Wireless Personal Communications (2023) 130:1161–1190
https://doi.org/10.1007/s11277-023-10325-3

AFA: Anti-Flooding Attack Scheme Against Flooding Attack in MANET

Vivek Mankotia[1] · Ramesh Kumar Sunkaria[1] · Shashi Gurung[2]

Accepted: 25 February 2023 / Published online: 9 March 2023

Abstract
Security in a mobile ad-hoc network is an essential requirement that helps in preventing attacks from the malicious node. A flooding attack is a type of denial of service attack that consumes the network bandwidth due to flooding of the fake packets by the flooder node. The different forms of flooding attacks are route request flooding attacks and data flooding attacks. In a route request flooding attack, the flooder node exhausts the network resources with a high number of fake request packets in the network whereas in a data flooding attack; the flooder node sends the fake data packets to the destination. In this paper, we have proposed an Anti-Flooding Attack (AFA) scheme that can detect both types of flooding attacks. NS-2.35 simulator is used to validate the efficiency of the proposed scheme under the effect of different mobility speeds and the number of nodes scenario. The simulation results show that the proposed AFA scheme performs better as compared with an existing scheme on the various performance metrics.

Keyword Flooding attack in MANET · Anti-flooding attack · Security in MANET · Dual security

1 Introduction

The mobile ad-hoc network is an infrastructure-less network where mobile devices do communication with each other through wireless links [1–4]. In this network, each node is having a limited range that can be used for transmitting or receiving the packets. The nodes within each other's range can communicate directly and when the nodes are not within

✉ Vivek Mankotia
vivekmankotia1947@gmail.com

Ramesh Kumar Sunkaria
sunkariark@nitj.ac.in

Shashi Gurung
gurungshashi68@gmail.com

[1] Department of Electronics and Communication Engineering, National Institute of Technology, Jalandhar, India

[2] Department of Computer Science and Engineering, Government Hydro Engineering College, Bilaspur, India

the range of each other, the originating node takes the help of the other nodes which forwards the packets to the destination node. Due to characteristics like openness and frequent change in network topology, the control of MANET is difficult [5–7]. MANET is susceptible to various kinds of attacks [8] and one such prominent attack is the flooding attack in which fake packets are sent frequently into the network to consume the network's resources. The flooding attack can be a route request flooding attack or a data flooding attack. Security in MANET has become an essential requirement to ensure safe communication between the source node and the destination node. Many schemes in the available literature have been proposed to deal with route request flooding attacks mostly but these schemes fail to give protection from data flooding attacks in MANET. Therefore, In this paper, an Anti-Flooding Attack scheme is presented based on dual security mechanisms which can deal with both types of flooding attacks i.e. route request flooding attacks and data flooding attacks. The contributions made in this paper are as follows:

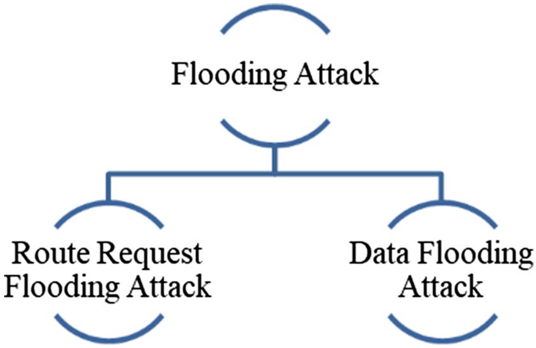
1. Proposed an Anti-Flooding Attack (AFA) scheme against both types of flooding attacks in MANET.
2. Evaluated the performance of the AFA scheme and compared it with AODV and F-IDS schemes.

The various further sections in this paper are structured as follows. In Sect. 2, the flooding attack and types of flooding attacks have been discussed. Section 3 has discussed various existing schemes with their limitations. In Sects. 4 and 5, the proposed AFA scheme and simulation parameters values have been discussed respectively. In Sects. 6 and 7, the performance metrics and the results obtained through the NS-2 simulator tool are discussed. Finally, Sect. 8 has provided the conclusion.

2 Flooding Attack

A flooding attack is an attack in which an attacker sends fake packets into the network to disturb the network's operation and exhaust the bandwidth [9–13]. There are generally two types of packets used in the network which are control packets and data packets. When the attacker sends fake request control packets in the whole network, it is termed as request flooding attack and when the attacker sends the fake data packets to the destination, it is termed as data flooding attack. The type of flooding attack is shown in Fig. 1.

Fig. 1 Flooding attack



3 Literature Review and Motivation

In this section, the existing techniques available in the literature are discussed along with their limitation which has been highlighted in Table 1.

3.1 Literature Review

Chouhan et al. [14] presented a scheme to remove the request flooding attack in the mobile ad-hoc network. It divided the nodes into three categories: stranger, acquaintance, and friendly. Every node maintains a table that contains information about each node in it as an acquaintance or friendly type depending on the trust level. Any node which is absent in the table is assumed as a stranger node. Each type also has a threshold which is different for each type. Friend-type nodes have the highest value and stranger types nodes have the lowest value. When any node receives the Route requests, it first checks the category of the source node and calculates the number of requests generated by the node. If it is higher than the threshold value, then the sender node is treated as a malicious request-flooding attacker and further requests from that sender node are dropped. This technique does not deal with data flooding attacks.

