IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 30, 2020, accepted January 17, 2021, date of publication January 27, 2021, date of current version March 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3054891

An Active-Routing Authentication Scheme in MANET

JINBIN TU, DAHAI TIAN, AND YUN WANG, (Member, IEEE)
Key Laboratory of Computer Network and Information Integration, MOE, Nanjing 210096, China
School of Computer Science and Engineering, Southeast University, Nanjing 210096, China

Corresponding author: Yun Wang (ywang_cse@seu.edu.cn)

This work was supported in part by the National Hi-Tech Project, China, under Grant 315055101, and in part by the Collaborative Innovation Center of Novel Software Technology and Industrialization.

ABSTRACT Mobile ad-hoc networks (MANET) is a network mode that does not depend on network infrastructure and central access. The fast and flexible networking mode of MANET renders its wide applications in specific scenarios. However, rapidly changing topology and open channels bring potential security problems. In this paper, we proposed an active-routing authentication scheme (AAS) based on the characteristics of active routing protocols. We formally demonstrated that the AAS is effective against selective forwarding attack, false routing attack, byzantine attack and route spoofing attack using the BAN logic considering the possibility of malicious nodes mingling in MANET. Experimental results show that the AAS is compatible with multiple active routing protocols and it is able to increase the packet delivery rate by 33.9%, with an average increase of 18.4% in the network containing some malicious nodes. Furthermore, the AAS is robust which remains the average network connection rate reach 1.6 times of the collusion attack prevention-OLSR(Cap-OLSR) protocol and preserves 79.2% of the network performance in simulation experiments with attacks from malicious nodes.

INDEX TERMS Mobile ad-hoc network, active routing, authentication scheme, secure routing.

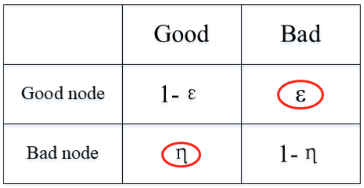
I. INTRODUCTION

Mobile ad-hoc networks (MANET) [1] is a self-configuring wireless network consisting of wireless devices with mobility. MANET has the characteristic of minimal configuration and rapid deployment, which is suitable for emergency situation scenarios such as natural disasters, military conflicts and emergency medical care, etc. Due to the characteristics of network and application scenarios, the topology of MANET is variable and unpredictable, bring great challenges to security [2]. In MANET, traditional security measures are no longer effective. Various attack behaviors, such as, selective forwarding attack, false routing attack, byzantine attack and so on cause the security problems of MANET increasingly prominent.

Active routing protocols [3], also known as table-driven routing protocols or prior routing protocols, are based on the principle that each node maintains a routing table that contains routing information for all reachable nodes in the network. A node obtains the route to the destination by looking up the routing table immediately for sending messages with few delays.

Active routing protocols periodically maintain the topology of the network and update routing information, relying on the perception of local topology changed by nodes. Each node can periodically broadcast the HELLO message. The time to live (TTL) of the message is set to 1, so that the message cannot be forwarded. The node maintains its neighbor list by receiving the HELLO messages. When the source node of the HELLO message is not in the neighbor list, it indicates that a new node has joined the local topology. And when the node cannot receive the HELLO message sent by a neighbor node periodically, it means that the neighbor node has exited local topology. When nodes in the network sense the change of local topology information, they will reflect the change to the entire network in time by broadcasting the topology control (TC) messages. After that, nodes will recalculate the routes to other nodes based on the updated topology information and the routing algorithm agreed in advance. Common active routing protocols, such as Optimized Link State Routing Protocol (OLSR) and Destination-Sequenced Distance Vector Protocol (DSDV) [4], use the above mechanism to update routing information.

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Verticale.



	Good	Bad
Good node	1- ε	ε
Bad node	η	1- η

FIGURE 1. Probability of node authentication.

In the actual environment, it is necessary to set the network number for the nodes. Nodes with the same network number will automatically join the same network.. In order to ensure the security of networks, a node, which is about to join the network, needs to pass the verification of authentication algorithms at first. If the authentication failed, in principle, the node should not communicate with other nodes in the network and participate in the construction of the network topology. In the viewpoint of the active routing protocol, nodes that are configured for the network have no difference from others. It means that the failure of the authentication algorithm cannot affect the routing protocol's behavior on the node. The unauthenticated node is able to play the same role as other authenticated nodes in the network topology maintained by the routing protocol, for instance, acting as a hop on communication routes. Unless the unauthenticated node actively moves away from the network, the impact on other nodes in the network is inevitable. Therefore, in MANET with active routing protocols, it is a challenge to prevent nodes that does not pass the authentication from affecting the construction of topology and routing table of the network.

As shown in figure 1, the rows mean the types of the node, and the columns mean the probability of the certification results. As we can see that there are η false-positive and ε false-negative nodes since the accuracy of the authentication algorithm cannot be perfectly ensured resulting from the probability of bit error in the wireless channel and the capture of trusted nodes by malicious nodes.

False-positive nodes referred that the malicious nodes are misjudged as the trusted nodes through authentication due to the interference of uncertainties, while false-negative nodes are the trusted nodes which are misidentified as the malicious nodes. The uncertainty consists of three scenarios: authentication algorithm error, wireless channel error code and tampering due to attack. The presence of both false-positive and false-negative nodes have adverse effects on the network. How to reduce the effect is the second challenge of this paper.

Considering the mentioned challenges, we propose the AAS and contributions of this paper are summarized as follows:

1) The novel AAS we proposed is the first authentication scheme for active routing in MANET as far as we know. The AAS is compatible with multiple active routing and uncouples the relation between authentication and routing in MANET. Meanwhile, it can prevent malicious nodes from participating in the construction of the network, which is a big challenge for traditional active routing protocol.
2) We formally demonstrated that the AAS is effective against selective forwarding attack, false routing attack, byzantine attack and route spoofing attack using the BAN logic considering the possibility of malicious nodes mingling in the network.
3) We introduced an expiration time in the AAS considering the possibility of the node attributes changing over time. We considered connectivity and certification costs as the evaluation criteria and obtained the optimum reference value of expiration time by Analysis of Variance Analysis of Variance (ANOVA).

TABLE 1. Abbreviations table.

