J Supercomput (2017) 73:5173–5196
DOI 10.1007/s11227-017-2075-x

DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system

Shahram Jamali[1] · **Reza Fotohi**[2]

Published online: 24 May 2017

Abstract Mobile ad hoc networks (MANETs) are mobile networks, which are automatically outspread on a geographically limited region, without requiring any preexisting infrastructure. Mostly, nodes are both self-governed and self-organized without requiring a central monitoring. Because of their distributed characteristic, MANETs are vulnerable to a particular routing misbehavior, called wormhole attack. In wormhole attack, one attacker node tunnels packet from its position to the other attacker nodes. Such wormhole attack results in a fake route with fewer hop count. If source node selects this fictitious route, attacker nodes have the options of delivering the packets or dropping them. For this reason, this paper proposes an improvement over AODV routing protocol to design a wormhole-immune routing protocol. The proposed protocol called defending against wormhole attack (DAWA) employs fuzzy logic system and artificial immune system to defend against wormhole attacks. DAWA is evaluated through extensive simulations in the NS-2 environment. The results show that DAWA outperforms other existing solutions in terms of false negative ratio, false positive ratio, detection ratio, packet delivery ratio, packets loss ratio and packets drop ratio.

Keywords Mobile ad hoc networks · Wormhole attacks · Artificial immune system · Fuzzy logic · DAWA

✉ Shahram Jamali
Jamali@uma.ac.ir

✉ Reza Fotohi
Fotohi@ieee.org; fotohi.reza@gmail.com

[1] Computer Engineering Department, University of Mohaghegh Ardabili, Ardabil, Iran

[2] Department of Computer Engineering Germi Branch, Islamic Azad University, Germi, Iran

1 Introduction

With the quick growth in wireless network, ad hoc networks have appeared in multiple forms. These networks act in the license-free frequency band and do not require any investment in infrastructure, making them yummy for military and selected commercial applications. Nevertheless, there are many unsolved questions in ad hoc networks. The open medium characteristics of MANETs such as changing topology, approximately no central monitoring, cooperative algorithms and no clear defense approach had made MANETs to be very delicate to various attacks. Furthermore, the use of wireless links in a MANETs generates the feasibility of link attacks from passive eavesdropping to active impersonation, message distribution and message falsification [1–6]. The information security principles could be easily compromised with eavesdropping that might give a malicious access to secret information. Other security principles of availability, integrity and authentication could be rejected by an active attack, which would be able to delete data, inject erroneous messages and impersonate a node [2]. One of the most dangerous attacks in MANETs is the wormhole attack. In wormhole attack, an attacker node captures packets from one position in the MANETs and tunnels them to another attacker node at a distant point, which replays them locally. The tunnel can be established in many different methods, e.g., via an out-of-band channel, a packet encapsulation or a high-powered transmission. This makes the tunneled packet arrive either quickly or with a smaller number of hop counts compared to the packets sent over ordinary multi-hop routes. This establishes the delusion that the two ends points of the tunnel are very close to each other [7–9]. As a result, these attacker nodes are captivated in the route between the source and the destination node; therefore, they can do many types of sabotages such as packet dropping and manipulating. Figure 1 shows an example of wormhole attack. Attacker nodes w1 and w2 are connected by an out-of-band channel, which they use to tunnel network data from one end of the network to the other.

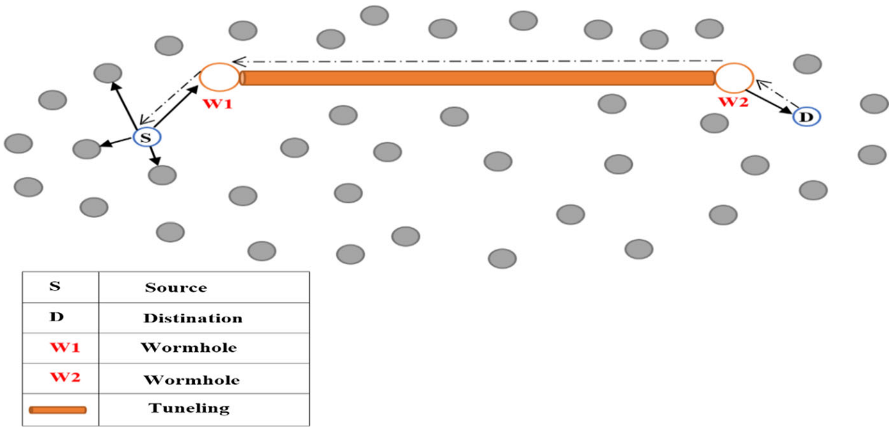


Fig. 1 MANETs with wormhole attack

This paper employs fuzzy logic and AIS technique to design an AODV-based routing protocol, which is robust against wormhole attacks. DAWA (proposed approach) is implemented in the NS-2 simulator to evaluate its performance. The rest of this paper is organized as follows. Section 2 presents the preliminaries of the research. In Sect. 3, we present the related works around the defense approach against wormhole attack, and Sect. 4 brings details of the DAWA. Performance evaluation parameters and simulation results are introduced in Sect. 5. Finally, we present our conclusions in Sect. 6.

2 Preliminaries

In this section, we provide a brief review over some basic issues such as the wormhole attack, AIS and the fuzzy logic system.

2.1 Types of wormhole attacks

In the literature [10–13], wormhole attacks are categories based on its implementation and the medium used.

2.1.1 Implementation-based classification

Based on the implementation method, wormhole attacks can be classified into the following types: encapsulation method, out-of-band channel method and high-power transmission method.

2.1.1.1 Encapsulation method In this method, there are many nodes that are preoccupied along the route (nodes along the path may or may not be aware of wormhole attack) between w1 (attacker 1) and w2 (attacker 2). The packet is encapsulated at the both nodes and travels the route in encapsulated form, hence avoiding the increase in hop count. The attacker's w1 and w2 in this scenario are not connected directly to each other, but make the other nodes feel that they are directly connected. The packets are transmitted using a virtual tunnel between w1 and w2. Once successfully launched, all paths will include a channel that will comprise of the link between the w1 attacker and w2 attacker.

2.1.1.2 Out-of-band channel method The attacker nodes are directly connected via a high-bandwidth out-of-band channel. The channel can be achieved by a wired connection or using a wireless channel which is long range and directional. Due to the requirement of extra hardware, it is difficult to launch but provides an ease because it will not need any encapsulation or decapsulation since the attackers are directly connected.

2.1.1.3 High-power transmission method This particular type of wormhole is launched from two attacker nodes that have a high-power transmission capability.

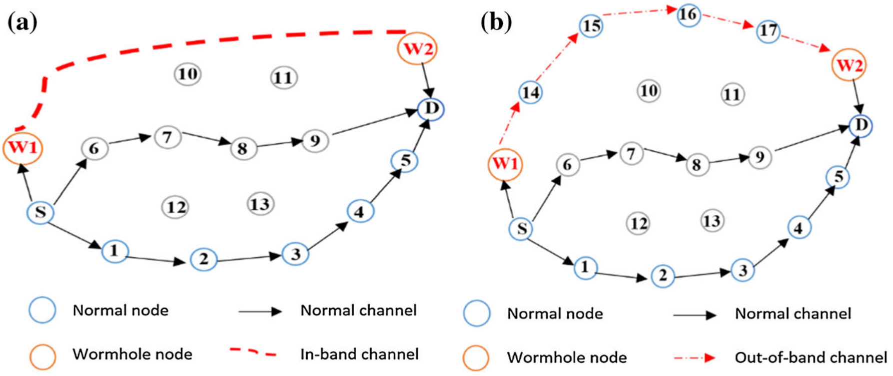


Fig. 2 Two possible implementation methods of wormhole attacks. **a** Out-of-band channel. **b** In-band channel

2.1.2 The medium used

Wormhole attacks can be also categorized as an in-band channel and out-of-band channel as shown in Fig. 2a, b, respectively.