Roshan et al. [15] proposed a solution for a data flooding attack in which according to blacklist and priority, the packets are processed. The blacklist is maintained by the node which contains the maximum number of the received data packet for the certain source and destination node pair. This technique lacks the security mechanism for dealing with the route request flooding attack.

In [16], Hakak et al. discussed the impact of route request attacks in mobile ad-hoc networks but no security mechanisms are provided against route request flooding attacks and data flooding attacks. However, in this paper, security mechanisms against both types of flooding attacks are presented.

Surendra Kumar et al. [17] developed the model to prevent route request flooding attacks in MANET. In this technique, each node maintains three lists: black list, gray list & white list. When the node receives the request, it checks the list. If the source node is present in the blacklist table then its request is rejected. If the request packet is from that node that is listed in the graylist, then the node checks about the black alarm for the sender node, If the black alarm is already broadcasted for the sender node, then the sender request is dropped otherwise it is accepted. If the request from the sender is listed in the whitelist then the request is processed. The criterion of nodes is dependent on the number of route requests generated by the sender. If the number of generated requests is more than the maximum threshold, the node is listed in the blacklist and black alarm is transmitted in the network. If the number of generated requests is more than the minor threshold, the node is listed in the graylist and gray alarm is transmitted in the network. Apart from that, it will be listed in the whitelist. This proposed model is checked in four algorithms. In all four scenarios, it exhibits an equal threshold value but with different energy consumption. This technique does not deal with data-based flooding attacks.

Bhalodiya et al. [18] designed a model against request flooding attacks in MANET. This technique makes use of the filtering method to scrutinize the RREQ RATE LIMIT for each node. If any node sends the request packet more than RREQ RATE LIMIT, it is declared as a malicious node. The value of the RREQ RATE LIMIT is 10. The proposed technique

Table 1 Limitations of conventional techniques

S. no	References	Year	Proposed scheme	Limitation
1	[14]	2011	Trust Based Scheme	Lacks security mechanism against a data flooding attack
2	[15]	2012	Priroity Based Scheme	Lacks security mechanism against route request flooding attack
3	[16]	2014	Not proposed security mechanism against flooding attacks	No security mechanism against route request and data flooding attack
4	[17]	2015	Threshold Based Scheme	Lacks security mechanism against a data flooding attack
5	[18]	2015	Filtering Based Scheme	Lacks security mechanism against a data flooding attack
6	[19]	2016	Energy threshold Based Scheme	Lacks security mechanism against a data flooding attack
7	[20]	2016	Threshold Based Scheme	Lacks security mechanism against a data flooding attack
8	[21]	2017	Dynamic Profile Based Detection Scheme	Lacks security mechanism against a data flooding attack
9	[22]	2017	Threshold Based Scheme	Lacks security mechanism against a data flooding attack
10	[23]	2018	Flooding-Intrusion Detection System	Lacks security mechanism against a data flooding attack
11	[24]	2018	Fuzzy-based flooding attack detection System	Lacks security mechanism against a data flooding attack
12	[25]	2019	Avoiding and Isolating Flooding Attack by Enhancing AODV	Lacks security mechanism against a data flooding attack
13	[26]	2019	Threshold Based Scheme	Lacks security mechanism against a data flooding attack
14	[27]	2020	Deep Learning Based Scheme	Lacks security mechanism against route request flooding attack and not evaluated on important performance metrics
15	[28]	2021	Threshold Based Scheme	Lacks security mechanism against a data flooding attack
16	[29]	2021	Bayesian Inference Based	Lacks security mechanism against a data flooding attack
17	[30]	2021	Adaptive Neuro-Fuzzy Inference Model	Lacks security mechanism against a data flooding attack
18	[31]	2022	Median Filter Based flooding attack detection algorithm	Lacks security mechanism against a data flooding attack

exhibited an improvement in packet delivery ratio and throughput in comparison to AODV but it fails to deal with data flooding attacks.

Jatthap et al. [19] proposed a technique against the RREQs-based flooder attacker nodes depending on the energy consumed by the nodes. This model calculates the energy consumption of nodes with or without route request flooding attacks. This energy consumption by the nodes is used to calculate the maximum and minimum energy threshold. If the consumption energy of the node is less than or equal to the minimum energy threshold, that node is considered as dead node. If energy consumption of the sender node's is more than the threshold value, that node is declared as the attacker node and its address is entered into the blacklist table for the isolation and it is restricted from participating in any further communication. However, this model also does not deal with the data flooding attack.

Srinivasa Rao et al. [20] provided a new method in which the network is partitioned into clusters to remove RREQs-based flooding attacks. In this, the cluster head nodes are authorized to send the request packet. If RREQs come from a normal node, it will be dropped. In this, the network is partitioned into three phases which are the join network phase, cluster head election phase, and path cut-off phase. When any node joins the network during the join network phase, it attaches itself in nearby the cluster, and then it listed itself as a unique identifier (UID). In a subsequent operation, cluster head nodes are selected for effective communication. In the path cut-off phase, when nodes receive RREQs from other than cluster head nodes. These requests are not entertained and subsequently, these RREQs will be dropped. In this technique, the main limitation is the lack of a security mechanism against the data flooding attack.

