing protocol (IAODV) based on learning method is constructed. Five attributes of node energy, rate, credit value, computing power and transmission distance are taken as the basis of segmentation. By learning the selected samples and calculating the information gain of each attribute, the decision tree of routing node is constructed, and the rules of routing node selection are determined. IAODV algorithm realizes the adaptive evaluation and classification of network nodes, so as to determine the optimal transmission path from the source node to the destination node. The simulation results verify the feasibility, effectiveness and security of IAODV.

Keywords

Ad Hoc Network, Adaptive, Decision Tree, Intelligent Routing Protocol

1. Introduction

The information society expects the adaptability of the network to have higher performance. Ad Hoc mobile network has the features of simple equipment, no infrastructure requirements, self-organization, strong adaptability to the environment, and can be flexible and excellent in the difficult environment of communication tasks [1-3]. However, due to the weak performance of the equipment, the use of wireless channel communication and frequent node movement, the possibility of data intercepted by illegal users is very high, which makes the routing security of the network face a major threat [4-6].

There are many routing protocols designed for the characteristics of Ad Hoc networks at home and abroad. Routing protocols such as ad-hoc on-demand distance vector (AODV) [7], destination-sequenced distance vector (DSDV) [8] and dynamic source routing (DSR) [9,10] are widely used. The common feature of these routing protocols is to establish communication links between the two terminals as quickly as possible to adapt to the mobility of ad hoc networks. When establishing routing, it is assumed that the trust between nodes is strong enough and that nodes can always cooperate to complete data forwarding. In these routing protocols, security issues are seldom considered, which provides an

Manuscript received May 9, 2019; first revision November 4, 2019; accepted February 22, 2020.

Corresponding Author: Xinghua Sun (1030704295@qq.com)
* School of Information Science and Engineering, Hebei North University, Zhangjiakou, China (yeyongfei005@126.com, mjdyouxiang@163.com, yanting_pku@163.com, 876065611@qq.com)
** College of Environmental and Geographical Sciences, Shanghai Normal University, Shanghai, China (1030704295@qq.com)
*** College of Economics and Management, Hebei North University, Zhangjiakou, China (461053520@qq.com)

opportunity for intruders. Many targeted attacks have appeared, such as flooding attacks, witch attacks, wormhole attacks, and so on. So far, great progress has been made in improving the routing protocols of ad hoc networks at home and abroad. At the same time, some research results on secure routing have emerged. For example, Xiao and Shan [11] have analyzed and summarized the security problems of ad hoc networks, and also analyzed media access control protocol (MAC) and the quality of service (QoS). Some researchers have constructed safe routing protocols such as secure AODV (SAODV) and secure routing protocol (SRP) [12]. Snazgiri et al. [13] once put forward using IPSec to avoid the routing safety risk in mobile ad hoc networks. However, the feasibility is very poor for the energy- and storage-constrained ad hoc networks due to the need to maintain more databases and carry out a great deal of calculation in the mechanism.

Ad hoc network is strongly autonomous; so traditional network security technology cannot be applied without modification. Previous research results have some security weakness. Therefore, it is necessary to design a targeted security mechanism to make sure the network is in a normal state.

The routing protocols need to meet the expectations of stability, robustness, optimality, simplicity, low overhead and strong adaptability in ad hoc networks. Each node in ad hoc network has data forwarding function, so the routing algorithm needs to be integrated into the distributed algorithm and maintained by all legal nodes. The transmission bandwidth of ad hoc network is limited, so the bandwidth occupied by the designed routing protocol should be within the controllable range. The characteristics of the changeable topology of ad hoc networks also require higher computing speed. For the sake of avoiding the exhaustion of node resources, the computational complexity of routing algorithm should also be limited. In addition, necessary security measures should be considered in the design of routing protocols to prevent attacks.

Therefore, it is necessary to make a comprehensive analysis of the structure of ad hoc network, take every factor into consideration, and construct a more secure and reasonable routing protocol.

2. Typical Routing Protocols for Ad Hoc Networks

Academic research on routing protocol algorithm in ad hoc networks began in the early 1980s. Many typical routing algorithms have been designed through unremitting efforts, such as table driven routing protocol which can lower transmission delay, on-demand routing protocol which can be established immediately when communication is needed, single path routing protocol and multipath routing protocol that can choose the best channel from the source to the destination [14-19].

2.1 Table Driven Routing Protocol

Destination-sequenced distance vector (DSDV, target sequence distance vector routing protocol) belonging to table-driven routing protocol, is also called proactive routing protocol. The shortest path is preferred in communication. Table-driven routing protocol has the characteristics of small delay, but high communication overhead. It can update adaptively and dynamically according to the network structure. In such routing protocols, every node should maintain a table that stores the path information linked to other nodes on its own. When changes occur in the network, such as new nodes joining, old nodes exiting or the location of nodes changing, the network topology will change. At this time, the affected network nodes need to update their routing protocol tables in time and transmit relevant message to involved nodes to maintain consistency, real-time and safety. DSDV routing protocol is suitable for bidirectional link communication, and maintains local routing data table in real time. It solves the problem of high frequency infinite computation, and avoids the generation of loops in data transmission in network.