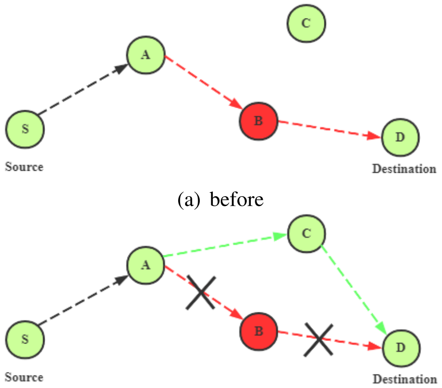
Abbreviations	Full Words
MANET	Mobile ad-hoc networks
AAS	Active-routing authentication scheme
Cap-OLSR	Collusion attack prevention-OLSR
TTL	Time to live
TC	Topology control
OLSR	Optimized Link State Routing Protocol
DSDV	Destination-Sequenced Distance Vector Protocol
ANOVA	Analysis of Variance Analysis of Variance
TOHIP	Topology-hiding Multipath Routing Protocol
ZRP	Zone Routing Protocol
SZRP	Secure Zone Routing Protocol
UAVs	Unmanned aerial vehicles
SAR	Security-aware ad-hoc Routing
MPR	Multi point Relay
SAFEACO	Safety Aware Fuzzy Enhanced Ant Colony Optimization
UDP	User Datagram Protocol

The abbreviations table of this paper is as shown as table 1, and the rest of this paper is organized as follows. Section II introduces the related work. In section III, we describe various possible attack modes, corresponding solutions and the AAS scheme in detail. Furthermore we give a formal description and proof of related strategies using BAN logic in section IV. The effectiveness and robustness of the scheme are explored experimentally in section V. And section VI are the conclusions and future work.

II. RELATED WORK

A lot of research literature is working on the MANET security issue. There are two categories can be separated from these articles. One focuses on increasing the confidentiality of information such as network topology and data transmission to protect against external attacks. Zhang *et al.* [5] propose the topology-hiding multipath routing protocol TOHIP for the problem of topology exposure in multipath routing protocols. The protocol does not include link connection information in the routing information, thereby avoiding malicious nodes inferring the network topology by capturing the routing information, ensuring the confidentiality of the network. When there is no attack, the TOHIP protocol maintains normal route lookup performance, and in the presence of the attack, TOHIP resists the attack with lower overhead and shorter route convergence time. Rahman and Mahi [6] propose a hybrid Adhoc routing protocol based on the zone routing protocol(ZRP), Secure Zone Routing Protocol(SZRP). The SZRP protocol integrates digital signatures and asymmetric encryption algorithms through advanced security techniques such as SHA-256, HMAC and pbkdf2 to ensure the security of data transmission in the network. In [7], a heuristic algorithm is proposed to find the safest path from the source UAV to the destination UAV. These algorithms do not remove malicious nodes from the network, so they can still participate in the construction of the network.

The other pays attention on the node authentication algorithm for trusted routing to defend against some internal attack. Eirefaie *et al.* [8] make improvements to the ZRP protocol against packet loss attacks, using the concept of trustworthiness to detect packet loss attacks by nodes. After sending a data packet to the neighbor node, the node keeps a copy of the packet and sets a timer to monitor the behavior of the neighbor node. If the neighbor node completely forwards the data packet within a certain period of time, the node is considered to be performing well and the confidence value is raised. Otherwise, it is considered that the neighbor nodes with malicious behavior will reduce the trust value. Within an updated interval of trust value, when the number of lost data packets exceeds the predefined threshold, the node is identified as a malicious node. Trust-based ZRP protocol selects the most reliable and safe route to the destination by trust value of node. Yi *et al.* has presented the security-aware ad-hoc routing (SAR)method (SAR) [9]. The classification of nodes by SAR scheme depends on the trust level of nodes. This happens by sharing the secret group key for the nodes under same classification. The source node S should ensure the basic necessary security during the process of route discovery. This is done with the help of the element in the path followed during routing between source S and destination D. This mentioned stipulation can be enforced by S by means of the shared key encryption on route request packet using the shared key linked to the respective security level. In spite of the observed merits, shared key method has problems in the SAR approach as the possibility of more malicious agents over other nodes is considered by classifying under high security for accessing to the secret group keys. In [10],there are two measures available for the main node, one is local isolation, and the other is to notify the entire network that the malicious node is isolated by the entire network. In Cap-OLSR [11], address of the malicious nodes will be removed from the list of one-hop and two-hop neighbors, causing the node to be isolated from the network. The routing strategy of [12] is to exclude nodes whose trust value is lower than the threshold, and consider that the remaining nodes can constitute a trusted network. Nabou *et al.* [13] propose a new Multi point Relay (MPR) computation in OLSR, MPR can ensure the security of OLSR routing in the process of route construction against single black hole attack. The distributed fuzzy logic module eliminates the linear nodes of complexity from the Safety Aware Fuzzy Enhanced Ant Colony Optimization (SAFEACO) [14] routing process, resisting black hole, Sybil and inundation attacks at the same time. In [15], it uses two phases to counter malicious Unmanned aerial vehicles (UAVs) attacks. Firstly, they identify and remove malicious UAVs. Secondly, a mobile agent is used to eliminate malicious UAVs. It can ensure the reliability of neighbor UAVs. Above paper ensures the trustworthiness of the nodes forming the route by shielding the nodes considered untrustworthy according to some trust mechanism. However, once the malicious node hijacks the normal node and shields the surrounding normal nodes, there will be no node available for routing. Otherwise, these authentication algorithms have high coupling degree with the routing protocol.



(a) before

(b) after

FIGURE 2. Selective forwarding attack example.

III. THE AAS APPROACH

A. ASSUMPTIONS

We supposed that in a MANET, some malicious nodes can obtain the network number to join the network and can become authenticated node by hijacking a normal node or exploiting a misjudgment of authentication algorithm like figure 1. These malicious nodes have the ability to tamper with neighbor node authentication messages, to selectively forward and tamper with passing packets. Malicious nodes are always minority.

B. ATTACK METHODS AND COUNTERMEASURES

1) SELECTIVE FORWARDING ATTACK

A node, as a hop in the communication route of other nodes, which selectively forwards or discards the packets that need to be forwarded. This node can launch selective forwarding attack [16].

The result of the execution of the authentication algorithm does not affect the behavior of the active routing protocol at the node. However, the malicious node still has the opportunity to participate in the construction of topology and routing table even if it cannot directly communicate with other nodes in the network without authentication.

As shown in figure 2(a), although node B does not pass the authentication in the communication range of nodes, this node is still selected as a hop of the communication route

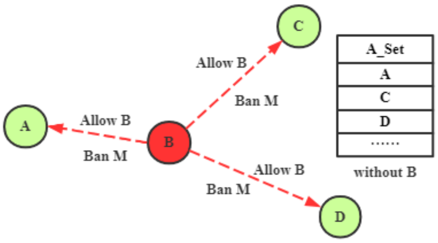


FIGURE 3. False routing attack example.

between node S and node D by active routing protocol. As a result, node B can maliciously attack the passing messages.