Pandikumar et al. [21] provided a model based on the Dynamic Profile Based Detection Scheme for dealing with the requests (RREQs) based flooder node. In this model, every node keeps records of the number of requests sent and received to calculate the average RREQs and calculates the RATE LIMIT. The value of the Threshold is computed with the help of RATE-Limit. If any node sends the RREQs packets more than the calculated threshold value, then that node is considered as malicious node and isolated from the network. The limitation of this model is that it does not deal with data flooding attacks.

Vimal et al. [22] proposed a technique against route request-based flooding attacks. There are two phases in this technique which are the detection phase and the prevention phase. The value of the threshold is computed by using the total number of neighbor nodes present. In the detection phase, when any node sends RREQ packets as more than the threshold value then that particular node is treated as a malicious node. In prevention mode, the neighbor nodes are alarmed about the address of the malicious node. The new routes are modified by accordingly deleting the malicious node entry. To continue the communication process, the malicious node is replaced with a nearby node. Although this technique can deal with route request flooding attacks but it cannot deal with data flooding attacks.

In [23], Gurung et al. presented a technique to mitigate the impact of request flooding attacks in MANET. In this model, extra special Flooding-Intrusion Detection System (F-IDS) nodes have been deployed. These F-IDS nodes are positioned in such a location that the maximum network's area is covered and monitor the neighboring node's behavior. In this model, three phases are used which are: dynamic threshold computation, confirmation and resetting phase. The dynamic threshold value is computed in the first phase. In confirmation mode, the final presence of a malicious flooding node is confirmed and in the resetting phase, all the blacklisted flooding nodes are given the chance to participate in the network. If even after giving them multiple chances, the behavior of the flooding node remains a malicious, then that node is permanently blocked from the network for participation. This model also lacks a security mechanism against the data flooding attack which is a limitation.

In [24] Nithya et al. proposed a robust detection system called as Fuzzy-based Flooding Attack Detection System (FFADS) to detect request-based flooding attacks using a first-order Mamdani type fuzzy inference. The proposed method uses a network-specific parameter rather than node-specific parameters. This model also lacks a security mechanism against the data flooding attack which is the limitation.

M.A. Zant et al. [25] proposed a protocol called as Avoiding and Isolating Flooding Attack by Enhancing AODV MANET for the detection and isolation of RREQs-based flooding attacks. This proposed model has two mechanisms which are flooding avoidance and attacker isolations. Each node in the network maintains a request-counter table during the flooding avoidance algorithm which carries the information of the source of requests and the total count of requests got from the same source. When any node in the network gets the requests, it first checks the source of the request. If the source node is available in the request-counter table, it increases the value in the table for that source of the requesting node otherwise, it adds new information for the source node in the request-counter table. After this, the node will check the number of requests received by requesting the source node. If the number of requests received by the source requesting nodes is higher than the threshold value then the requesting source node will be declared as a flooding attacker node or else process the RREQs normally in the network. This proposed technique also does not deal with data flooding attacks.

Mohammadi [26] et al. proposed a model which consists of two parts namely a misbehavior detection system in the network and a flooding detection system. The hello messages are transmitted between nodes regularly so that nodes can update the information of neighboring nodes. The extra field is added in the hello message which contains the information regarding the transmitted and received request packets by nodes. If the number of route request packets is greater than the threshold, the first part will inform the network regarding the malicious activity. The duty of the second part is to find out the resources of malicious activity by using APTR criteria. If any node is declared as a malicious node, it will be added to the detention list and no data packets will be sent to the malicious node. This model also lacks a security mechanism against the data flooding attack which is a limitation.

In [27], Sbai et al. have proposed a technique for data flooding attacks but they have not evaluated the technique on various network performance metrics like packet delivery rate, throughput, overhead, etc. However, in this paper, we have evaluated the proposed technique on different metrics.

Singh et al. [28] proposed a Statistical Ad-Hoc On-Demand Distance Vector (SAODV) approach to detect request-based flooding attacks in MANET. If the number of route request packets sent by the node is more than the threshold value, then that node is declared as a malicious node. This model also lacks a security mechanism against the data flooding attack which is the limitation.

In [29], Nishanth et al. proposed a model for request-based flooding attacks based on Bayesian Inference. The two models of uncertain reasoning namely Bayesian Inference and Dempster-Shafer (D-S) evidence theory were used for detecting request flooding attacks. This model also lacks a security mechanism against the data flooding attack.

Nand et al. [30] proposed a hybrid routing protocol that prevents requests flood attacks by using ANFIS (Adaptive Neuro-Fuzzy Inference System) classifier. This model also lacks a security mechanism against the data flooding attack which is a limitation.