DSDV routing protocol is suitable for small and medium-sized ad hoc networks. It can show its advantages when the network topology is stable and the nodes joining or leaving the network is not frequent. DSDV routing protocol can quickly generate routing for nodes, ensure delivering real-time messages, and meet the time-limited needs of the network. Based on the characteristics of DSDV routing protocol itself, this routing algorithm is not suitable for networks with frequent topological changes. Otherwise, it will cause problems such as high computing cost, high processing overhead and large bandwidth occupancy, which will seriously affect the network, thus reducing the availability of the network.

2.2 On-demand Routing Protocol

Two typical on-demand routing protocols are as follows.

2.2.1 DSR routing protocol

The basic principle of DSR is the establishment of communication links between source and destination nodes caused by data message sending requirements. It mainly consists of two parts: routing discovery and routing maintenance. In the network, each node maintains a local routing information table. Each entry in the table writes down the routing data to the reachable end in the network, including the IP address of the source, via nodes and the destination.

The source will first check whether there is a reachable path to the destination in its local routing table before sending data packets in the network, and if so, then attaches it to the head of the datagram. According to the established routing, the packets are forwarded to the destination with the help of related intermediate nodes. In the process of forwarding data, the intermediate nodes can establish routing information cache and route to the destination node for future communication with the destination node.

The working mechanism of DSR protocol can avoid the generation of communication loops in the network. Because the routing information contains the full routing path to the destination, the transit node does not need to take time to maintain the real-time changes in the network topology. Routing discovery plays an important role in DSR. If node S needs to transport packet to node D, and there’s no well-established routing path between two nodes, it needs to use routing discovery mechanism to establish the path.

DSR protocol has no independent routing maintenance operation. The protocol allows multiple data transmission paths in the network, and is suitable for asymmetric channel network environment. Because DSR protocol broadcasts messages by flooding mechanism when routing is established, conflicts will occur in the process of data transmission, and the routing information cached by each node may expire due to the lack of active maintenance process. In the process of sending datagram, the head of the datagram stores the corresponding routing information, which will occupy more channels. Based on the above characteristics, DSR protocol is more suitable for small and medium-sized networks.

2.2.2 AODV routing protocol

AODV is a common reactive routing protocol in ad hoc networks supplied by Perkins and Royer [7], which is proposed on the basis of DSDV protocol and the improvement of on-demand routing mechanism in DSR. The principle of AODV routing protocol is to establish routing between nodes on demand when datagram needs to be transmitted in the network. When communication is completed, the established routing is no longer maintained and the entries of control information are reduced, thus improving the efficiency of operation. This protocol effectively utilizes network resources, establishes routing on demand, and adapts to the characteristics of ad hoc network.

AODV routing protocol consists of routing discovery and routing maintenance. When a network node needs to transport data but has no right routing, the routing discovery is necessary.

To avoid data congestion in communication links, the source node needs to wait for feedback after sending RREQ messages to its neighbors. If the waiting time exceeds the preset time, it will retransmit the RREQ message.

The routing maintenance is mainly used to maintain the established routing in the network. AODV routing protocol monitors active routing by periodically sending Hello message frames in the network. Once a node finds that a link is not working, it should broadcast RERR packets to the relevant nodes on the affected link to inform them of the update or deletion of the routing information. The routing error frame RERR is sent in three ways. When RERR is forwarded, all network nodes associated with this invalid routing need to delete the corresponding routing entries in their local routing information table.

The operation of reconstructing routing occurs when the two following situations occur:

(1) When the sender accepts the RERR frame about a route, it can re-initiate the request to establish the route if there is still a need to transport message to the destination.

(2) When the intermediate node on a certain route forwards the packets to the destination node, the destination node is not reachable due to the problem of computing the routing time exceeding the preset time. It is necessary to store the received packets temporarily, and then re-establish the routing with the destination node by sending the RREQ message.

AODV routing protocol asks every node to maintain its own serial number in the network which is used to determine whether the routing information is expired.

AODV routing protocol adapts to the dynamic change of network structure, but the routing delay when establishing routing is large, the routing has a certain lifetime, and will be abandoned after the timeout. AODV routing protocol combines DSDV with DSR, and uses sequence number labeling to prevent routing outage or loops same as the former, while the routing discovery mechanism is formed by improving the latter.

3. Security Threats and Attacks of Routing Protocols

The routing between source node and destination node based on routing algorithm depends on trust between nodes in the network and cooperates with each other. If a node fails to cooperate with routing message forwarding with the aim of saving its power energy or the network nodes are captured due to the weak security of wireless channels, it will lead to attacks on routing protocols in the network, which will make the network face security threats, and in serious cases will lead to network communication system paralysis.

Each node has the functions of both host and router, and is responsible for setting up routing and transmitting data in ad hoc network. When the network is intruded, malicious nodes will attack the routing algorithm and destroy the establishment of routing. Common routing attacks include forgery, tampering, selfish behavior, routing table overflow and black hole attack. Here are some typical attack types.