2.1.2.1 In-band channel wormhole attack Attackers are using the same medium for creating a link between them, e.g., encapsulation, packet relay and protocol deviations. Our DAWA approach focuses on detection of this type of wormhole attacks.

2.1.2.2 Out-of-band channel wormhole attack Attackers are not using the same medium as normal network nodes, e.g., out-of-band channel and high transmission mode.

2.2 Artificial immune system

The human immune system (HIS) is a rather complicated mechanism that is capable of defending humans against a wonderful set of unessential pathogens. This mechanism is exceptionally efficient, mostly, in discriminating between self- and non-self-antigens. A non-self-antigen is anything that can initiate an immune response; examples are a bacteria or attacks. The opposite of non-self-antigens are self-antigens; self-antigens are human organism's own cells [14]. Artificial immune system (AIS) is adaptive systems inspired by theoretical immunology and observed immune systems, principles that are applied to complex problem domains. Different areas of authors attempt to build a bridge between immunology and engineering by using the approaches of mathematical and computational approaches of immunology. The basic of AIS is rooted in the early theoretical work of Farmer et al., Perelson and Varela et al. [15–17]. It was first proposed in the mid-1980s and became a subject of its own in mid-1990s. AIS aimed to find efficient abstractions of processes in the immune system [18]. By carefully reviewing the efficient natural approach, a number of computer scientists proposed artificial immune-based computer models to solve different problems ranging from attacks detection, fault analyzing to clustering. Authors played an important

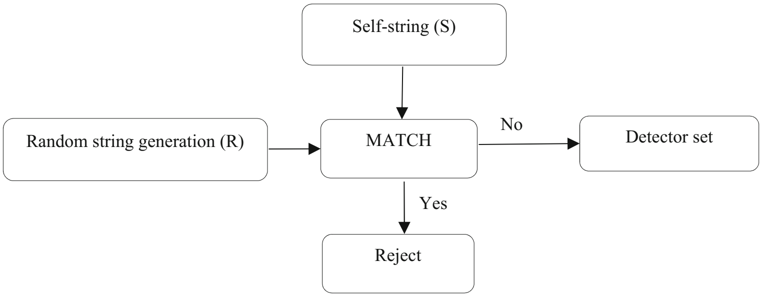


Fig. 3 T-cell (detector) generation by random generate and test process [17]

role in crossing the divide between computing and immunology. Bersini and Forrest did many basic works rooted from immunology and their works formed a solid foundation of the area of artificial immune system. With regard to $Bersini$, he was focusing on the basic theory of immune network and examining how the immune system maintained its memory and how to build a model to mimic that progress. Moreover, for Forrest, she was focusing on the application region of the artificial immune system. She proposed the idea of introducing the immune system into the computer security region by using its ability to distinguish between self and non-self [15].

2.2.1 Learning

The flow of T-cells maturation in thymus gland is used as an inspiration for learning in artificial immune system (AIS). The maturation of T-cells (detectors) in thymus gland is a result of pseudorandom flow. After a T-cell is created (Fig. 3), it undergoes censoring flow named negative selection (NS). During negative selection, T-cells that bind self are destroyed. Remaining T-cells are introduced into the body. The recognition of non-self is then done by simply comparing T-cells that survived negative selection with a suspected non-self. This process is depicted in Fig. 4. It is possible that the self-set is incomplete, while a T-cell matures (toleration period) in the thymus gland. This leads to generating T-cells that should have been removed from the thymus and can cause an autoimmune reaction, i.e., it leads to false positives (FP).

2.3 Fuzzy logic system (FLS)

In the year 1965, fuzzy logic system (FLS) was presented by Lotfi A. Zadeh, as a form of reasoning, derived from fuzzy set theory. The fuzzy logic variables have a truth value that ranges between 0 (False) and 1 (True) [19]. These truth values can be used to specify how the brakes should control. Linguistic variables are the input and output variables of the system that is separated into a set of linguistic terms. For example, if

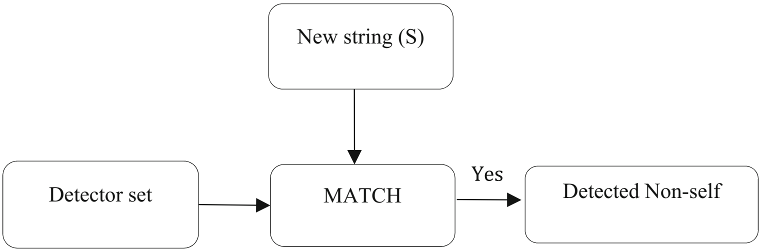


Fig. 4 Recognizing non-self is done by matching T-cells (detectors) with non-self-antigens (new strings) [17]

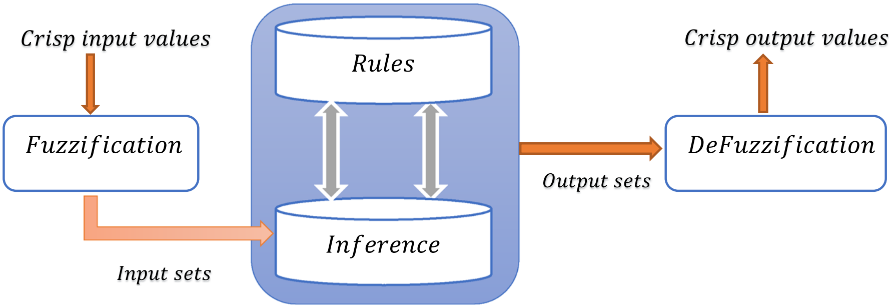


Fig. 5 Fuzzy logic system

milk filthiness is a fuzzy variable, then linguistic variables such as clean, almost clean, dirty and normal. Fuzzy logic system is shown in Fig. 5.

3 Related works

Defense against wormhole attacks has received considerable attentions in the literature. Teotia et al. [20] proposed a novel wormhole detection approach for MANETs that includes the COTA flooding in the direction of the destination node. When a source node S wants to send packets to a destination node D, it first finds the so-called expected zone and request zone in order to discover the route to the destination node. All the neighboring nodes that fall in the request zone receive the RREQ from the source or any intermediate node. Then, the RREQ is forwarded to all the neighbors. This process is continued until the RREQ packet achieves the destination node. Once the route is discovered, the S node sends the data on the discovered route.

Lu et al. [21] proposed the method that first attempt toward creating a graph theoretical approach, called Worm Planar, that just utilizes localized connectivity information and is capable of capturing the global require symptoms of wormholes directly in the wireless networks. Worm Planar acts position-free network planarization approach to done connectivity-based wormhole detection. This design makes a successful attempt to detect wormholes by capturing the global symptoms of wormholes directly in the wireless networks. Worm Planar leverages the network planarization approach and works in a distributed method with solely relying on the network connectivity information.