Luong et al. [31] proposed a Median Filter based flooding attacks detection algorithm (MFFDA) to detect the request flooding attack in MANET. The authors also proposed the Flooding Attacks Prevention and Detection Routing Protocol (FAPDRP) but this model lacks a security mechanism against the data flooding attack which is the limitation.

3.2 3.2 Research Gaps and Motivations

Many works in the available literature have provided solutions for route request flooding attacks during the route discovery phase but these solutions lack the security mechanism against the data flooding attack during the data transmission phase. There are very few solutions available for data flooding attacks but these solutions cannot deal with the route request flooding attack. To the best of our knowledge, there is no solution available that can deal with both types of flooding attacks. Therefore the limitation in existing schemes has motivated us to propose an Anti-Flooding Attack scheme that protects the MANET from both types of flooding attacks during route discovery and data transmission phases which is the novelty in the proposed approach.

4 Anti-Flooding Attack (AFA): Proposed Scheme

In this section, the working mechanism of the Anti-Flooding Attack (AFA) scheme is discussed. The AFA scheme is composed of two security mechanisms which are as follows:

1. Anti-Route Request Flooding Attack (ARRFA)
2. Anti-Data Flooding Attack (ADFA)

To deal with different types of flooding attacks in MANET, two security mechanisms are proposed. The first security mechanism deals with route request flooding attacks during the route discovery phase and the second security mechanism deals with data flooding attacks during the data transmission phase. The three types of nodes taken in this paper are mentioned below.

- Flooding nodes: These nodes are malicious nodes that do flooding attacks in the network.
- Monitoring nodes: These nodes execute an AFA scheme security mechanisms that monitor the activities of the nodes and deal with both types of flooding attacks in MANET.
- Normal nodes: These nodes execute a modified AODV protocol that broadcast an ALERT packet whenever it finds a flooder node in the network which contains the malicious node's identity information.

Following are the assumptions taken in the proposed scheme.

1. All the nodes except the monitoring nodes have the same physical characteristics in the network.
2. The source, destination, and monitoring nodes are trusted nodes.
3. The monitoring nodes are in overhearing mode and are placed in such a way to cover a maximum area as depicted in Fig. 2. They are also within range of each other.

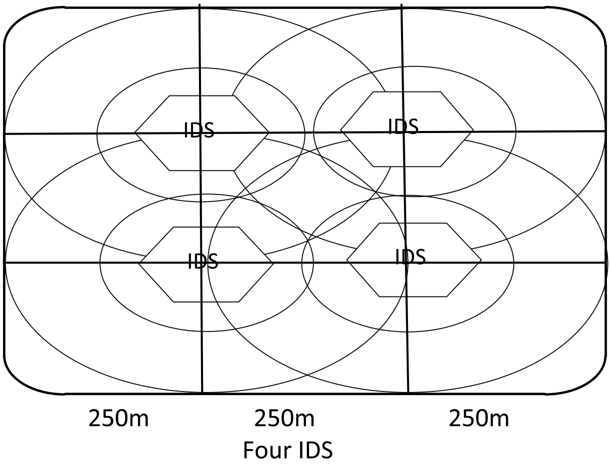


Fig. 2 Placement of monitoring nodes in the network

4.1 Anti-Route Request Flooding Attack

In the route discovery phase, the originating nodes send the request packet to the destination nodes to set up the path before the transmission of the data packets. Upon getting the request packet, the destination node sends a reply to the originating nodes and thereafter data transmission takes place. In route request flooding attacks, many fake request packets are sent frequently by the flooder node. To deal with route request flooding attacks, the monitoring nodes execute an Anti-Route Request Flooding Attack security mechanism and monitor the number of route request packets sent by the source nodes within its range as shown in Fig. 3. It maintains the count of the number of request packet for each sender node during preset timer of 10 s and calculates the average (A) and standard deviation value according to equations Eqs. 1 and 2 respectively. The value of the standard