3.1 Wormhole Attack

Wormhole attack, also known as tunnel attack, implements routing attacks by establishing an illegal channel outside the normal communication channel. There is a high-quality communication tunnel between two attackers in the network. When the attacker at one end of the tunnel eavesdrops or receives the data packets sent from the neighboring nodes, he sends them directly to the attacker at the other end by using a secret channel and forwards the data to the destination end, which makes the destination node mistakenly believe that the data packets can be forwarded through just one hop in the middle of the channel. This will cause the target node to abandon the correct communication channel. Because the nodes choose the shortest path preferentially when communicating, and thus, the attack takes advantage of this weakness to launch wormhole attack.

Wormhole attacks can cause confusion in the routing table information of the attacker's legitimate neighbors, invalidate the routing discovery mechanism, and damage the integrity and confidentiality of data. If not monitored and controlled, there will be serious consequences.

3.2 Rushing Attack

The attacker blocks other normal routing from sending requests by sending routing request messages to the network and then quickly replying to them, so as to suppress the normal routing requests receiving.

3.3 Sybil Attack

Sybil attack was originally proposed by Douceur [20]. Its main working principle is that a malicious node forges multiple identities to communicate with the outside world so as to control most nodes in the network and destroy the redundancy mechanism in the network.

The common means of Sybil attack: forgery of identity, identity theft, direct communication, and indirect communication.

In addition to the several attacks described above, there are many attacks against routing protocols in ad hoc wireless networks, so routing security is also a key issue to consider when constructing and maintaining networks.

4. Intelligent On-demand Routing Protocol for Ad Hoc Network

In ad hoc networks, every network node has dual roles. When routing messages and datagram are being transmitted, all nodes need to work with others in the network. A reachable path is the basic requirements of secure and reliable data transmission, and the security of routing protocols is very important to the availability of networks. Therefore, after identifying the nodes requesting to join the network, the effective routing between nodes is the fundamental guarantee for the safe transmitting of messages such as datagram in the network.

Adapting to the self-organizing characteristics of ad hoc wireless networks, AODV protocol is improved. A more secure and adaptive intelligent on-demand routing algorithm is designed, which actively, quickly and optimally establishes the path between nodes, and realizes the purpose of resisting illegal attacks against such routing protocols. Several technical points mainly guarantee security in this routing algorithm: key information hiding; the use of mathematically difficult functions; authorized users to obtain routing information. This routing protocol uses ID3 algorithm to test five attributes such as energy, computing power, speed, transmission distance, and data forwarding ability, so as to determine the best routing from the source to the destination. The private key of system is used to authenticate the network nodes identity in a distributed way, which gives a higher level of security.

4.1 Correlation Algorithm

4.1.1 Distributed authorization CA

In traditional networks, when a node joins the network, the authentication of identity legitimacy is completed by a specific authentication center, and the management authority is centralized. Because of the poor security of ad hoc network, if the centralized CA (certification authoring) is damaged, the whole network will fall into disorder, may be even on the verge of collapse. This scheme uses distributed CA mechanism to verify the validity of node identity.

In 1979, Shamir [21] first proposed the concept of secret sharing scheme. The implementation strategy of the scheme is to divide a secret into sub-secrets called secret shares and distribute. The secret shares to a participant. It takes the combination of any t secret shares to cooperate to recover the secret S, and the secret cannot be recovered with less than t secret shares. The value t is the threshold to acquiring the secret S. It has certain requirements for its value, which is called threshold.

Zhou and Hass [22] put the idea of secret sharing into the authenticating the identity of nodes the first time in 1999. In this management strategy, every node is regarded as a holder of the sub-secret to decentralize the authentication privileges and realize the distributed CA authentication of the identity legitimacy of the network nodes. The distributed CA signature authentication of the node certificate will not be realized until t nodes uses their own secret share to sign the certificate of the requesting node effectively and then synthesize the certificate through the algorithm when one node asks for authentication service to attend the network. Thus, the authentication of the identity of the node is completed.

4.1.2 Decision tree

In machine learning, decision tree is a prediction model with tree structure. Decision tree is mainly used for classification and regression, which can be used for supervisory learning. The main function of decision tree is to classify the samples by generating a classifier. When new objects appear, the classifier can classify them correctly. The advantage of decision tree is that it can evaluate the risk and judge the feasibility according to the occurrence probability of each attribute of the object.

Decision tree presents the attributes, attribute values and categories of nodes in a tree structure. There are three main symbols used in decision tree:

Rectangular box - decision node, if the decision is made up of multiple levels, there will be many intermediate decision nodes, but the root node is the final decision scheme. Each decision node is the best result of one decision.

Circle - state node represents the expected value of each scheme. By comparing the economic effects of each state node, the best scheme can be selected according to the predetermined decision criteria.

Line - probability branch, the number of branches from the state node indicates the quantity of possible states, while the number labeled on the branches is the probability of corresponding states.

Triangle - Result Node, the profit and loss value of each scheme in various situations is marked on the right side of Result Node.

The decision tree can intuitively reflect the characteristics of data, which is intelligent and easy to operate. So it is suitable for the construction of data transmission path between nodes in ad hoc network. This algorithm will use the idea of decision tree to realize the on-demand routing protocol reasonably and quickly.