For the selective forwarding attack, we propose the firewall global shielding strategy. As shown in figure 2(b), assuming that node B fails to pass the authentication launched by node A and node D, and then, node A and node D will set shielding rules about node B according to its IP address and broadcast it to entire network. After receiving the broadcast message, other nodes will also set the same shielding rules. The active routing protocols are aware of the network topology and maintains routing tables by receiving Hello message from neighbor nodes, while firewall can prevent nodes in the network receiving Hello messages from unauthenticated nodes. So firewall global shielding strategy can avoid unauthenticated nodes participating in the construction of topology and routing. Moreover, this strategy can fundamentally avert the influence of unauthenticated nodes in the network.

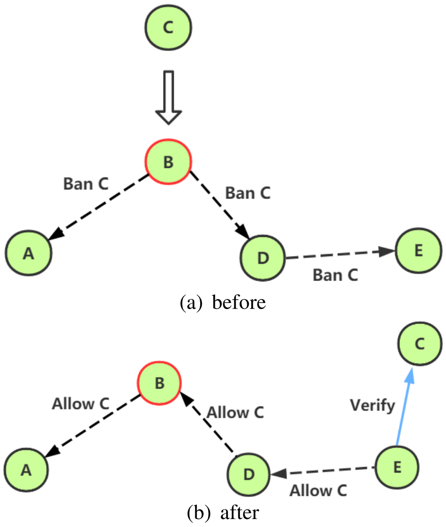
2) FALSE ROUTING ATTACK

As shown in figure 3 shown, assuming that node B does not pass the authentication initiated by node M. Node B sends broadcast messages attempting to shield node M before being shielded globally. This mode of attack is called false routing attack [17].

To prevent the false routing attack, we introduced an authenticated node list called A_Set for each node. The A_Set will initialize to the N_Set in section III-B4. When they receive the broadcast message from node B, these nodes will ignore the malicious broadcast message from node B since it is not in A_Set. After that, the malicious shielding attack launched by node B before the shielding rules about node B will be prevented.

3) BYZANTINE ATTACK

In the network, false-negative nodes will be permanently shielded and unable to join the network again. More seriously, false-positive nodes will maliciously shield other normal nodes which want to join the network by broadcasting the shielding rules. This kind of behavior will produce a large number of false-negative nodes. As a result, there are less nodes available in the network, which eventually brings the network to a halt. And we call this attack byzantine attack [18]. As shown in the figure 4(a), node B is a false-positive node. When node C attempts to join the network through node B, node B will maliciously shield node C and force it to be a false-negative node, so that node C cannot join the network normally.



(a) before

(b) after

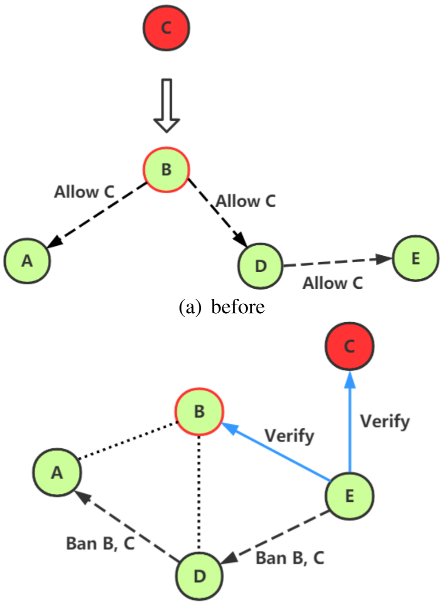
FIGURE 4. Byzantine attack example.

In order to avoid the byzantine attack, we introduce an expiration mechanism for shielding rules based on the global shielding strategy. During the expiration time, the Hello message from the shielded node cannot be received by other nodes due to firewall shielding rules. When the shielding rules expire, the Hello message from those nodes can be received again so that they can be authenticated again. Meanwhile, the mobility of the nodes enables the false-negative node to move to other nodes in the network to authenticate again. As shown in figure 4(b), after the shielding rule for false-negative node C expires, node C moves to the communication range of trusted node E, gets the authentication opportunity again and successfully joins the network, thus correcting the previous authentication results. It can be seen that the expiration mechanism of shielding rules can effectively resist byzantine attack from the false-positive nodes and avoid the network paralysis caused by no node available in the network.

4) ROUTE SPOOFING ATTACK

In figure 5(a), node B is a false-positive node in the network. When the malicious node C tries to join the network through node B, node B broadcasts a message to the network that node C is authenticated. In this way, the malicious node C be added to the A_Set easily, which will introduce more malicious nodes into the network. And we call it route spoofing attack [19].

In response to the route spoofing attack, each node in the network maintains a list of neighbor nodes called N_Set. For each node in the network, once a new node appears in its N_Set, the node will launch the authentication process. Therefore, for false-positive nodes B and C, as long as they appear in the communication range of other trusted nodes, they will be re-authenticate. In this way, there is an opportunity to identify the identity of malicious nodes B and C in



(a) before

(b) after

FIGURE 5. Route spoofing attack example.

Algorithm 1 Process Broadcast Messages Algorithm

```
1:  $M$ in the network receive a broadcast message from $N$
2:  if message type is $HELLO$ then
3:      if $N$ is a new neighbor of $M$ then
4:          initiate authentication process to $N$
5:      else
6:          maintain local topology information normally
7:      end if
8:  else if message type is $ShieldingNode$ then
9:      if $N$ is in $A\_Set$ of $M$ then
10:         set shielding rules for related node in the message
11:         remove it from $A\_Set$ if it exists
12:     else
13:         discard the message
14:     end if
15: else if message type is $NodePassAuthentication$ then
16:     if $N$ is in $A\_Set$ of $M$ then
17:         add the node in message into $A\_Set$
18:     else
19:         discard the message
20:     end if
21: end if
```

the network, so as to resist the routing spoofing attacks of nodes B and C.

C. THE AAS DESIGN

Based on the above analysis, we design the AAS as figure 6. There are three types of broadcast messages that each node may receive related to the AAS: HELLO messages, Shielding Node broadcast message, and Node Pass Authentication broadcast message. The processing flow of message (line 4) is shown in algorithm 1.

Algorithm 2 Authentication Process Algorithm

```
1:  $identify_{num} = 0$
2:  while $identify_{num} <= IDENTIFY_{MAX}$ do
3:      execution authentication algorithm
4:      if $N$ is illegal then
5:          $identify_{num}++$
6:      else
7:          add $N$ into A_Set of $o_i$ and broadcast Node Pass
    Authentication message
8:          return
9:      end if
10: end while
11: set shielding rule for $N$ and broadcast Shielding Node
    message
```

When node N attempts to join the network, N needs to pass the authentication of nodes in the network which are within the communication range of node N at first. When nodes receive the HELLO message broadcasted from node N, they will detect whether node N is a new neighbor node, and if so, they will initiate the authentication process to node N. The new node of the network may receive authentication requests from multiple nodes at the same time. Set $O\{o_1, o_2, \ldots o_n\}$ as the set of nodes that initiate the authentication process to node N, then node N needs to respond to the authentication requests of all nodes in set O (line 2-7). The authentication process is shown in Algorithm 2.