Amish et al. [22] proposed a wormhole detection approach to detect the wormhole attacks. However, their scheme does not rely on any special hardware. All they have done is calculated the round trip time (RTT) of every route to calculate threshold RTT. When the source node (S) broadcasts an RREQ packet note time $t1$ and when the corresponding RREP packet is received by the source, again note the received time of the packet. If multiple RREP packets received, which means there is more than one route available to the destination node (D), then note the corresponding times T_{2-i} of each RREP packet. By using the above two values, one can calculate the round trip time T_{3-i} of the established route or routes [23]. Take RTT of each route T_{3-i} and divide it by respective hop count. Calculate the average RTT of all the routes with the help of this value say T_{s-i} . The value obtained is threshold $\mathrm{RTT}_{\mathrm{tth}}$. After comparing the threshold value with each RTT T_{s-i} , if the total RTT T_{s-i} is fewer than threshold $\mathrm{RTT}_{\mathrm{tth}}$ and hop count of that particular ith route is equal to two, then wormhole link is existing in that route else no wormhole link present in that route. Since wormhole link spotted in that route, sender detects first neighbor node m1 as wormhole node and sends false RREQ packet via that route i and neighbor m1. At the destination end, receiver receives false RREQ packet from its neighbor's m2 and detects neighbor m2 as wormhole node. Routing inputs for m1 and m2 are deleted from the source node and broadcast to other nodes. Thus, wormhole-affected link is shut off and is no more used. So from the next time when a source node needs a route to that destination node, first it checks in the routing table in the route established phase for a route and it will come to know that the route is having wormhole link and it will not take that route; instead, it will take another route from the routing list of the source node which is free from wormhole link if available. Benefit of using AOMDV protocol in our proposed approach is that it has less overhead and end-to-end delay.

In [24] proposed an approach for defending against wormhole attack in MANETs environment using NS-2 simulator with AODV routing protocol. It is based on the Hash based Compression Function (HCF) algorithm, which is really using any hash function to calculate a value of the hash field for RREQ packet.

DAWN mechanism [25] proposed a local information-based scheme to detect wormhole attacks that use network coding system. DAWN is a distributed detection algorithm against wormhole node in wireless network, by tracking the change in the flow directions of the innovative packets affected by wormhole nodes. The approach rigorously proves that DAWN guarantees a good lower bound of successful detection rate (DR). They find that the robustness belongs on the node density in the wireless networks, and prove a necessary condition to get collision resistance. DAWN does not rely on any position information, special hardware. It is only based on the local information that can be achieved from regular wireless network coding protocols and thus does not introduce any overhead by extra test messages.

A hash-based compression function (HCF), intrusion detection solution against the wormhole and black hole attack in MANET is proposed in reference [26] by Patidar et al. However, their scheme preoccupies the use of a counter for specifying correct AODV routing behavior and individual nodes monitor the routing behavior of their neighbors for detecting run-time violation of the specifications. Moreover, one additional field, count in the RREP message, is proposed to enable the monitoring. Another important modification is that RREP packets are broadcasted as opposed to unicast to the source in normal AODV.

Tan et al. [27] has proposed temporal packet leashes and geographic packet leashes to prevent wormhole attack in MANETs. In temporal packet method, accurate clock synchronization (ACS) is used to limit the propagation time of packets. In geographic leashes method, loose clock synchronization (LCS) and position information are used to limit the migration distance of packets. However, the clock synchronization (CS) and position information (PI) must be obtained via extra hardware (e.g., GPS or other positioning systems) [28–30]. In addition, both theirs are required to add authentication information to each packet, which takes up large amounts of storage.

An AODV-based wormhole attack detection solution (Delphi) in MANET is proposed in Reference [31] by Chiu et al. In these schemes applied a multi-path approach and recorded the delay and hop counts in transmitting RREQ and RREP (actually named DREQ and DREP in Delphi method) through the paths. In this method, the average time taken by each hop count can be calculated. In the case of a path subjected to wormhole attacks, the delay would be obviously longer than a normal path with the same hop count (i.e., the wormhole nodes may have a heavy load, and therefore, packet processing is slow). Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

Because multi-path routing is vulnerable against wormhole attacks, a scheme called statistical analysis of multi-path (SAM) [32] has been proposed to detect malicious nodes. Due to tunneling by wormhole nodes, the number of hops of the path with wormhole nodes appears to be smaller than normal paths. Thus, the routing path with the wormhole nodes is more attractive to routing discovery of the sources. Through statistics calculation of the relative frequency of each routing path, the path that has the biggest relative frequency is identified as the path with the wormhole nodes. However, the drawback is that, in non-multi-path routing protocol, e.g., AODV, this proposal cannot work.

Su et al. [33] proposed a secure-based routing protocol (S-AODV) on the AODV routing protocol wormhole defending routing protocol. Based on the characteristic that wormhole nodes can easily grab the route from the source node to destination node, S-AODV enables the neighbors of the attacker nodes to discover that the wormhole nodes have abnormal path attractions. S-AODV does not require any hardware. It considers link-disjoint multi-paths during path discovery and provides greater path selections to avoid attacker's nodes, but eventually uses only one route to sending data. Then, the attacker nodes would be gradually isolated by their normal neighboring nodes and finally be quarantined by the whole network. However, some nodes may be misjudged to be wormhole nodes because they are located at the key positions of connectivity within the MANETs.

Su et al. [34] proposed a method to detect wormhole attacks. This method is a modification of the [35] routing protocol and can only defend against in-band channels of wormhole attacks. Their method calculates the average time in transmitting RREQ through normal nodes so that a normal node can distinguish particularly long duration in transmitting a RREQ when malicious nodes executing in-band wormhole attacks.

4 Proposed approach

In this section, we design a wormhole-immune routing protocol by jointly employing the fuzzy logic and the artificial immune system.

4.1 Phase 1: Fuzzy approach to select high-performance routes

Before considering the security, we take into account the performance problem and follow a fuzzy logic approach to select some high-performance routes from among all possible routes between the source and the destination. For this purpose, we use three parameters i.e., residue energy (RE), distance between the source node and the destination node (D) and hop count (HC) to differentiate high-performance routes from others. As shown in Fig. 5, the three major processes of fuzzy inference system are the fuzzification, the fuzzy inference and the defuzzification [29,30].

4.1.1 Step 1: Inputs fuzzification

As mentioned above, the three inputs to be fuzzified are the distance, residue energy and hop count. We use terms of 'Low,' 'Medium' and 'High' to fuzzify the residue energy, hop count and distance. Output of our fuzzy system is a set of fuzzy variables, called 'fuzzy route priority.' These variables give the fitness of any route in terms of performance. To increase the precision of our design, we consider 9 levels for our 'fuzzy route priority' variables which are Very Low (LL), Low Medium (LM), Low High (LH), Medium Low (ML), Medium (MM), Medium High (MH), High Low (HL), High Medium (HM) and Very High (HH). The membership functions (hop count, residue energy and distance) are shown in Figs. 6, 7 and 8, and fuzzy route priority is as shown in Fig. 9. The linguistic set always the interval between zero and one.