4.1.3 ID3 algorithm

ID3 algorithm is a classification and prediction algorithm for decision tree supplied by Quinlan [23]. Based on information theory, through the calculation of information entropy and information gain, each time the attributes with high information gain are selected to divide, and the process is repeated until a decision tree can be generated which can classify training samples, so as to acquire the aim of data induction and classification.

The key of ID3 algorithm is to select the attributes with the largest information gain after splitting according to the attributes of information gain measurement. Two important concepts of information entropy and information gain are involved in the algorithm.

The basic idea of ID3 algorithm is as follows:

(1) Initialization of attribute sets and data sets.
(2) Calculate the information entropy S of data set and all attributes, and select the attributes with the greatest information gain as the current decision node.
(3) Update the data set and attribute set (delete the attributes used in the previous step, and divide the data set of different branches according to the attribute value).
(4) Repeat step (2) for each subset in turn.
(5) If the subset contains only a single attribute, the branch is a leaf node, marked according to its attribute value.
(6) Complete the partition of all attribute sets.

After comprehensive comparison, it is found that small decision trees are superior to large decision trees.

4.2 Intelligent Routing Decision Mechanism

The communication path between source node S and destination node D is established on demand. As the remarkable characteristics of ad hoc wireless network is that nodes move frequently and the topology is unstable, it does not cost much to maintain the routing to each node in the node. This intelligent routing decision mechanism considers the communication performance of each node before the node communicates, and chooses the best path according to the principle of decision tree, which greatly improves the effectiveness, reliability and security of communication.

4.2.1 Training samples for decision model

In this routing algorithm, five attributes of node energy, transmission distance, rate, credit value and computing power are selected as reference values. The training samples are obtained through continuous testing of five attribute values as shown in Table 1.

The algorithm refers to five attributes of the network node, each of which has a certain range of values, and sets a threshold, as shown in Table 2.

In this paper, the ad hoc network is regarded as a connected graph $G = (S, C)$, where S is the set of network nodes and C is the set of communication links between network nodes within the communication range. Each network node is marked as n_i, $n_i \in S$, i=1,2,3,…N, the attribute set of the node is marked as $A = \{a_i^1,\ a_i^2,\ a_i^3,\ a_i^4,\ a_i^5\}$.

Whether a node in the network is selected as a routing node is determined by its attributes. Nodes that are selected as routing are positive-examples, and those that are not selected as routing are counter-examples. In order to measure the attribute purity of the routing node determined as forwarding data, entropy is introduced here:

$$H(A) = -\sum_{i=1}^{2} p_i log_2 p_i \tag{1}$$

In the formula, p_i is the probability that attribute a_i^j produces positive examples, and $1 - p_i$ is the probability that attribute a_i^j produces negative examples. If the entropy value is 0, then the sampling data is completely pure, and the attribute of the node can be used as the basis of division, without further segmentation; if the entropy value is not 0, it means that the sampling data is not pure and needs further segmentation.

Table 1. Samples of relationship between node attributes and forwarding capability

Serial number	Energy P (electricity, %)	Transmission distance D (m)	Rate R (kbps)	Credit value T (0–1)	Computing power C (MHz)	Is it a routing node?
1	90	50	115	0.90	624	Y
2	80	30	76.8	0.70	192	N
3	75	40	2,000	0.60	2,400	N
4	70	45	4,000	0.80	1,200	Y
5	40	20	100	0.60	1,500	N
6	60	50	1,000	0.80	190	N
7	40	40	153	0.90	192	N
8	80	10	110	0.85	220	N
9	90	40	4,000	0.85	2,400	Y
10	20	20	100	0.90	1,500	N
11	60	40	1,000	0.90	900	Y
12	75	30	153	0.70	634	Y
13	20	50	8,000	0.40	624	N
14	80	40	10,000	0.85	1,500	Y
15	80	50	20,000	0.50	1,200	N

Table 2. Description of node attributes

Attribute	Range of values	Threshold
Energy (electricity, %)	1–100	50
Transmission distance (m)	0–300	30
Rate (kbps)	0–60,000	100
Credit value	0–1	0.7
Computing power (MHz)	150–3,000	200

In order to determine the node attribute that should be first partitioned, the maximum information gain is introduced. The information gain can represent the correlation between the attributes of nodes. The range of values is [0,1]. The calculation is based on formula (2):

$$Gain(A, a^j) = H(A) - \sum_{v \in Values(a^j)} \frac{|A_v|}{|A|} H(A_v) \quad (2)$$

In the formula, V is a subset of the values of node attributes a^j, $|A_v|$ is the length of the subset, $|A|$ is the sample length, and $H(A_v)$ is the purity of the values of the attributes of node n_i.

Using formulas (1) and (2) synthetically, according to ID3 algorithm, the information gains of each node are calculated, and the branches with large information gains are selected to cycle back and forth until the end of the leaf. An intelligent decision tree is constructed to determine whether a network node has routing capability when creating a communication link, as shown in Fig. 1.