During authentication process, node N is allowed to retry up to $IDENTIFY_{MAX}$ times when it failed in order to avoid accidental factors. $IDENTIFY_{MAX}$ is an empirical value which is set to 3 in our experiments. When node N passes authentication, node o_i will add node N into A_Set and broadcasts Node Pass Authentication message about node N to the network. If node N does not pass authentication within the threshold, node o_i will shield the node N and broadcast Shielding Node message about it.

In addition, as shown in figure 7, the AAS decouples the authentication algorithm from the routing protocol. Active routing protocols provide authentication triggering mechanisms to authentication schemes, which provide trusted nodes to routing protocols. The authentication algorithm authenticates the node identity, and the communication encryption algorithm provides encrypted secure channel for the authentication scheme. In this way, research on authentication algorithms can focus on itself without considering the corresponding routing mechanism. In the worst case, each node in the network needs to execute authentication algorithm $IDENTIFY_{MAX}$ times for m neighbors, which means the time complexity is $O(m * IDENTIFY_{MAX})$. Because the AAS is based on the active routing protocols, each node needs to maintain the global topological information. In addition, they also need to preserve an A_Set and a N_Set for AAS, so the space complexity is $O(n)$, where n is the capacity of the network.

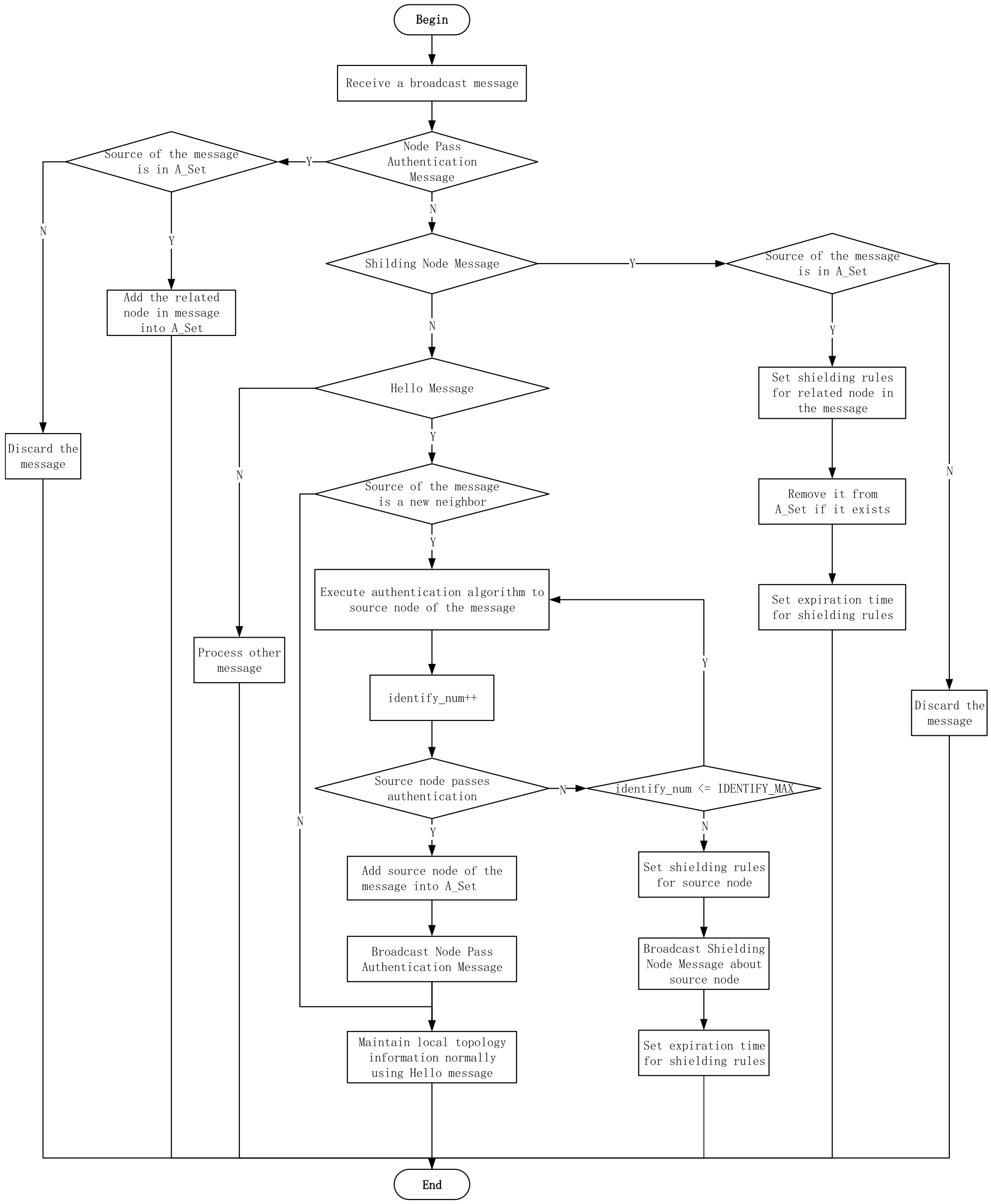

Begin
Receive a broadcast message
Node Pass Authentication Message
Source of the message is in A_Set
Y
N
Add the related node in message into A_Set
Discard the message
Shilding Node Message
Source of the message is in A_Set
Set shielding rules for related node in the message
Remove it from A_Set if it exists
Set expiration time for shielding rules
Discard the message
Hello Message
Process other message
Source of the message is a new neighbor
Execute authentication algorithm to source node of the message
identify_num++
Source node passes authentication
identify_num <= IDENTIFY_MAX
Add source node of the message into A_Set
Broadcast Node Pass Authentication Message
Maintain local topology information normally using Hello message
Set shielding rules for source node
Broadcast Shielding Node Message about source node
Set expiration time for shielding rules
End

FIGURE 6. The AAS scheme.

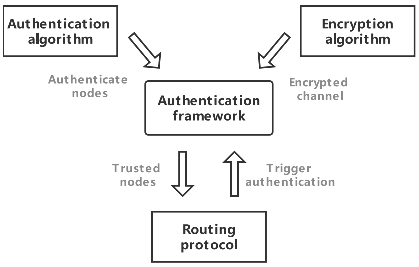


FIGURE 7. The decoupling principle.

IV. LOGIC PROOF

This section provides a formal description of the AAS using BAN logic to prove that the AAS can withstand attacks based on assumptions.

BAN logic is the most influential tool among the many formal analysis methods for authentication protocols. BAN is a belief-based modal logic. When applying BAN to inference the message is converted into a formula at first. Then reasonable assumptions are made according to the circumstances, and the reasoning rules of the logic is to infer that whether the agreement will accomplish the desired goals based on idealized protocols and assumptions.