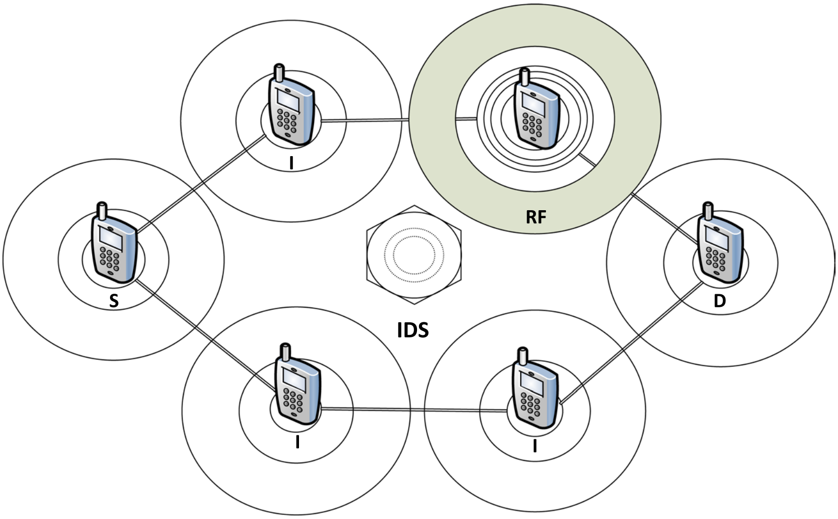


Fig. 3 IDS nodes monitoring the neighboring nodes

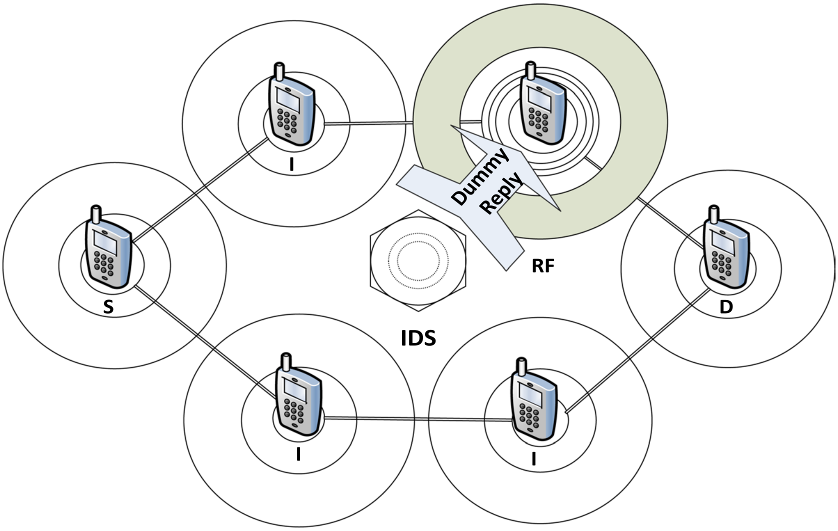


Fig. 4 IDS nodes sending Dummy reply to Request Flooder Node

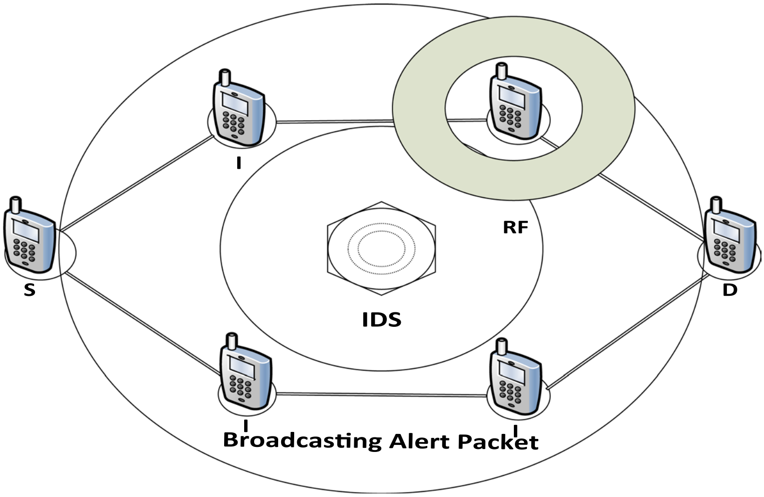


Fig. 5 Broadcasting ALERT packet to notify about Request Flooder Node

deviation will be the threshold value (*T*). If the number of route request packets sent by any node is higher than the value of the threshold, the monitoring node sends the dummy reply packet on the behalf of the destination node to that node only which is suspicious as shown in Fig. 4. If no data transmission starts from that node within the preset timer period of 1 s, the monitoring node considers that node as a malicious node and does not process any request packet from that node thereafter and in the future also. Thereafter, the identity of that malicious node is broadcasted in the network through an ALERT packet to inform other IDS nodes and normal nodes as shown in Fig. 5. The other IDS nodes and normal nodes make an entry of the malicious node identity into their blacklist table and drop subsequent request packets coming from this malicious node. If data transmission starts after sending the dummy reply packet, it means it is an honest node. The monitoring node sends the route error message to the source node and the source node rebroadcasts the route request packet to set up the path with the destination node (Fig. 6).

$$A = \sum_{i=1}^{n} \frac{x_i}{n} \tag{1}$$

$$T = \sqrt{\sum_{i=1}^{n} \frac{(x_i - A)^2}{n}} \tag{2}$$

where x_i represents number of route request packet sent by i^{th} node, n is number of source node, A is Average and T is Threshold

4.2 Anti-Data Flooding Attack

Whenever the route is established between the originating and targeting node, data transmission takes place. In a data flooding attack, the flooder node sends a high number of fake data packets during the data transmission phase to the destination node. To deal with the data flooding attack, the monitoring nodes execute an Anti-Data Flooding Attack security mechanism and monitor the number of data packets sent by the source nodes within its range as shown in Fig. 7. It maintains the count of the number of the data packet for each sender node and computes the average (A), and standard deviation value according to