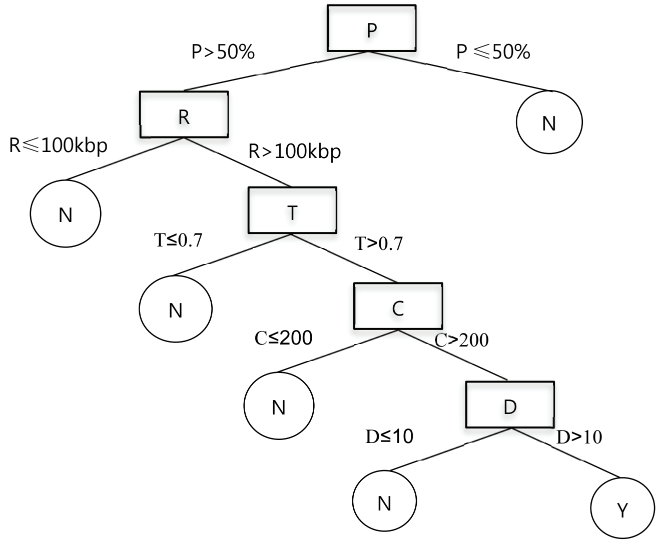

Fig. 1. Routing node decision tree based on attributes.

4.2.2 Implementation of intelligent routing decision mechanism

When the identity of the node joining the network is authenticated, the topology construction of the Ad Hoc network is completed. Every node in the network must store the attribute value tables of all its one-hop neighbors, and the data in the tables will change dynamically as the network does of the network.

The intelligent routing decision protocol consists of two parts: Route Discovery and Route Maintenance, when the source node S is transmitting message to the destination node D.

4.2.2.1 Route discovery

The main task of routing discovery is to establish the routing for transmitting data packets in the channel. It also includes routing request sending (RREQ), routing request forwarding, routing reply sending (RREP) and routing reply forwarding operations. It mainly has two stages: route request and route response.

For the sake of improving the robustness of the network and resist the damage of irresistible anomalies to the network, two one-hop neighbor nodes are selected at a time.

The routing request process is as follows:

(1) The source node S sends a RREQ packet that contains important information such as the IP addresses of the source and the destination. If node D is a one-hop neighbor of node S, then no decision-making is needed. The routing request message is sent directly to node D and the routing request ends. If two nodes are not adjacent, the next operation is performed.
(2) According to the locally stored node attribute table, the source node S calculates the information gain and selects the two nodes with the largest value as one-hop forwarding node. Assuming that node C and node E have the largest information gain, node S sends routing request messages to node C and node E.
(3) After receiving RREQ, node C and node E search whether there is information about destination node D in the locally stored node attribute table. If so, they send the routing request message directly to D. If not, they need to calculate the information gain of each neighboring node again, and then only select the node with the maximum information gain as forwarding nodes for the next hop. Assuming that the neighbor node with the maximum information gain of node C is F, and the neighbor node with the maximum information gain of node E is H.
(4) Nodes F and H repeat the above operation and select the nodes K and I with the largest information gain respectively.
(5) A jump neighbor of node F and H is found to be the destination node D by searching. If the parameters of node D can meet the basic communication requirements, the RREQ packet will be smoothly transmit to the target node D.

During the above operation, each intermediate node forwarding RREQ message needs to maintain and store the reverse route to the source node.

In the process of routing response, a time threshold RREQ_RETRIES of routing response needs to be preset, and the timeout will be regarded as no response. Therefore, the next hop node needs to be re-selected by the upper node.

The routing response process is as follows:

(1) After receiving RREQ, target node D examines the authenticity of the packet according to the principle of digital signature. If the message is validated, node D adds a new entry in its routing table to record the node information that sends the routing request message to it. It is assumed that node C and E are the last jump neighbors belonging to node D, and then node D conveys the RREP packet to the last hop neighbors C and E.
(2) Nodes C and E continue to send RREP to the node that forwarded the RREQ message to itself. The forward routing from itself to target node D is written down in the home routing table.
(3) Execute in turn until the routing reply message is forwarded to node S. The routing between the

source node S and the target node D should be stored.

After completing the above work, the two communication routes between the source node S and the target node D are built completely. Considering the frequent dynamic changes of ad hoc network structure, for the sake of preventing the unexpected failure of routing in the process of message transmission, two paths are selected intelligently according to the decision tree to enhance the invulnerability and security of network transmission.

The process of establishing routing between source node S and target node D is shown in Fig. 2.

The routing table stored in the network node mainly contains the following fields: the IP address of the target node, the serial number of the target node, the effective flag bit of the destination node's serial number, the IP address of the next hop node, the hop number of this node reaching the destination node, the precursor list, the lifetime (routing failure or deletion time), the network layer interface, other states and routing flags.

Each source node will increase its serial number by 1 before sending RREQ; when the target node obtains the RREQ packet, it will increase its serial number by 1 before sending RREP. When the source node gets RREP, it can judge whether to update the valid routing by comparing whether the serial number of the target node is increased or not.