A. BAN LOGIC BASIC SYMBOLS

We used some basic symbols of the BAN logic in this section as follows.

1) $P| \equiv X$: Entity P believes X or P would be entitled to believe X.

2) $P| \sim X$: Entity P once said X.
3) $P\#X$: Entity P says X.

The meaning of symbols, related lemmas and more details can be seen in [20].

B. EXTENDED SYMBOLS AND AXIOMS

In order to express the primitive operation in the AAS formally, we extend some symbols and a few rules. The extended symbols and their meanings are as follows:

1) AS : The set A_set.
2) $N_P^{t_i}$: N_set of P in time t_i.
3) $P| \times Q$: Entity Q is not accredited at entity P.
4) $P \Rightarrow AS$: Entity P joins in AS.
5) $P \Leftarrow AS$: AS rejects entity P.

And the extended axioms are as follows:

1) Rejection rule

$$ER1 : \frac{P \notin AS, P\#X}{AS| \times X}$$

2) AS belief rule

$$ER2 : \frac{P \in AS, P| \sim P\#X}{AS| \equiv X}$$

3) Join-in rule

$$\begin{aligned} \Phi &= ((N_Q^{t_{i+1}} - N_Q^{t_{i+1}} \cap N_Q^{t_i}) \cap AS) \\ ER3 &: \frac{AS| \times Q, \forall P_i \in \Phi, P_i\#P_i| \equiv Q}{AS| \equiv Q} \\ ER4 &: \frac{AS| \equiv P, P \notin AS}{P \Rightarrow AS} \end{aligned}$$

4) Rejected rule

$$\begin{aligned} \Phi &= ((N_Q^{t_{i+1}} - N_Q^{t_{i+1}} \cap N_Q^{t_i}) \cap AS) \\ ER5 &: \frac{Q \in AS, \exists P \in \Phi, P\#P| \times Q}{AS| \times Q} \\ ER6 &: \frac{P \in AS, AS| \times P}{P \Leftarrow AS} \end{aligned}$$

ER1 indicates that all entities in the AS do not believe any messages sent by the P which does not belong to the AS. *ER2* expresses that AS believe any messages sent from AS members, including the trust and doubt about other entities. *ER3* and *ER4* mean that if an untrusted entity Q wants to join AS, when its N_set changes, Q can gain the trust of the AS and join the AS only if all new legal neighbors trust Q. And if there is a new legal neighbor P thinks that Q is not trustworthy, the AS will not believe Q either and it will be removed from the AS as described as *ER5* and *ER6*.

C. BAN PROOF AGAINST SELECTIVE FORWARDING

According to the section III-B1, the initialization assumption is:

$$AS = \{A, C, D\}$$

The proved goal is:

$$AS| \times B$$

Proof :

Because $B \notin AS$, according *ER1* then

$$\frac{B \notin AS, B\#X}{AS| \times B\#X}$$

D. BAN PROOF AGAINST FALSE ROUTING

According to the section III-B2, the initialization assumption is:

$$\begin{aligned} AS &= \{A, C, D\} \\ B\#B| &\equiv B \\ &B\#B| \times M \end{aligned}$$

The proved goal is:

$$AS| \times B| \equiv B$$
$$AS| \times B| \times M$$

Proof :

Because $B \notin AS$, according *ER1*, then

$$\frac{B \notin AS, B\#B| \equiv B}{AS| \times B| \equiv B}$$
$$\frac{B \notin AS, B\#B| \times M}{AS| \times B| \times M}$$

E. BAN PROOF AGAINST BYZANTINE

According to the section III-B3, the initialization assumption is:

$$\begin{aligned} AS &= \{A, B, D, E\} \\ B| &\sim B| \times C \\ N_C^{t_i} &= \{B\} \\ N_C^{t_{i+1}} &= \{E\} \\ E\#E| &\equiv C \end{aligned}$$

The proved goal is:
$C \Rightarrow AS$

Proof :

Because $B \in AS$, according *ER2*, then

$$\frac{B \in AS, B| \sim B| \times C}{AS| \times C}$$

Thus $(N_C^{t_{i+1}} - N_C^{t_{i+1}} \cap N_C^{t_i}) \cap AS = \{E\}$, according *ER3*, then

$$\frac{E\#E| \equiv C, E \in AS, AS| \times C}{AS| \equiv C}$$

according *ER4*, then

$$\frac{AS| \equiv C}{C \Rightarrow AS}$$

F. BAN PROOF AGAINST ROUTE SPOOFING

According to the section III-B4, the initialization assumption is:

$$\begin{aligned} AS &= \{A, B, C, D, E\} \\ B| &\sim B| \equiv C \end{aligned}$$

TABLE 2. Relevant parameters.

Parameter	Value
Moving area	800 m * 800 m
Communication node pair	3
Number of relay nodes	20
Proportion of false-positive nodes	5%∼50%
Communication range	200m
Mobility model	Mass Mobility
Speed of node	exponential(10) m/s
Simulation time	40s
Send Interval	100ms
Data type	UDP message
Link layer protocol	CSMACA

$$N_C^{t_i} = \{B\}$$
$$N_C^{t_i+1} = \{B, E\}$$
$$E\#E| \times C$$

The proved goal is:

$C \Leftarrow AS$

Proof :

Because $(N_C^{t_i+1} - N_C^{t_i+1} \cap N_C^{t_i}) \cap AS = \{E\}$, according *ER5*, then

$$\frac{E\#E| \times C, E \in AS}{AS| \times C}$$

according *ER6*, then

$$\frac{AS| \times C}{C \Leftarrow AS}$$

V. EXPERIMENTAL ANALYSIS

A. EFFECTIVENESS

The effectiveness is that the scheme can exclude malicious nodes from the network and prevent them from participating in the construction of network topology and routing, so as to eliminate the influence of malicious nodes on network communication.

Experiments on the OMNeT ++ simulation platform are carried out to show the effectiveness. The experimental parameters are set as table 2.

In this experiment, we set three pairs of nodes (source, destination) to communicate, which randomly locate at the initial position of the network. Meanwhile, in order to avoid the influence of accidental factors, we randomly select the malicious nodes which can discard all received packets for each proportion of them. And the average value of multiple experiments are considered as the experimental result. The node movement model is set to MassMobility mode, that is, random Waypoint mode, and the node movement speed follows the exponential distribution with the mean value of 10m/s. In the 40s simulation time, each source node sends a total of 400 User Datagram Protocol (UDP) datagrams.