Fig. 6 Fuzzy member function for hop count

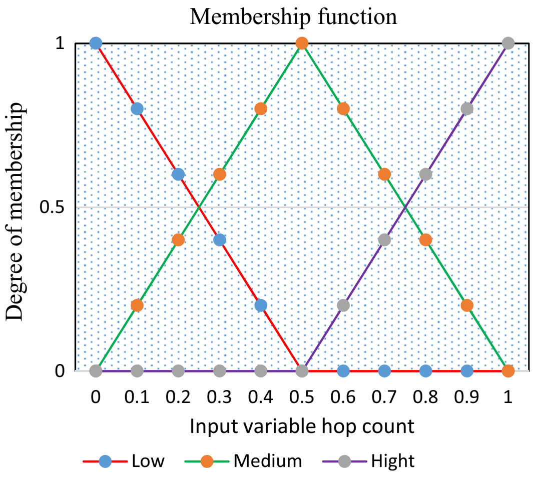


Fig. 7 Fuzzy member function for residue energy

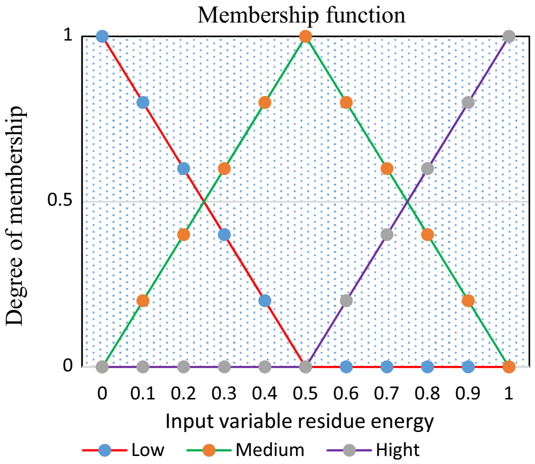
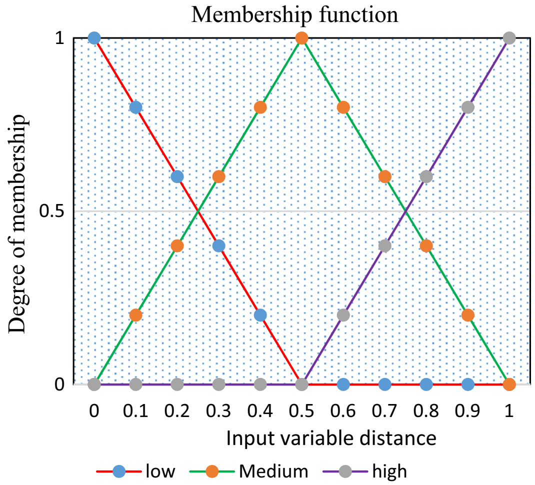


Fig. 8 Fuzzy member function for distance



4.1.2 Step 2: Inference engine and knowledge base

Knowledge is a set of rules developed by an expert system. These rules connect inputs and outputs. The fuzzy rules are in the form of IF–THEN structure. The inputs are combined using the AND–OR operators. As an example, if hop count is low, residue energy is high, and if distance is low, then the fuzzy route value is HH (Very High). The fuzzy rules are given in Table 1.

4.1.3 Step 3: Defuzzification

There are many kinds of defuzzifiers, such as centroid, maximum, center of maxima and height defuzzifiers. We use the maximum defuzzifiers in our design. That

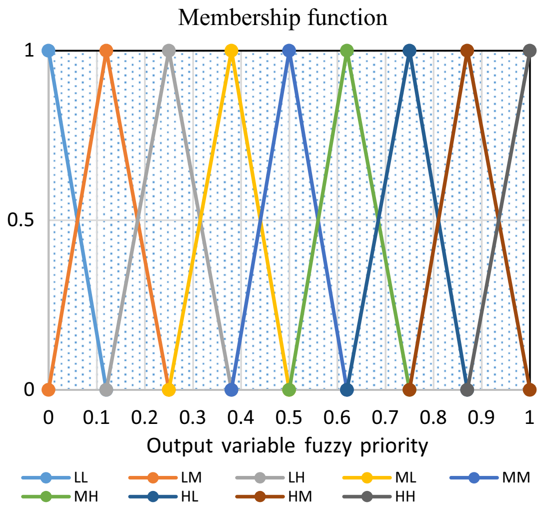


Fig. 9 Fuzzy member function for the fuzzy priority

is, the routes with the priority levels of HH, HM and HL are selected for the next step.

4.2 Phase 2: Proposed AIS-based defense scheme against wormhole attack

In order to make computer networks intelligent, we can make use of existing knowledge in the nature. One of these systems is the artificial immune system inspired by the human's immune system mechanism, which is an effective solution for convoluted predicaments in computer networks, such as in misbehavior detection or various attacks. In AODV routing protocol, once the first RREP is received by the source node, the packets will be transmitted to the destination node. This shortest route path approach disregards route's security. In this paper, we do not send immediately packets toward the destination node, upon the first RREP reception. Rather, source node considers entire received RREPs and then selects the most secure route by using the artificial immune system. The main idea of this approach comes from the human being immune system, where antibodies are trained to detect and eliminate malicious antigens. To this end, the proposed approach develops and updates a set of conditions that could detect the routes infected by wormhole attackers and avoid from selecting them. As shown in Figs. 10 and 11, the proposed scheme has two different phases. In the first phase, as discussed in Sect. 4.1, the fuzzy logic is used to select the efficient routes and in the next phase, immune routes are selected among them by using AIS approach. Table 2 represents the mapping between human body and mobile ad hoc networks, considered in this paper. As shown in Fig. 11, the source, the destination and the intermediate nodes, each one, have their own behavior in our design.

AIS has a detection phase that is based on a continuous training process. In this research, the proposed training of the detectors consists of different elements: antibody

Table 1 Fuzzy rules for fuzzification

Rules	Hop count	Distance	Residue energy	Fuzzy priority
1	Low	Low	High	HH
2	Low	Low	Medium	HM
3	Low	Low	Low	HL
4	Medium	Low	High	MH
5	Medium	Low	Medium	MM
6	Medium	Low	Low	ML
7	High	Low	High	LH
8	High	Low	Medium	LM
9	High	Low	Low	LL
10	Low	Medium	High	HM
11	Low	Medium	Medium	HM
12	Low	Medium	Low	HL
13	Medium	Medium	High	MH
14	Medium	Medium	Medium	MM
15	Medium	Medium	Low	ML
16	High	Medium	High	LH
17	High	Medium	Medium	LM
18	High	Medium	Low	LL
19	Low	High	High	MH
20	Low	High	Medium	MM
21	Low	High	Low	ML
22	Medium	High	High	MH
23	Medium	High	Medium	MM
24	Medium	High	Low	ML
25	High	High	High	LH
26	High	High	Medium	LM
27	High	High	Low	LL

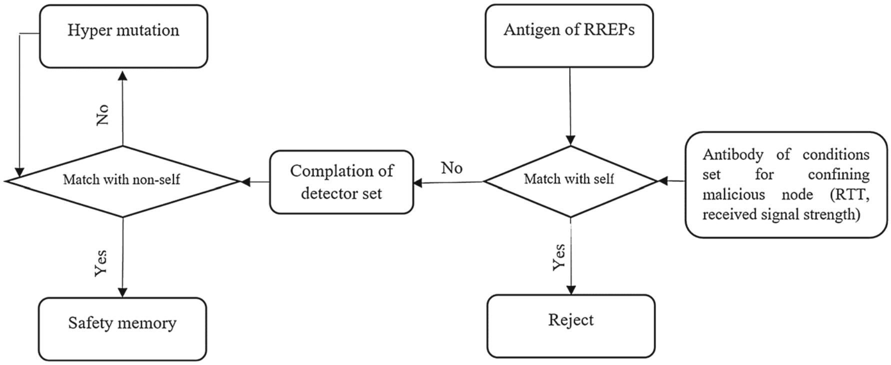

Hyper mutation
Antigen of RREPs
No
Match with non-self
Complation of detector set
No
Match with self
Antibody of conditions set for confining malicious node (RTT, received signal strength)
Yes
Yes
Safety memory
Reject