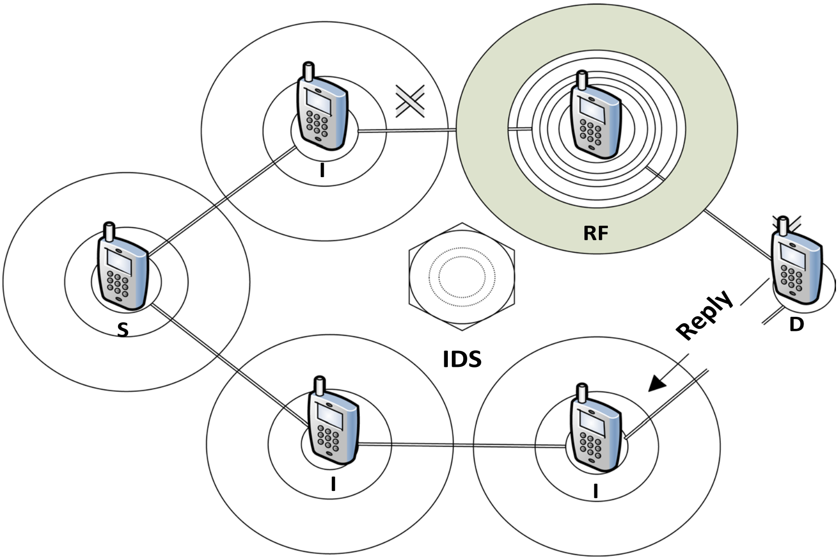


Fig. 6 Destination ignoring fake request packet and Source resending request packet. Meaning: S = Source, D = Destination, RF = Request Flooder Node, I = Intermediate

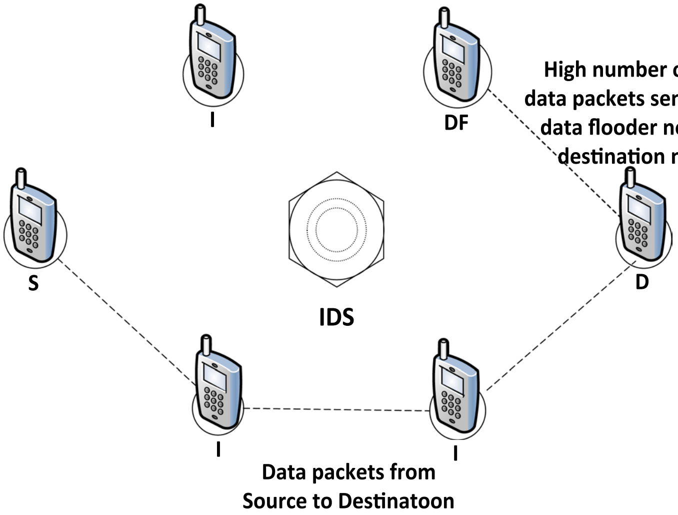

I
DF
High number of fake data packets sending by data flooder node to destination node
S
IDS
D
I
I
Data packets from Source to Destinatoon

Fig. 7 IDS nodes monitoring neighboring nodes

equations Eqs. 3 and 4 respectively. The value of the standard deviation will be the threshold value (T). If the number of fake data packets sent by any source node is higher than the value of the threshold, the monitoring node considers that node as the malicious node, and the identity of that node is notified to other neighbouring IDS and normal nodes in the network through ALERT packet as shown in Fig. 8. The other IDS nodes and normal nodes add the identity of the malicious node in their blacklist table and ignore the data packets coming from this malicious nodes in the future. The algorithm, flowchart, and pseudocode of the proposed AFA scheme are presented in Figs. 9, 10 and 11 respectively.

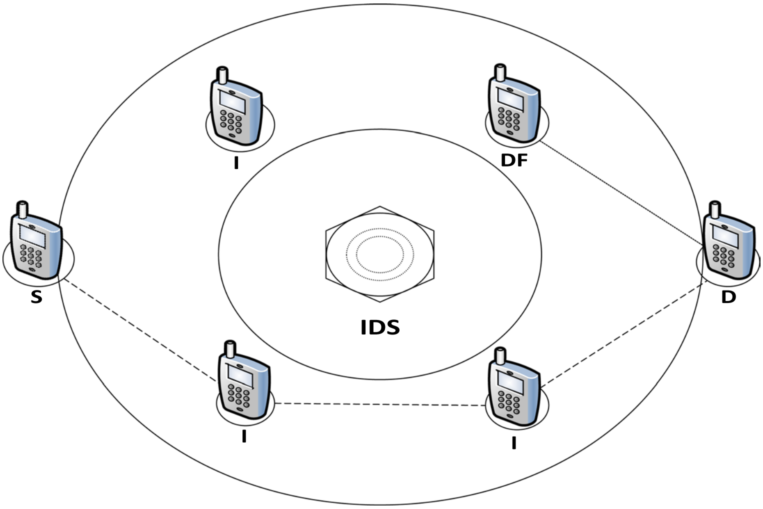
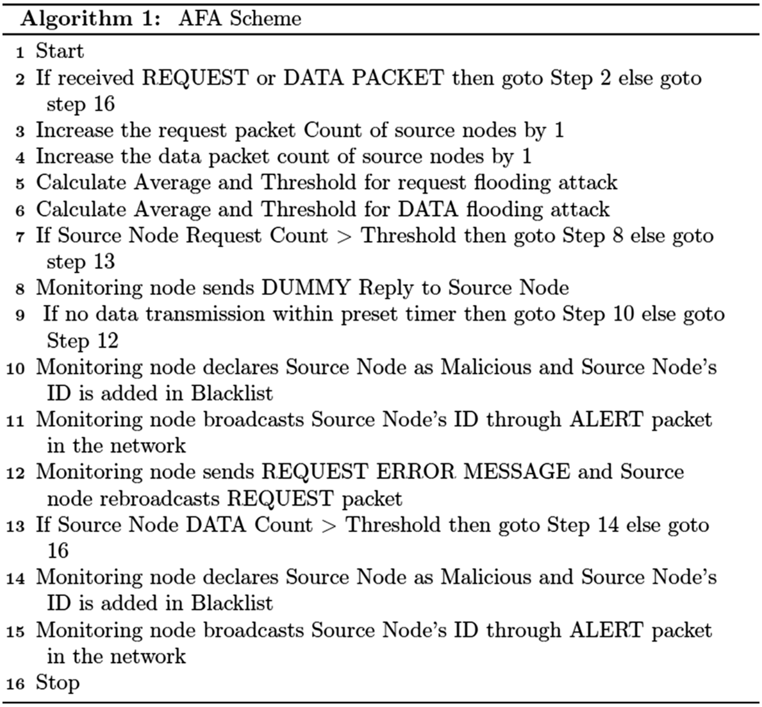