We compare with the Cap-OLSR protocol to verify the effectiveness of the AAS. Based on the OLSR protocol, this protocol adds an authentication algorithm for the identity of neighbor nodes, and improves the routing update algorithm based on the authentication results, so as to shield the malicious nodes in the process of routing update. Similarly, AAS can achieve the same effect as Cap-OLSR protocol when the AAS is introduced in the network where OLSR routing protocol and node authentication algorithms are deployed. There are three groups of experiments, namely (1) OLSR protocol & Authentication algorithm, denoted as group 1; (2) OLSR protocol & Authentication algorithm & AAS, denoted as group 2; (3) Cap-OLSR protocol, denoted as group 3. The experimental results are shown in figure 8. In order to exclude the influence of irrelevant factors, we set the authentication algorithms for node identity in the three groups of experiments the same as Cap-OLSR.

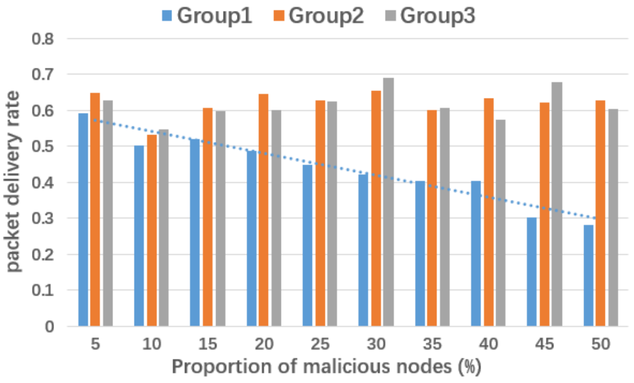


FIGURE 8. Results of packet delivery rate.

In figure 8, it can be seen that with the increase of proportion of malicious nodes, the packet delivery rate declines in group 1. Because once the malicious node becomes a hop of the communication route, all packets passing through it will no longer be forwarded, resulting in the drop of packet delivery rate. But in group 2 and group 3, due to the mechanism of avoiding the participation of malicious nodes in route construction, the delivery rate of packets is kept at a normal level and is barely affected by the increasing proportion of malicious nodes. What's more, it can be seen that our scheme achieves almost the same effect as Cap-OLSR under each proportion of malicious nodes.

In addition, our scheme is independent of specific routing protocols and is compatible with various active routing protocols and authentication algorithms. We use the DSDV protocol to verify the compatibility of our scheme with the active routing protocol. In the experiment, the packet delivery rate is compared before and after the introduction of the AAS with the combination of DSDV protocol and authentication algorithm for node identity in last experiment. The results are shown in figure 9.

The graph tells us that the packet delivery rate with the AAS is significantly higher by the increasing proportion of malicious nodes. The AAS is able to increase the packet delivery rate by 33.9%. The average increase of the ten groups of experiments is up to 18.4%. It manifests that the AAS is also compatible with DSDV protocol.

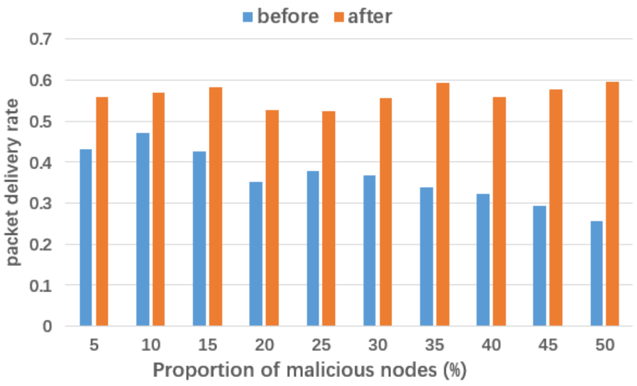


FIGURE 9. Results of packet delivery rate.

B. ROBUSTNESS

Connectivity is an significant foundation for network topology control in MANET. If any two nodes in MANET are able to communicate over one or more hops, the network is connected [21]. Connectivity determines the successful transmission of data between nodes, while the acquisition of network connectivity is the fundamental guarantee for designing the routing layer. In short, any design of the network is based on the assumption that the network is connected. There are many factors that affect connectivity, such as user density, transmit power, channel model, interference, etc. [22]. Polo Sanfi *et al.* obtained the critical transmission radius of the simple connectivity of the MANET (k = 1) under the Random Waypoint mobile model in [23], Christian Bettstetter obtained simple connectivity in [24]:

$$P_{noisonode} = (1 - P_{nodeiso})^n \tag{1}$$

$$P_{nodeiso} = e^{-n*\frac{\pi r^2}{S}} \tag{2}$$

where n denotes the number of nodes, r denotes the transmission range of the node, and S denotes the area of the network range where the nodes are located. This connectivity equation is used as a criterion for judging subsequent experiments.

The robustness of the AAS is manifested by the fact that when the authentication algorithm fails, the AAS can prevent the error from further affecting the network. From the analysis in section III, it is clear that the scheme compensates for the effects of errors in case the authentication algorithm makes an error. Reducing the dependence on the accuracy of the authentication algorithm is the embodiment of the robustness of the scheme. The robustness verification experiment simulation parameters are set as table 3.

As we know, false routing attacks, byzantine attacks, and route spoofing attacks may lead to the reduction of available nodes in MANET and eventually affect the connectivity of the network. In this experiment, we use connectivity as the criterion for validation. The higher the connectivity, the higher the percentage of routes found for the packet to be sent, and the higher the probability of the successful node transmission. And we assume that the normal nodes around the false-positive nodes will be considered as malicious nodes. Under the parameters of the table 3, the results are shown in the figure 10. The Cap-OLSR reduces the connectivity rate to 0 in a very short time. It means that there are no more available nodes in the network and the entire network has been paralyzed. The reason why it drops to 0 is that Cap-OLSR does not have the correction mechanism for nodes. The connectivity rate decreases in the early stages of the AAS experiment. This is because the normal node cannot participate in the network construction after the attack. When decreasing to the certain level, the connectivity rate will fluctuate up and down at a certain benchmark. It can be concluded that when facing errors or attacks due to the authentication algorithm, our proposed method can control the impact of the attack within a certain range, which reflects the robustness of the AAS.

We measure the average connectivity in multiple experiments by varying the radius of communication, as shown in figure 11. The results show that as the communication

TABLE 3. Relevant parameters.

Parameter	Value
Moving area	2000 m * 2000 m
Number of iterations	10000
Number of nodes	200
Number of false-positive nodes infiltrated	10
Communication range	200m
Mobility model	Random Waypoint
Speed of node	4 m/s
Expiration time	300

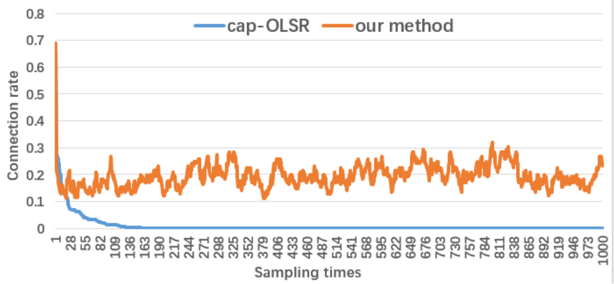


FIGURE 10. Connection rate result.