Fig. 10 Flowchart training of the detectors

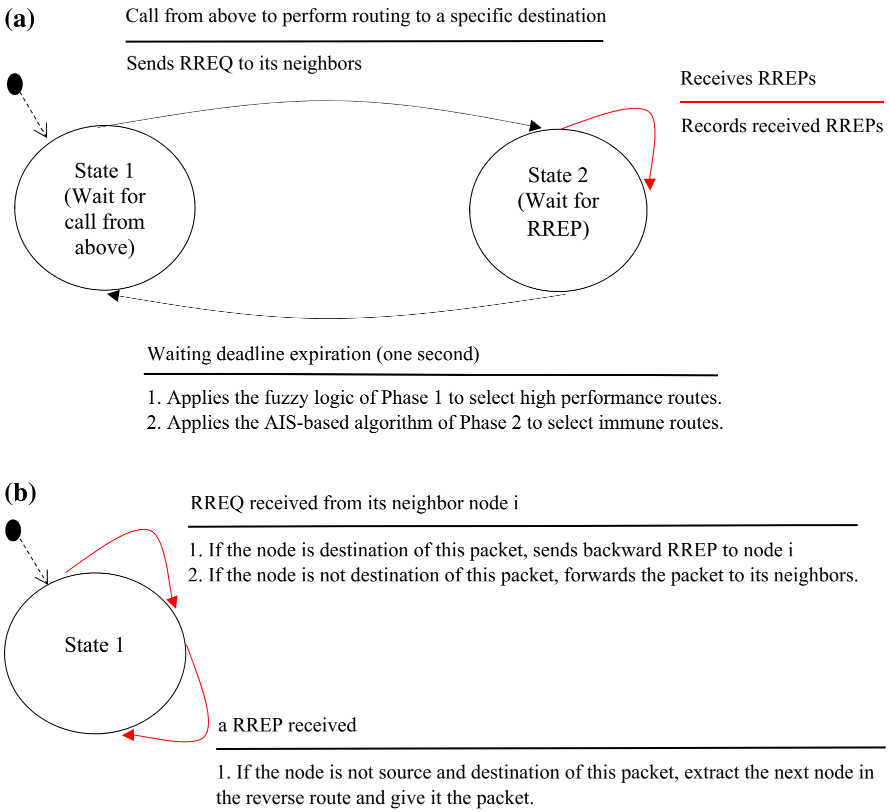

(a)
Call from above to perform routing to a specific destination
Sends RREQ to its neighbors
Receives RREPs
Records received RREPs
State 1 (Wait for call from above)
State 2 (Wait for RREP)
Waiting deadline expiration (one second)
1. Applies the fuzzy logic of Phase 1 to select high performance routes.
2. Applies the AIS-based algorithm of Phase 2 to select immune routes.
(b)
RREQ received from its neighbor node i
1. If the node is destination of this packet, sends backward RREP to node i
2. If the node is not destination of this packet, forwards the packet to its neighbors.
State 1
a RREP received
1. If the node is not source and destination of this packet, extract the next node in the reverse route and give it the packet.

Fig. 11 DAWA description by the state diagram approach. **a** The state diagram of the source node. **b** The state diagram of the intermediate and destination node

(conditions set for confining malicious node), antigen (all candidate's routes) and reject, match with self, match with non-self, completion of detector set, safety memory and hypermutation. Each of these elements will be explained in the following steps. The proposed approach has two steps: initialization and AIS-based learning.

4.2.1 Step 1: Initialization

In this step, each route that is introduced by a received RREP would be examined in terms of security. The variable that is used to detect malicious node is $P_{\mathrm{wh}}(r)$, which is called the route infection probability. The initial value of $P_{\mathrm{wh}}(r)$ is 0. To dynamically update of $P_{\mathrm{wh}}(r)$, a test packet will be sent over the route and the destination node should send a confirmation packet. Obviously, if a route has a malicious node, the test packet would not reach to the destination, and therefore, confirmation packet would not be received. In this case, the probability of being a malicious node in the route will be increased by 50 and otherwise will be decreased by 20. The test packet will be sent three times to increase accuracy of the initialization step. If $P_{\mathrm{wh}}(r)$ value of a

Table 2 Mapping between AIS and MANETs

Human body	MANETs
Self-cells	Well-behaving nodes
Non-self-cells	Misbehaving nodes
Antigen	All routes between source to destination
Antibody	Conditions set for limiting wormhole attacks (RTT, signal strength)
Chemical binding of antibodies to antigens	Matching function, between detectors and antigens, defined in detail in Fig. 4
Colonization	Reproduction of antibodies with the most antigens adaptation
Affinity	Received signal strength and RTT
Mutation	Comparison between RREPs and selection of that route which has the first RREP

route is larger than 50, the route is labeled as infected and if its value is lower than 50 the route's will be sent to Phase 2.

4.2.2 Step 2: AIS-based detection

As mentioned, the wormhole attack shows hop count much lower than actual amount; so, in the case of having smaller hop count by a route, the probability of infection of this route would be increased. Therefore, the desirable route is a route, which based on Eq. (1) maximizes F_r indicator.

Definition 1 In practice, RSS is defined as a voltage measured by a receiver's circuit. Often, RSS is equivalently reported as a measured power.

$$F_r\ (\mathrm{RTT},\ \mathrm{RSS}) = \left(\frac{\text{Max RTT}}{\text{RTT Route } i}\right) + \left(\frac{\text{Received signal strength node } i}{\text{Max received signal strength}}\right) \tag{1}$$

Integrating step 1 and step 2, an indicator of the immune route is as Eq. (2):

$$\text{Immune Route} = (1 - P_{\mathrm{wh}}\,(r)) \times\ F_r\ (\mathrm{RTT},\ \mathrm{RSS}) \tag{2}$$

Algorithm (1) shows the training procedure of the detectors according to which antibodies are trained in such a way they can recognize the self-antigens and defend against non-self-antigen (wormhole attack).

Algorithm (1): Training of the Detectors

```
Initialization:
Set counter $n_a$ as the number of self $ALCs$ to train;
Create a set of self $ALCs$ as $C$;
Determine the training of self-element as $D_t$;
Procedure Training of Detectors
    While size of $C$ not equal to $n_a$ do
        Randomly generate an $ALC$, $X_i$;
        Matched = false;
        For each self-set $Z_p$ € $D_t$ do
            If affinity between $X_i$ and $Z_p$ is higher than affinity threshold $r$ then
            Matched = true;
            Break;
            End if
        End for
        If doesn't match then
            Add $X_i$ to set $C$;
        End if
    End while
End Procedure
```

Affinity As definition in AIS, antibodies (Ab), which have a greater degree for attaching to an antigen (Ag), will be selected as a superior *antibody* in comparison with other antibodies. In the DAWA, those routes are selected that have low round trip time and high received signal strength. Hence, the affinity is calculated by using Eq. (3):

$$\text{Affinity} = \sum\nolimits_{i=1}^{L} \left|\text{Ab}_i - \text{Ag}_i\right| \qquad \text{where L is antibody and antigen length} \tag{3}$$

Details about first and second features of antibody in the matching step First feature, RTT between source and destination; it calculates and justifies RTT for the entire received RREPs from the source to the destination node.

Definition 2 RTT is defined as the time between the moment in which a 'HELLO' packet is transmitted to neighbors and the moment in which the answer to respective 'HELLO' message is received. RTT_{avg} is computed as follows:

$$\text{RTT}_{\text{avg}}\ (i) = \left(\text{RTT}_{\text{avg}}\ (i-1) \times a\right) + \ ((1-a) \times \text{RTT}_i) \tag{4}$$

Once source node receives each 'HELLO' answer, it updates average round trip time or RTT_{avg}. The initial value for variable a has been set to 0.875.

As the final step, we find those routes that their $P_{\text{wh}}(r)$ are lower than 50, but they are immune, yet. Algorithm 2 is used for this purpose.