The routing table stored by the node is composed of multiple routing entries. Each entry does not need to record all the node information of the routing, but only needs to mark the message of the next jump node. This can reduce the burden of generating the routing table and the maintenance cost. For an established routing, it is necessary to assign a sequence number as an identifier and store it in the source node and target node. In the later stage, the size of the sequence number can also be used to determine whether the routing is the latest.

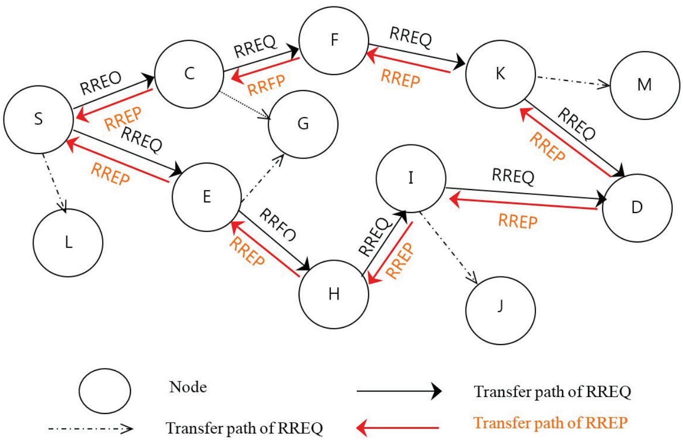

Fig. 2. IAODV route discovery diagram.

4.2.2.2 Routing maintenance

The core function of routing maintenance is the spontaneous monitoring of links between adjacent nodes by each node with strong ability. This routing algorithm adopts the method of intelligent control to manage the routing table. Routing maintenance operates differently in different network, mainly in the following two ways:

(1) If the quantity of mobile nodes in the network reaches 40%, it is unnecessary to maintain the

routing table. When there is message transmission, it intelligently establishes the path between the source and the target node on demand.

(2) When the quantity of mobile nodes in the network does not match up 40%, AODV routing protocol is still used to send Hello message frames to one hop neighbor node periodically to monitor its activity. In the process of monitoring, if the node does not get the response message frame of the neighboring node in the specified ALLOWED_HELLO_LOSS* HELLO_INTERVAL millisecond time, it is considered that there is no path between the node and the neighboring node, and the path is deleted from the routing table directly and broadcast the message in the network. If it is found that the two attribute values of some nodes have reached the critical value, the broadcast node IP and the routing error frame RREP in the network will be deleted, and if there is a data transmission task in the future, the routing between the nodes will need to be re-established. If all the nodes on the path are in good condition and can continue to be competent for the transmission task, no updates will be needed, when the transmission is received, continue to use this path for data transfer tasks.

4.3 Simulation Experiment

For the sake of verifying the availability and validity of the intelligent routing algorithm (IAODV), in an environment where two attribute values of nodes are below the critical value of communication, NS2 is used to simulate the IAODV and AODV routing protocols. Fifty test nodes are placed in the experimental scenario. The main parameters tested are packet loss rate, packet delivery rate and routing overhead. The transmission delay per hop is set to 100 milliseconds. All the experimental results are obtained from the Trace file.

4.3.1 Packet loss rate

Packet loss rate mainly calculates the probability of unsuccessful delivery in the process of data transmission. There are many reasons for packet loss, such as attacks, selfish behavior of nodes or interference of wireless channels. The smaller the packet loss rate is, the higher the routing reliability is, and the better the routing protocol is. Fig. 3 is the test result of packet loss rate of IAODV routing protocol and AODV routing protocol. From the graph, it can be seen that the packet loss rate of IAODV routing protocol is less than that of AODV routing protocol. This is mainly because the route of IAODV is achieved by evaluating each index of the node.

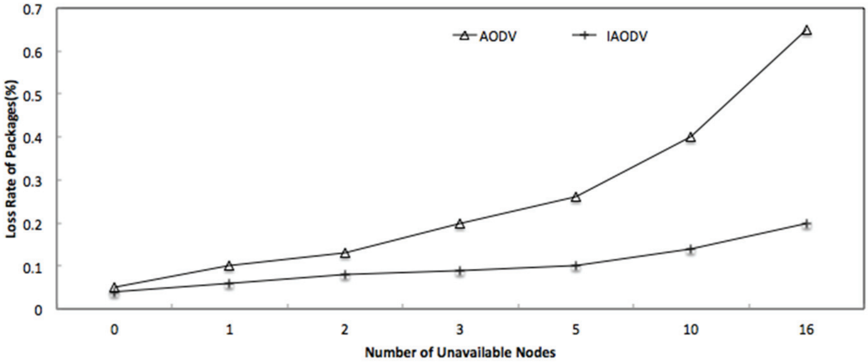

Fig. 3. Packet loss rates of IAODV and AODV routing protocols.

4.3.2 Packet delivery rate

Packet delivery rate is a key to estimating routing protocols as well. It comes from the result of calculating the ratio of the number of valid datagram received by the destination to the quantity of datagram transmitted from the source. If the packet delivery rate is high, it means that the probability of data message being lost is small, which indicates that the routing protocol is better. Fig. 4 is a comparison of packet delivery rates between IAODV and AODV routing protocols. The experimental demonstrates that the packet delivery rate of IAODV routing protocol is instable, but the overall performance of IAODV routing protocol is significantly better than AODV routing protocol. As can be seen from the results, the established routing improves the proportion of effective transmission of messages because it takes the ability of each node forwarding data into account based on intelligent decision tree selection.