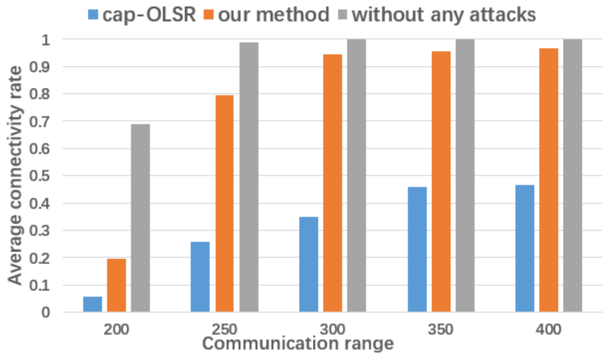


FIGURE 11. Average connectivity rate.

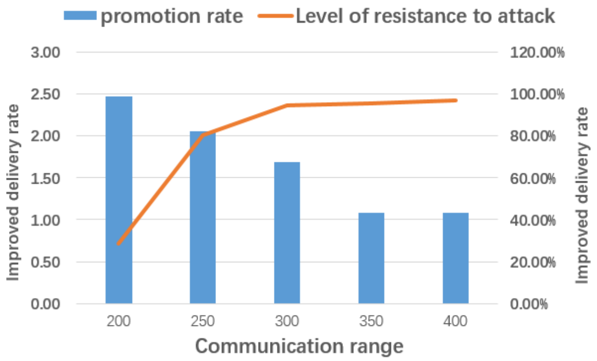


FIGURE 12. Improved delivery rate.

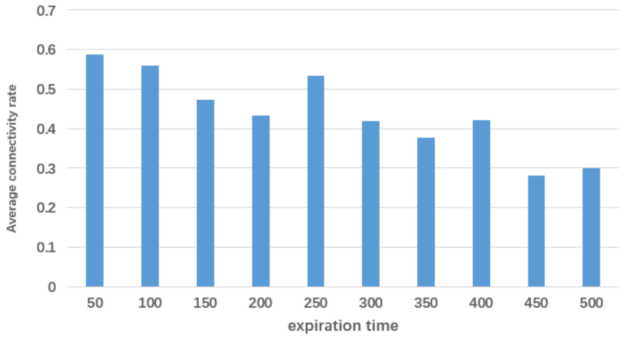


FIGURE 13. Average connectivity rate with different expiration time.

radius increases, the average connectivity rate of the different modes has an upward trend, because the increase in communication radius is more conducive to the connectivity between nodes. From figure 12, compared with the Cap-OLSR, in all cases, our method has a significant improvement effect, which is 1.6 times the Cap-OLSR average in the experiment. We also compare the connectivity rate with the same parameters without any attack to demonstrate the ability of AAS against attack. In figure 12, the resistance of our methods to malicious attacks increases with the radius of communication, and the average level of resistance is 79.2% which can demonstrate the robustness of the AAS.

C. SELECTION OF EXPIRY TIME

In this section, we study that how to set the value of expiration time. According to the parameters in the table 3, we perform several designed experiments by varying the expiration time. The results are shown in figure 13.

As shown in figure 13, with the expiration time increasing, the average connectivity rate shows a downward trend. This is because the increase in the expiration time leads to the increase in the number of shielded nodes in a shielding cycle, which will lead to the reduction in the number of available nodes in the network, thereby reducing the network connectivity. Obviously, the experiment in the figure 13 has no consideration of how to choose the expiration time. If the expiration time keeps reducing, it would be meaningless to introduce the shielding mechanism, and a tiny expiration time will increase the count of authentication and communication overhead. With this in mind, we consider the count of authentication as one of the judging criteria and we change it to average connectivity/certification counts. According to the authentication strategies mentioned in section III, the node performs authentication when its N_Set changes. In order to make the experimental results general and more informative, we change the values of various types of parameters for experimental statistics, and perform ANOVA as the new parameter table 4. The reason why we change the expiration time into a radio is that the speed of different sites and notes has impact on it in the real situation. As a result, above setting is more conducive to carry out the analysis. According to the connectivity formula, when the proportion of expiration time exceeds 1, there will be a situation where the number of available nodes is smaller but the connectivity is larger, so the upper limit does not exceed 1 and $n \gg 1$ in the connectivity formula.

TABLE 4. ANOVA relevant parameters.

Parameter	Value
Moving area side	2,3,4k m
Number of iterations	10000
Number of nodes	200:50:400
Number of false-positive nodes infiltrated	2:2:20
Communication range	200m
Mobility model	Random Waypoint
Speed of node	4,8,12 m/s
Expiration time	0.1:0.1:1 * side/speed

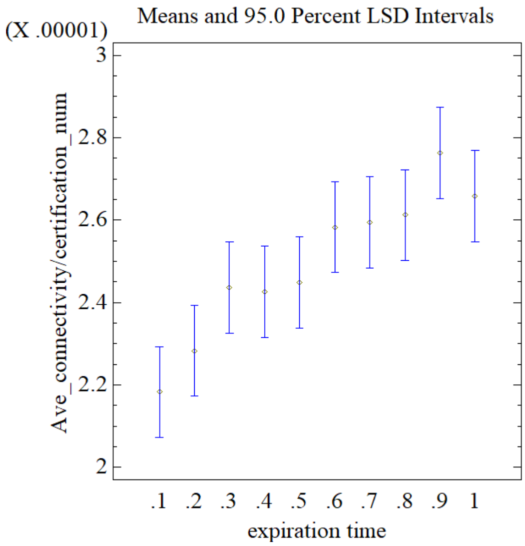


FIGURE 14. ANOVA result.

The ANOVA result indicates that when the expiration time is selected at a scale of 0.9, the evaluation function is max as shown in figure 14. Therefore, we believe that in the actual situation, when an expiration time is selected, the movement time of the node around the side of the area can be used as the benchmark, and the 90% time length can be used as the expiration time, which achieves better performance.

VI. CONCLUSION

This paper proposes the AAS based on active routing protocols in MANET. The scheme integrates four strategies: firewall strategy, firewall expiration time, authentication node list and neighbor node list. Without relying on authentication algorithms,AAS performs well on resisting the selective forwarding attacks, false routing attacks, byzantine attacks and routing spoofing attacks. Experimental results show that in a network including some malicious nodes, the AAS can increase the packet delivery rate up by 33.9%, with an average increase of 18.4%. At the same time, it can increase the network's connectivity rate to 1.6 times the Cap-OLSR rate under the attacks. In addition, the scheme provides the reference for setting the expiration time in real environment. In future work, we will further investigate the characteristics of reactive routing protocols as well as hybrid routing protocols to improve the compatibility of the security authentication scheme for routing protocols, and also we can focus on the other attack modes.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their constructive comments.