Algorithm 2: For selecting immune route

```
1: Initialization:
2: Let $P_{wh}(r)$ as the probability candidate route;
3: Let $R$ denote the number of candidate route;
4: Let $F_r$ denote the $fitness\ route$;
5: Let $IR$ denote the $immune\ route$;
6: Procedure Selecting $immune\ route$
7:         For r = 1 to R do
8:             If $P_{wh}(r) > 0.5$ Then
9:                 Push out $route_r$;
10:        Else
11:                $Fr\ (RTT.RSS) = \left(\frac{Max\ RTT}{RTT\ Route\ i}\right) + \left(\frac{received\ signal\ strength\ node\ i}{Max\ received\ signal\ strength}\right)$
12:                Select the route with maximum $IR = (1 - Pwh(r)) * Fr\ (RTT.RSS)$
13:            End if
14:        End for
15: End Procedure
```

5 Performance evaluation

In this part, we evaluate the performance of the proposed approach (DAWA) in the problem of prevention wormhole attack.

5.1 Performance metrics

We conduct extensive simulations to evaluate the effectiveness and performance of our DAWA approach and compare it with COTA [20] and Worm Planar approaches [12]. We evaluate the drop packets rate (DPR), packet lost rate (PLR), packet delivery rate (PDR), false positive rate (FPR), false negative rate (FNR) and detection rate (DR).

5.1.1 Drop packet rate

As mentioned above, when the malicious node recives a packet, doesn't forward the packet to the next hop. It drops the packet and send an Ack to the sender node. Thus, we can define DPR as shown in Eq. (5).

$$\mathrm{DPR} = \left(\frac{\sum_{j=1}^{n} \text{Number of dropped packets}}{\sum_{j=1}^{n} \text{Number of dropped packets} + \text{sent packets}}\right) \times 100 \tag{5}$$

5.1.2 Packet loss rate

Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The lower value of the packet loss means the better performance of the protocol. The PLR is calculated using Eq. (6) as follows:

$$\mathrm{PLR} = \left(\frac{\sum_{j=1}^{n} \text{Number of sent packets}}{\sum_{j=1}^{n} \text{Number of received packets}} \right) \times 100 \tag{6}$$

5.1.3 Packet delivery rate

Packet delivery rate is the ratio of the number of data packets delivered to the destinations to the number of data packets generated by the sources. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes. Thus, we can define PDR as shown in Eq. (7).

$$\mathrm{PDR} = \left(\frac{\sum_{j=1}^{n} \text{Number of received packets}}{\sum_{j=1}^{n} \text{Number of sent packets}} \right) \times 100 \tag{7}$$

5.1.4 False positive rate

False positive rate is defined as the ratio of a number of well-behaving nodes mistakenly detected as misbehaving nodes to the total number of well-behaving nodes. The FPR is calculated using Eq. (8) as follows:

$$\mathrm{FPR} = \left(\frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \right) \times 100 \tag{8}$$

5.1.5 False negative rate

The false negative rate is defined as the number of good nodes that were considered malicious by the trust system. The FNR is calculated by Eq. (9).

$$\mathrm{FNR} = \left(\frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{All}} \right) \times 100 \quad \text{where } \mathrm{All} = \mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN} \tag{9}$$

5.1.6 Detection rate

Detection rate is defined as the ratio of a number of detected misbehaving nodes to the total number of actual misbehaving nodes. On the other hand, the detection rate is defined as the probability that all wormholes nodes are successfully identified. Thus, we can define DR as shown in Eq. (10).

$$\mathrm{DR} = \left(\frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \right) \times 100. \tag{10}$$

5.2 Simulation setup and comparing algorithms

A simulation is a fundamental tool in the development of routing protocols because of the difficulty in deploying and debugging them in real networks. The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems. Network simulator version 2, widely known as NS-2 [6,36], is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. In general, NS-2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. To visualize the result, it is possible to use a network animator (NAM) in the NS-2 environment. In this section, we evaluate the performance of our proposed approach with simulation tool NS-2 and describe the simulation results. The proposed DAWA was compared with COTA and Worm Planar. All parameters and settings of DAWA, COTA and Worm Planar are considered equally.

5.3 Simulation results

We have implemented DAWA approached in the NS-2 on Fedora 10. The simulation parameters and AIS parameters are given in Tables 3 and 4.

Table 3 Parameters used for simulation

Parameters	Value
Simulator	NS-2 (version 2.34)
Channel type	Wireless channel
Radio propagation model	Propagation/two-ray ground
Antenna type	Omni antenna
Interface queue type	Drop Tail/PriQueue
Application layer protocol	Constant bit rate (CBR)
Transport layer protocol	User datagram protocol (UDP)
Simulation time	1000 s
Number of nodes	50
Topographical area	$700 \times 700\,\text{m}^2$
Transmission range	250 m
Mobility	Random waypoint
Routing protocol	AODV
MAC layer	IEEE 802.11
Max. node movement speed	20 m/s
Pause times	150, 200,..., 600 s
Packet size	512 bytes

Table 4 AIS parameters

Parameters	Value
Antigen collection time	10 s
Antigen toward min	70 s
Delay buffer size max	1200
Storing time	11 s
Antigen present time	250 s
Max number of antigens	1200
Max number naive	1000
Max naive time	500 s

Table 5 Comparison of packet delivery rate of DAWA, COTA and Worm Planar (misbehaving node ratio = 50% and time = 1000 s)

Time (s)	Packet delivery rate		
	DAWA	COTA	Worm planar
100	62.63435	53.81547	48.98964
200	65.12872	54.33804	49.98054
300	68.09147	56.30719	51.54003
400	72.81003	57.12004	53.77603
500	76.45001	59.12664	54.90912
600	79.34761	61.09023	56.12095
700	81.55881	62.27630	57.11093
800	82.80002	64.65002	58.44001
900	86.12039	65.19034	59.32091
1000	89.88092	67.32007	61.34023

Table 6 Comparison of packet loss rate of DAWA, COTA and Worm Planar (misbehaving node ratio = 50% and time = 1000 s)

Time (s)	Packet loss rate		
	DAWA	COTA	Worm planar
100	35.63435	44.81547	51.98964
200	33.12872	42.33804	50.98054
300	30.09147	41.30719	48.54003
400	25.81003	41.12004	45.77603
500	23.45001	40.12664	42.90912
600	19.34761	37.09023	41.12095
700	17.55881	35.27630	42.11093
800	16.80002	34.65002	39.44001
900	12.12039	33.19034	37.32091
1000	9.88092	30.32007	38.34023