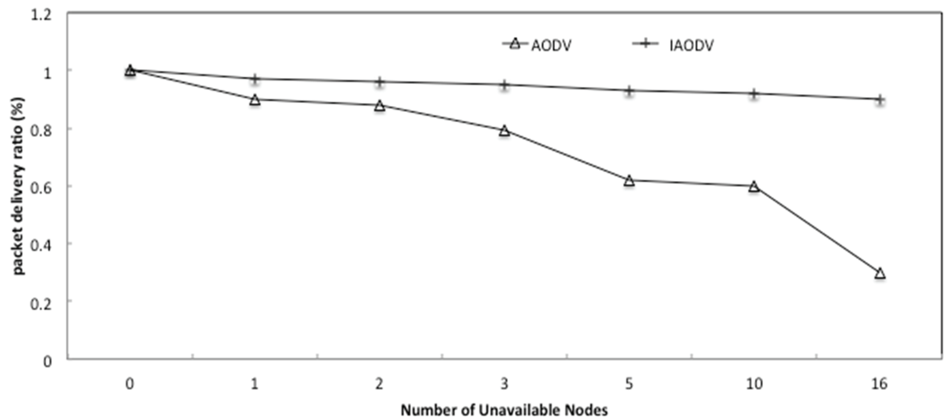

Fig. 4. Packet delivery rates of IAODV and AODV routing protocols.

4.3.3 Routing overhead

Finding effective routing requires bandwidth consumption. Routing overhead can be obtained by calculating the quantity proportion of sending routing messages to all data packets. The larger the proportion, the poorer performance of routing protocols. Fig. 5 shows the respective routing overhead of IAODV and AODV routing protocols under the same amount of nodes in the network. The

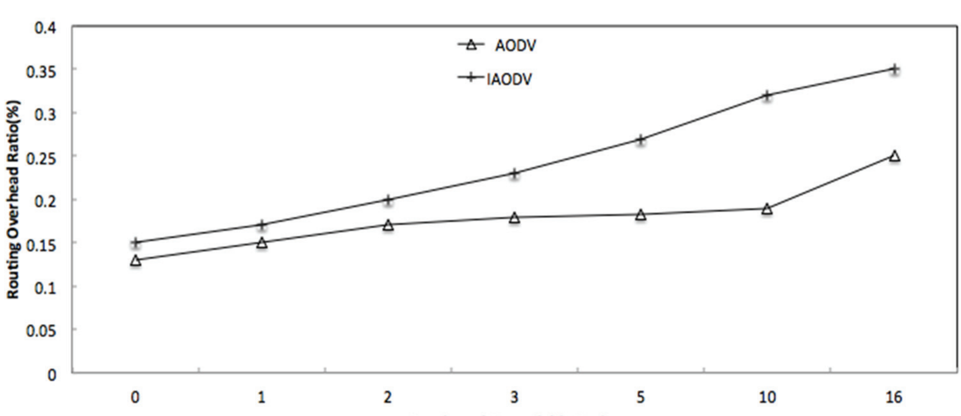

Fig. 5. Routing overhead of IAODV and AODV routing protocols.

experimental results evidently tell that the routing overhead of IAODV routing protocol is less than that of AODV routing protocol. This is mainly because IAODV routing protocol no longer consumes energy to maintain the network, but intelligently establishes communication links between nodes using on-demand strategy when the nodes in the network move too fast and the rigid topology changes frequently. Compared with AODV routing protocol, it significantly reduces unnecessary routing message sending, so the routing overhead is significantly lower than AODV routing protocol. Based on the above results, IAODV routing protocol is more applicable for dynamic Ad Hoc wireless networks.

5. Conclusion

There are many studies on routing protocols in Ad Hoc networks, but most of them are based on the assumption that there is a very friendly relationship between nodes, and every node will readily forward messages. Faced with the complex network environment, this assumption does not exist; and there are various targeted routing attacks, such as flooding attacks, witch attacks, which pose a great threat to the security of routing protocols.

Nodes in ad hoc networks have many characteristics, such as random movement, limited energy, self-protection and limited transmission capacity, which have a significant impact on the construction of communication links in the network. To solve the above problems, a decision tree is introduced to optimize routing nodes.

Based on AODV algorithm, an intelligent decision-making routing strategy (IAODV) is proposed. In the algorithm, the five attributes of node energy, computing power, speed, transmission distance, and reliability are taken as the basis of segmentation, and the information gain of each attribute is calculated. The attributes with the greatest information gain are selected as decision nodes in turn, and the decision tree of the routing node is constructed to determine the rules of the selection of the routing node. In the process of routing discovery, the idea of decision tree is integrated. After paying some extra storage space and computing time, the reliability, security and availability of routing are guaranteed, and the robustness of network is greatly improved, which avoids the disadvantage of using a single short path to select the best route. In the simulation experiment, three evaluation indexes, packet loss rate, packet delivery rate and routing overhead are selected to compare IAODV with AODV algorithm. The experimental results show that IAODV has better performance and better adaptability in ad hoc network with frequent node mobility.