REFERENCES

[1] N. Khanna and M. Sachdeva, "BEST: Battery, efficiency and stability based trust mechanism using enhanced AODV for mitigation of blackhole attack and its variants in MANETs," *Adhoc Sensor Wireless Netw.*, vol. 46, nos. 3–4, pp. 215–264, 2020. [Online]. Available: https://www.oldcitypublishing.com/journals/ahswn-home/ahswn-issue-contents/ahswn-volume-46-number-3-2020/18830-2/

[2] S. Jamali and R. Fotohi, "Defending against wormhole attack in MANET using an artificial immune system," *New Rev. Inf. Netw.*, vol. 21, no. 2, pp. 79–100, Jul. 2016.

[3] M. Boulaiche, "Survey of secure routing protocols for wireless ad hoc networks," *Wireless Pers. Commun.*, vol. 114, no. 1, pp. 483–517, 2020.

[4] P. Sarao, "Comparison of AODV, DSR, and DSDV routing protocols in a wireless network," *J. Commun.*, vol. 13, no. 4, pp. 175–181, 2018.

[5] Y. Zhang, T. Yan, J. Tian, Q. Hu, G. Wang, and Z. Li, "TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 21, pp. 109–122, Oct. 2014.

[6] M. T. Rahman and M. J. N. Mahi, "Proposal for SZRP protocol with the establishment of the salted SHA-256 bit HMAC PBKDF2 advance security system in a MANET," in *Proc. Int. Conf. Electr. Eng. Inf. Commun. Technol.*, Apr. 2014, pp. 1–5.

[7] R. Fotohi, E. Nazemi, and F. S. Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100267.

[8] Y. Eirefaie, L. Nassef, and I. A. Saroit, "Enhancing security of zone-based routing protocol using trust," in *Proc. 8th Int. Conf. Informat. Syst. (INFOS)*, May 2012, pp. NW-32–NW-39.

[9] S. Kianpisheh, N. M. Charkari, and M. Kargahi, "Ant colony based constrained workflow scheduling for heterogeneous computing systems," *Cluster Comput.*, vol. 19, no. 3, pp. 1053–1070, Sep. 2016.

[10] A. Adnane, C. Bidan, and R. T. D. Sousa, "Trust-based security for the OLSR routing protocol," *Comput. Commun.*, vol. 36, nos. 10–11, pp. 1159–1171, Jun. 2013.

[11] A. B. C. Douss, R. Abassi, and S. G. E. Fatmi, "A trust management based security mechanism against collusion attacks in a MANET environment," in *Proc. 9th Int. Conf. Availability, Rel. Secur.*, Sep. 2014, pp. 325–332.

[12] B. Wang and X. Chen, "Opportunistic routing algorithm based on trust model for ad hoc network," *J. Commun.*, vol. 34, no. 9, pp. 92–104, 2013.

[13] A. Nabou, M. D. Laanaoui, and M. Ouzzif, "New MPR computation for securing OLSR routing protocol against single black hole attack," *Wireless Pers. Commun.*, vol. 115, pp. 1–20, Nov. 2020.

[14] N. C. Singh and A. Sharma, "Resilience of mobile ad hoc networks to security attacks and optimization of routing process," *Mater. Today, Proc.*, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785320373478, doi: 10.1016/j.matpr.2020.09.622.

[15] M. Faraji-Biregani and R. Fotohi, "Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles," *J. Supercomput.*, vol. 76, pp. 1–28, Nov. 2020.

[16] R.-R. Yin, N. Zhao, and Y.-H. Xu, "An selective forwarding attack considered routing protocol for scale-free network," in *Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2020, pp. 1–6.

[17] Z. Yusen, G. Jingjing, W. J. Shuang, S. Yan, Y. Li, and J. Xin, "Formal verification approach for false route in MANET," *Comput. Sci.*, vol. 39, no. 2, pp. 118–121, 2012.

[18] A. Geetha and N. Sreenath, "Cronbach alpha reliability factor based reputation mechanism for mitigating byzantine attack in MANETs," *Wireless Pers. Commun.*, vol. 96, no. 3, pp. 4525–4541, Oct. 2017, doi: 10.1007/s11277-017-4400-3.

[19] V. Desai and N. Shekokar, "Performance evaluation of OLSR protocol in MANET under the influence of routing attack," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Dec. 2014, pp. 138–143.

[20] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

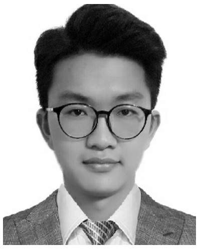
[21] C. Li and H. Dai, "Connectivity of multi-channel wireless networks under jamming attacks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 706–711.

[22] B.-T. Xu, Q. Zhu, and H. Hu, "Analysis of connectivity in ad-hoc network based on interference and fading channel," *J. China Universities Posts Telecommun.*, vol. 19, no. 5, pp. 77–82, Oct. 2012.

[23] X. Li and S. A. Zekavat, "Group-based cognitive radio network formation without common channels," *IET Netw.*, vol. 4, no. 4, pp. 235–246, Jul. 2015.

[24] Z. Gong and M. Haenggi, "Interference and outage in mobile random networks: Expectation, distribution, and correlation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 337–349, Feb. 2014.

JINBIN TU was born in Jingdezhen, Jiangxi, China, in 1996. He received the M.E. degree from the School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China, in 2019. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Southeast University, Nanjing. His research interests include distributed systems and computer networking.



DAHAI TIAN was born in Jinchang, Gansu, China, in 1997. He received the B.S. degree from the School of Software, Southeast University, Nanjing, China, in 2018. He is currently pursuing the M.S. degree with the School of Computer Science and Engineering, Southeast University. His research interests include distributed systems and computer networking.

YUN WANG (Member, IEEE) received the B.S. degree in computer software from Nanjing University, China, in 1989, and the M.E. and Ph.D. degrees in computer networking from Southeast University, China, in 2004 and 2007, respectively. She was a Postdoctoral Researcher with INRIA/IRISA, France. She joined Southeast University, in 1997, where she is currently a Full Professor with the School of Computer Science and Engineering. From 1999 to 2002, she was a Senior Researcher with the University of Texas at Dallas, USA. She was PI for more than 20 research projects supported by national and international grants. She has published more than 120 peer-reviewed journal and conference papers, including *TOC*, *JPDC*, InfoCom, ICDCS, and IPDPS. Her research interests include distributed systems, fault tolerance, and computer networking. She is the Executive Member of the Council of Jiangsu Computer Society, China. She received three Science and Technology Awards from Ministry of Education, China.