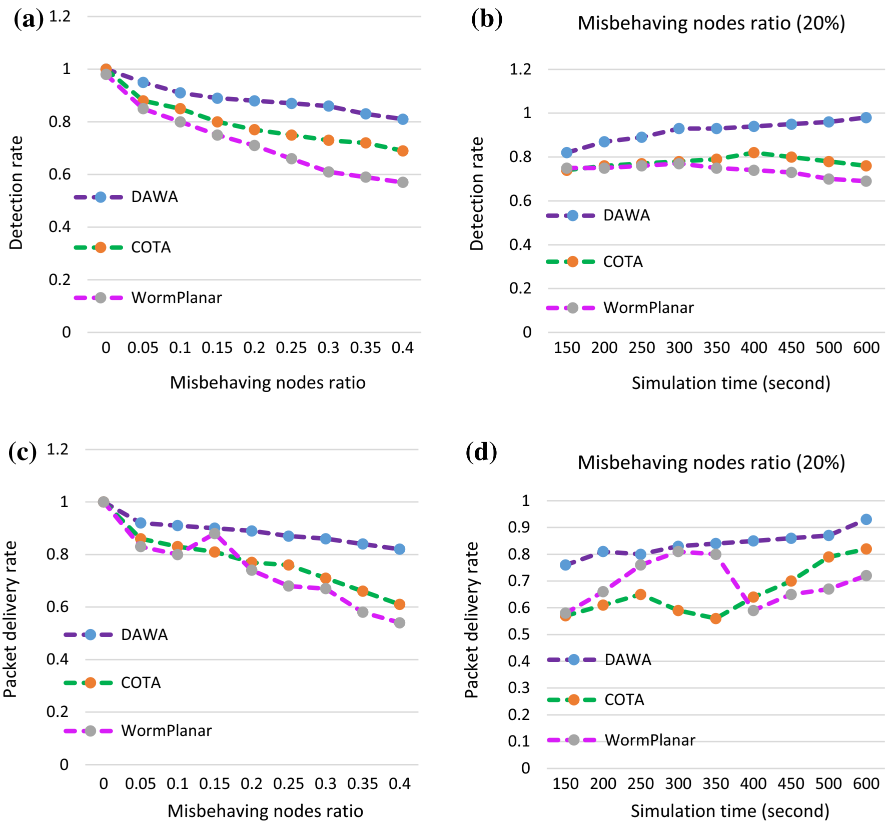


Fig. 12 Comparing DAWA performance with COTA and Worm Planar. **a** Detection rate versus misbehaving nodes ratio. **b** Detection rate versus simulation times. **c** Packet delivery rate versus misbehaving nodes ratio. **d** Packet delivery rate versus simulation times

Tables 5 and 6 compare the performance of DAWA with that of COTA and Worm Planar in terms of PDR and PLR as shown in the following tables.

Figure 12 compares the performance of DAWA with that of COTA and Warm Planar for detection of the wormhole attacks. As shown in the figure, DAWA increases the detection rate by more than 15 and 25% and increases the packet delivery rate by more than 22.5 and 22% those of COTA and Worm Planar, respectively.

Figure 13 compares the performance of DAWA with that of COTA and Worm Planar for detection of the routing attacks. As shown in the figure, DAWA decreases the false positive rate by more than 11.95 and 16.4% and decreases the false negative rate by more than 11.35 and 13.35% those of COTA and Warm Planar, respectively.

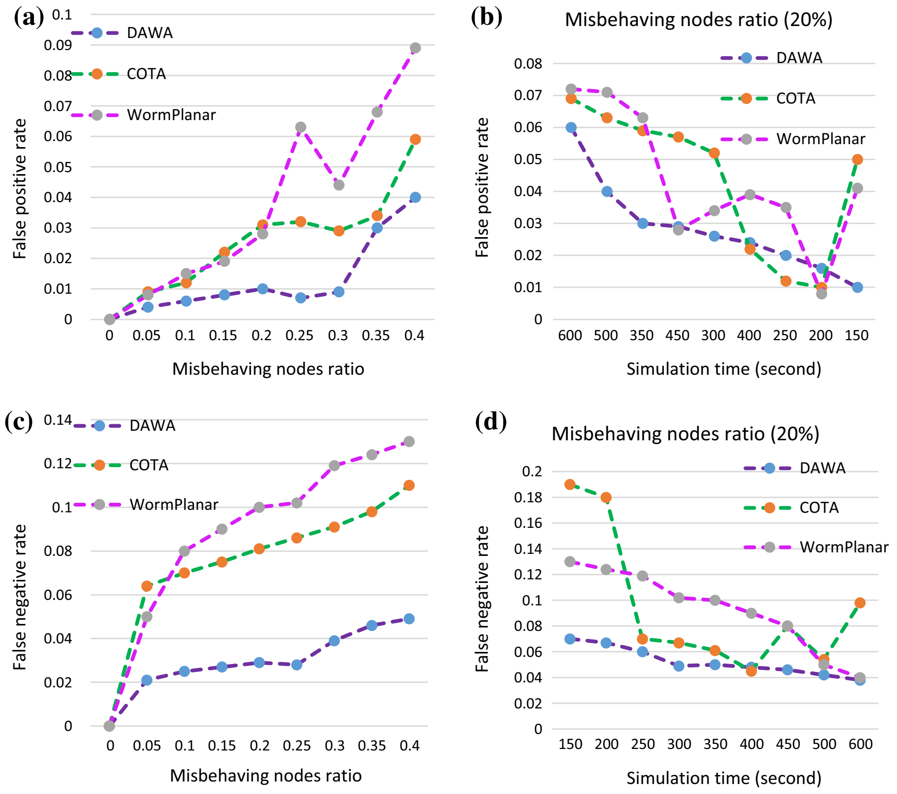


Fig. 13 Comparing DAWA performance with COTA and Worm Planar. **a** False positive rate versus misbehaving nodes ratio. **b** False positive rate versus simulation times. **c** False negative rate versus misbehaving nodes ratio. **d** False negative rate versus simulation times

Figure 14 compares the performance of DAWA with that of COTA and Worm Planar for detection of the routing attacks. As shown in the figure, DAWA decreases the packet loss rate by more than 8.45 and 17.05% and decreases the drop packets rate by more than 22.6 and 27.15% those of COTA and Warm Planar, respectively.

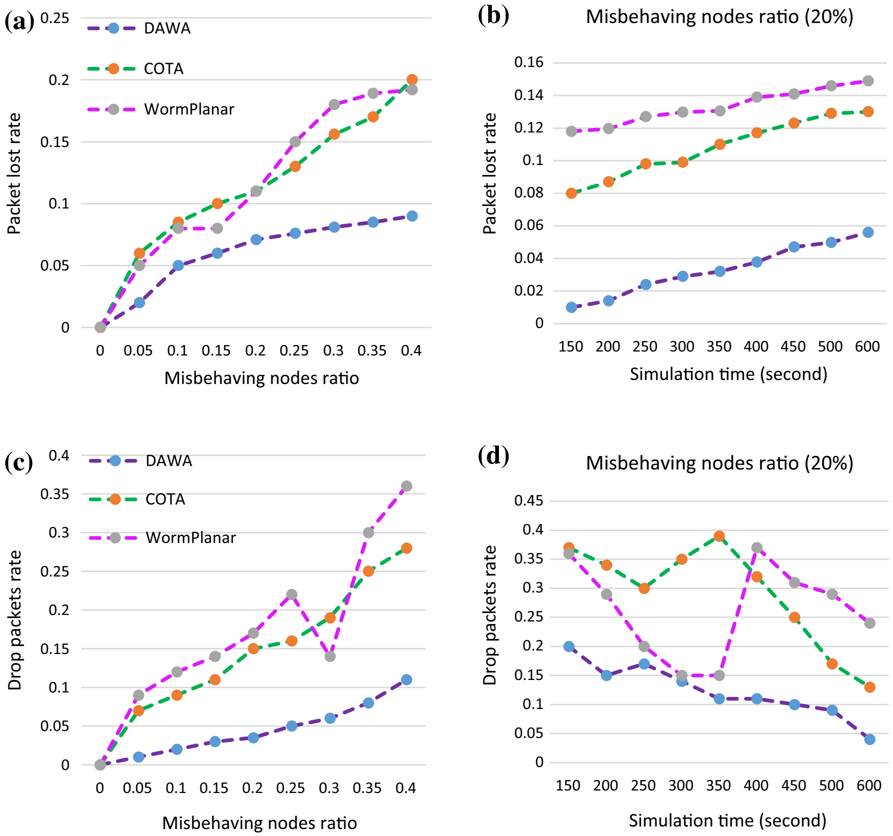


Fig. 14 Comparing DAWA performance with COTA and Worm Planar. **a** Packet lost rate versus misbehaving nodes ratio. **b** Packet lost rate versus simulation times. **c** Drop packets rate versus misbehaving nodes ratio. **d** Drop packets rate versus simulation times

6 Conclusion

In this paper, we proposed an approach for detecting wormhole nodes in MANETs based on the fuzzy logic and the artificial immune system. First, the fuzzy logic system was used to consider parameters such as node's residue energy, path's hop count and path's distance to differentiate the stable routes from others. Then the artificial immune system was employed to develop a learning approach to detect and bypass the wormhole attackers without affecting the overall performance of the MANETs. We compared the efficiency of our defensive scheme, i.e., DAWA with COTA and Worm Planar algorithms. Simulation results showed that, in average, the overall performance of DAWA is around 20% better than COTA and Worm Planar in terms of packet delivery ratio, wormhole node detection ratio, false positive ratio, false negative ratio and packet drop ratio. Also, the results show that DAWA can correctly detect wormhole nodes in many kinds of the network models.