Acknowledgement

This paper is supported by Hebei Population Health Information Engineering Technology Research Center.

References

[1] B. Xu, S. Hischke, and B. Walke, “The role of ad hoc networking in future wireless communications,” in *Proceedings of International Conference on Communication Technology Proceedings (ICCT)*, Beijing, China, 2003, pp. 1353-1358.

[2] J. Wang, C. Wang, Q. Wu, and Y. Gong, *Ad Hoc Mobile Wireless Network*. Beijing, China: National Defense Industry Press, 2004.

[3] J. N. Turner and C. S. Boyer, *Ad Hoc Networks: New Research.* New York, NY: Nova Science Publishers, 2009.

[4] X. Zhu, "Mobile ad hoc network security research," M.S. Thesis, Xi'an University of Electronic Science and Technology, Xi'an, China, 2004.

[5] S. Wang and H. Yang, "Research and analysis of mobile ad hoc network routing protocol," *Computer Age*, vol. 3, pp. 14-16, 2006.

[6] Q. Zhang and M. Luo, "Mobile ad hoc network security strategy," *Telecommunication Switching*, vol. 1, pp. 29-33, 2006.

[7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, New Orleans, LA, 1999, pp. 90-100.

[8] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications*, London, UK, 1994, pp. 234-244.

[9] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*. Boston, MA: Springer, 1996, pp. 153-181.

[10] D. B. Johnson, D. A. Maltz, and Y. C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)," 2004 [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-dsr-10.

[11] Y. Xiao and X. Shan, "Wireless Ad-hoc network and its research challenges," *Telecommunications Science*, vol 6, pp. 12-14, 2002.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21-38, 2005.

[13] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*, Paris, France, 2002, pp. 78-87.

[14] B. Dahill, B. N. Levine, E. M. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," University of Massachusetts, Amherst, MA, *Technical Report UM-CS-2001-037*, 2001.

[15] H. Jiang, Y. Meng, Y. He, and S. Cheng, "An energy-efficient multicast routing protocol for mobile ad hoc networks," *Journal of Circuits and Systems*, vol. 7, no. 2, pp. 115-118, 2002.

[16] C. Ying and M. L. Shi, "QoS Routing in ad-hoc network," *Chinese Journal Computers,* vol. 24, no. 10, pp. 1026-1033, 2001.

[17] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security*, Atlanta, GA, 2002, pp. 1-10.

[18] L. Venkatraman and D. P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 63, no. 2, pp. 214-227, 2003.

[19] M. Akhlaq, M. N. Jafri, M. A. Khan, and B. Aslam, "Integrated mechanism of routing and key exchange in AODV," *WSEAS Transactions on Communications*, vol. 6, no. 4, pp. 565-572, 2007.

[20] J. R. Douceur, "The Sybil attack," in *Peer-to-Peer Systems*. Heidelberg, Germany: Springer, 2002, pp. 251-260.

[21] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 24, no. 11, pp. 612-613, 1979.

[22] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.

[23] J. R. Quinlan, "Induction of decision trees," *Machine Learning*, vol. 1, no. 1, pp. 81-106, 1986.

Yongfei Ye https://orcid.org/0000-0002-1027-0501

She is working as an Associate Professor in School of Information Science and Engineering in Hebei North University, Zhangjiakou, China. She received M.S. in computer software and theory from Yanshan University in 2008. Her research interest fields include information security, data analysis and precision agriculture.

Xinghua Sun https://orcid.org/0000-0002-5636-1505

He is a PhD student at Shanghai Normal University. He is working as an Associate Professor in School of Information Science and Engineering in Hebei North University, Zhangjiakou, China. He received M.S. degree in School of Mathematical Information in Shanghai Normal University in 2007. His current research interests include mobile communication and lighting control network.

Minghe Liu https://orcid.org/0000-0002-5094-3993

He is working as a lecturer of school of Economics and Management in Hebei North University, Zhangjiakou, China. He received his LLM in Sociology from Guizhou University in 2010. His research interest fields include population and development, information transmission.

Jing Mi https://orcid.org/0000-0002-8768-1675

She is working as an Assistant in School of Information Science and Engineering in Hebei North University, Zhangjiakou, China. She graduated from North China Electric Power University in 2016 with a master's degree in Electronic and Communication Engineering. Her main research fields include electronic information and communication engineering.

Ting Yan https://orcid.org/0000-0003-4497-9014

She is working in School of Information Science and Engineering in Hebei North University, Zhangjiakou, China. She received a master's degree in software engineering from Peking University in 2018. Her research interest fields include data analysis, cloud computing and artificial intelligence.

Lihua Ding https://orcid.org/0000-0003-1803-5669

She is working in School of Information Science and Engineering in Hebei North University, Zhangjiakou, China. She received her master degree in computer technology from Capital Normal University in 2017. Her research interest fields include mobile communication and natural language processing.