Fig. 8 Broadcasting ALERT packet to notify about Data Flooder Node. Meaning: S = Source, D = Destination, DF = Data Flooder Node, I = Intermediate



```
Algorithm 1: AFA Scheme
1  Start
2  If received REQUEST or DATA PACKET then goto Step 2 else goto
     step 16
3  Increase the request packet Count of source nodes by 1
4  Increase the data packet count of source nodes by 1
5  Calculate Average and Threshold for request flooding attack
6  Calculate Average and Threshold for DATA flooding attack
7  If Source Node Request Count > Threshold then goto Step 8 else goto
     step 13
8  Monitoring node sends DUMMY Reply to Source Node
9   If no data transmission within preset timer then goto Step 10 else goto
     Step 12
10 Monitoring node declares Source Node as Malicious and Source Node's
     ID is added in Blacklist
11 Monitoring node broadcasts Source Node's ID through ALERT packet
     in the network
12 Monitoring node sends REQUEST ERROR MESSAGE and Source
     node rebroadcasts REQUEST packet
13 If Source Node DATA Count > Threshold then goto Step 14 else goto
     16
14 Monitoring node declares Source Node as Malicious and Source Node's
     ID is added in Blacklist
15 Monitoring node broadcasts Source Node's ID through ALERT packet
     in the network
16 Stop
```

Fig. 9 Algorithm for AFA Scheme

$$A = \sum_{i=1}^{n} \frac{d_i}{n} \tag{3}$$

$$T = \sqrt{\sum_{i=1}^{n} \frac{(d_i - A)^2}{n}} \tag{4}$$

where d_i represents the number of data packets sent by ith node, n is the number of the source node, A is Average and T is the Threshold

5 Experimental Setup

To check the effectiveness of the proposed scheme, the simulator i.e. NS-2.35 simulator has been used [32]. The number of nodes taken in the network is 50 which are distributed randomly in an area of 750 m × 750 m. Out of 50 nodes, one node is taken as a flooder node in the network for launching the flooding attack as shown in Fig. 12. Two pairs for communication are randomly chosen and each pair is sending UDP–CBR packets. Two ray-ground propagation radio models and a random waypoint mobility model are used in the network. Flooding-AODV (F-AODV) protocol is used to launch the flooding attack in the network generating fake route request packets at every 0.01 second (100 packets/sec) and Data flooding-AODV (D-AODV) protocol is used to launch the data flooding attack in