Compliance with ethical standards

Conflict of interest Shahram Jamali and Reza Fotohi declare that they have no conflict of interest.

Ethical approval This paper does not contain any studies with human participants by any of the authors.

References

1. Van G, Greeven MJ (2016) Mobile telecommunication standardization in Japan, China, the United States, and Europe: a comparison of regulatory and industrial regimes. Telecommunication Systems, p 1–12. doi:10.1007/s11235-016-0214-y
2. Bricha N, Nourelfath M (2014) Extra-capacity versus protection for supply networks under attack. Reliab Eng Syst Saf 131:185–196
3. Fotohi R, Ebazadeh Y, Geshlag MS (2016) A new approach for improvement security against DoS attacks in vehicular ad-hoc network. Int J Adv Comput Sci Appl 7:10–16
4. Fotohi R, Jamali SHA (2014) comprehensive study on defence against wormhole attack methods in mobile Ad hoc Networks. Int J Comput Sci Netw Solut 2:37–56
5. Adewole KS, Anuar NB, Kamsin A, Varathan KD, Razak SA (2016) Malicious accounts: dark of the social networks. J Netw Comput Appl 79:41–67
6. Rana AI, Jennings B (2016) Semantic aware processing of user defined inference rules to manage home networks. J Netw Comput Appl 79:68–87
7. Vatn J, Aven T (2010) An approach to maintenance optimization where safety issues are important. Reliab Eng Syst Saf 95(1):58–63
8. Fotohi R, Heydari R, Jamali SH (2016) A Hybrid routing method for mobile ad-hoc networks. J Adv Comput Res 7(3):93–103
9. Fotohi Reza et al (2013b) An Improvement over AODV routing protocol by limiting visited hop count. Int J Inf Technol Comput Sci (IJITCS) 5(9):87
10. Jamali SH, Fotohi R (2016) Defending against wormhole attack in MANET using an artificial immune system. New Rev Inf Netw 21(2):1–22. doi:10.1080/13614576.2016.1247741
11. Jamali SH, Shaker V (2014) Defense against SYN flooding attacks: a particle swarm optimization approach. Comput Electr Eng 40(6):2013–2025
12. Maulik R, Chaki N, A comprehensive review on wormhole attacks in MANET. In: 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), IEEE, 1010, pp 233–238
13. Fotohi R, Jamali SH, Sarkohaki F (2013a) Performance evaluation of AODV, LHC-AODV, OLSR, UL-OLSR, DSDV routing protocols. Int J Inf Technol Comput Sci (IJITCS) 5(10):21
14. Drozda M, Schaust S, Szczerbicka H (2007) AIS for misbehavior detection in wireless sensor networks: performance and design principles. In: 2007 IEEE Congress on Evolutionary Computation, IEEE, pp 3719–3726
15. Farmer JD, Packard NH, Perelson AS (1986) The immune system, adaptation, and machine learning. Phys D: Nonlinear Phenom 22(1):187–204
16. Perelson AS (1989) Immune network theory. Immunol Rev 110(1):5–36. doi:10.1111/j.1600-065X.1989.tb00025.x
17. Varela F, Coutinho A, Dupire B, Nelson N (1988) Cognitive networks: immune, neural and otherwise. In: Perelson AS (ed) Theoretical immunology, part two. SFI studies in the sciences of complexity, vol 3. Addison-Wesley, MA, pp 377–401
18. Shen J, Wang J, Ai H (2012) An improved artificial immune system-based network intrusion detection by using rough set. Commun Netw 4(1):41–47. doi:10.4236/cn.2012.41006
19. Zadeh LA (1965) Fuzzy sets. Inf Control 8(3):338–353
20. Teotia V, Dhurandher SK, Woungang I, Obaidat MS (2015) Wormhole prevention using COTA mechanism in position based environment over MANETs. In: 2015 IEEE International Conference on Communications (ICC), IEEE, pp 7036–7040

21. Lu X, Dong D, Liao X (2013) WormPlanar: Topological planarization based wormhole detection in wireless networks. In: 2013 42nd International Conference on Parallel Processing, IEEE, pp 498–503
22. Amish P, Vaghela VB (2016) Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. 7th International Conference on Communication, Elsevier, pp 700–707
23. Raju VK, Kumar KV (2012) A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks. In: 2012 International Conference on Computing Sciences (ICCS), IEEE, pp 271–275
24. Patel A, Patel N, Patel R (2015). Defending against wormhole attack in MANET. In: 2015 Fifth International Conference on Communication Systems and Network Technologies (CSNT), IEEE, pp 674–678
25. Ji S, Chen T, Zhong S, Kak S (2014) Dawn: defending against wormhole attacks in wireless network coding systems. In: 2014 IEEE Conference on Computer Communications, IEEE INFOCOM, IEEE, pp 664–672
26. Patidar K, Dubey V (2014) Modification in routing mechanism of AODV for defending black hole and wormhole attacks. In: 2014 Conference on IT in Business, Industry and Government (CSIBIG), IEEE, pp 1–6
27. Tan Z (2012) An efficient identity-based tripartite authenticated key agreement protocol. Electron Commer Res 12(4):505–518. doi:10.1007/s10660-012-9103-y
28. Petrova K, Wang B (2011) Location-based services deployment, and demand: a roadmap model. Electron Commer Res 11(1):5–29. doi:10.1007/s10660-010-9068-7
29. Aloudat A, Michael K (2011) Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. Electron Commer Res 11(1):31–74. doi:10.1007/s10660-010-9070-0
30. Zhou T (2013) An empirical examination of user adoption of location-based services. Electron Commer Res 13(1):25–39. doi:10.1007/s10660-013-9106-3
31. Chiu HS, Lui KS (2006) Delphi: wormhole detection mechanism for ad hoc wireless networks. In: 2006 1st International Symposium on Wireless Pervasive Computing, IEEE, p 6
32. Qian L, Song N, Li X (2005) Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path. In: IEEE Wireless Communications and Networking Conference, IEEE, vol 4. pp 2106–2111
33. Su MY (2010) WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Comput Secur 29(2):208–224. doi:10.1016/j.cose.2009.09.005
34. Su X, Boppana RV (2007) On mitigating in-band wormhole attacks in mobile ad hoc networks. In: 2007 IEEE International Conference on Communications, IEEE, pp 1136–1141
35. Hu YC, Johnson DB, Perrig A (2003) SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc Netw 1(1):175–192. doi:10.1016/S1570-8705(03)00019-2
36. Maulik R, Chaki N, A comprehensive review on wormhole attacks in MANET. In: 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), IEEE, 1010, pp 233–238