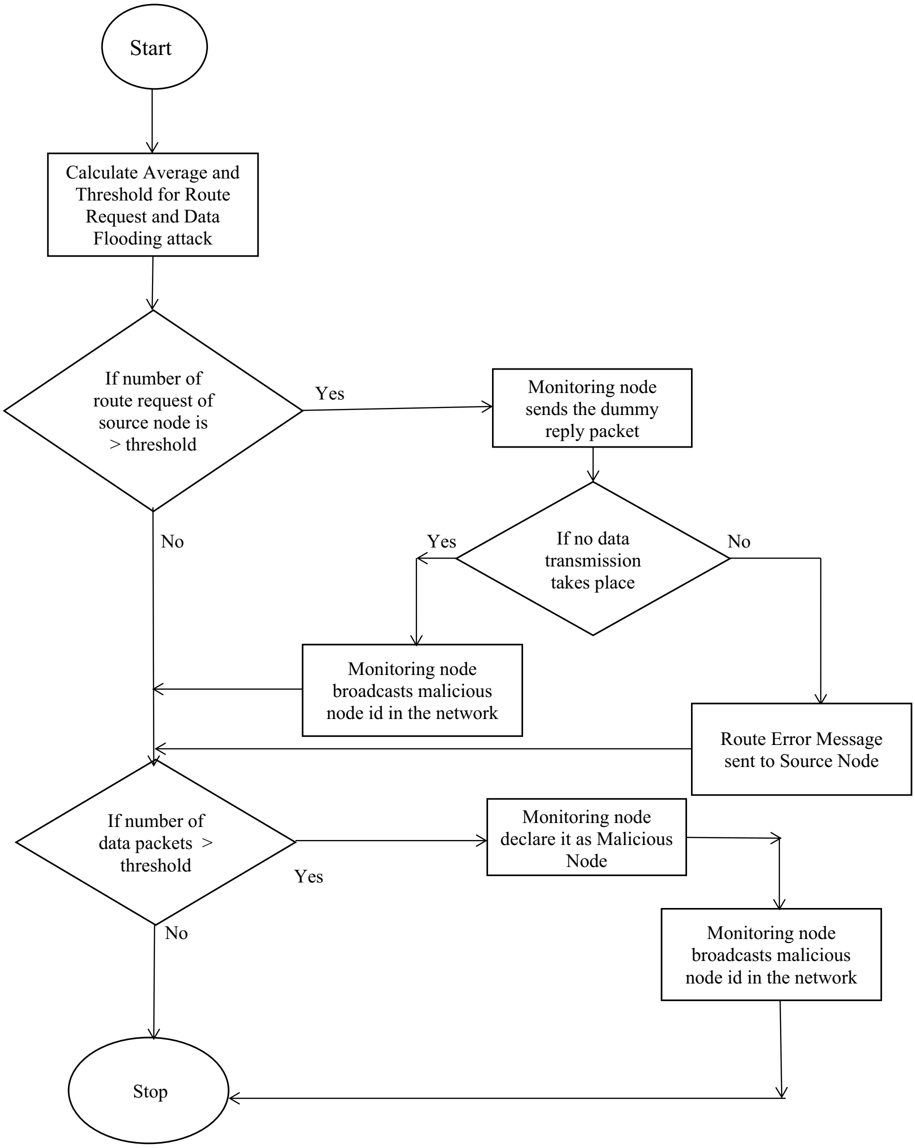
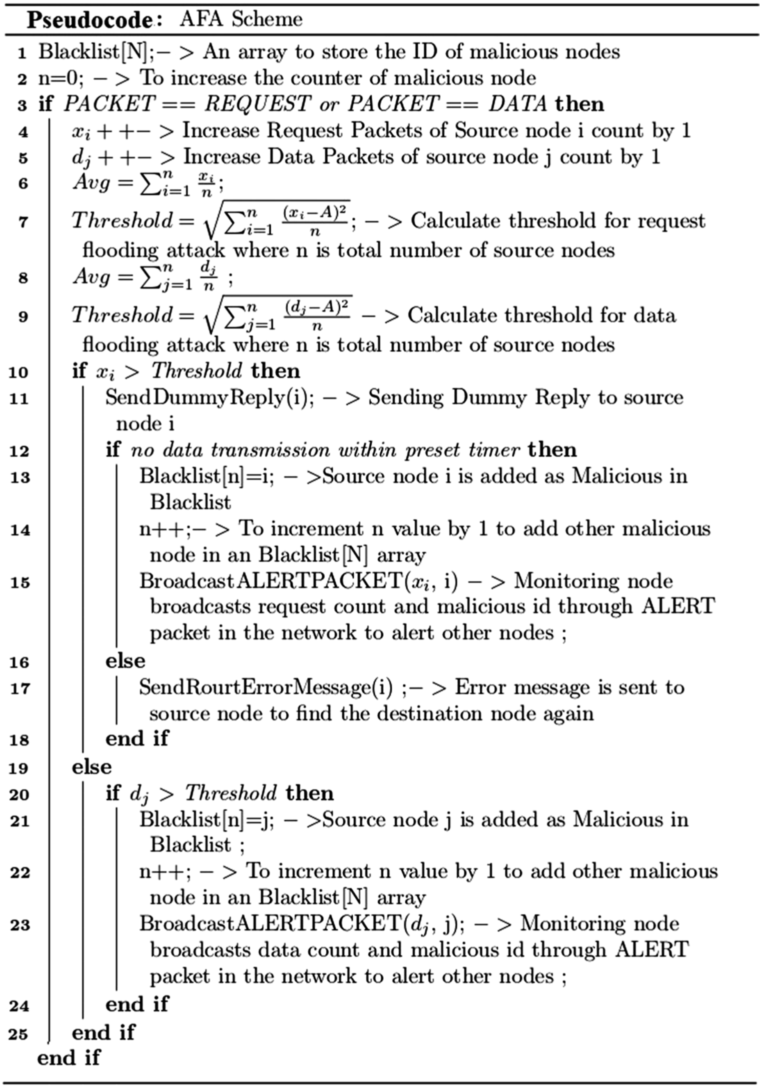

Start
Calculate Average and Threshold for Route Request and Data Flooding attack
If number of route request of source node is > threshold
Yes
Monitoring node sends the dummy reply packet
No
Yes
If no data transmission takes place
No
Monitoring node broadcasts malicious node id in the network
Route Error Message sent to Source Node
If number of data packets > threshold
Monitoring node declare it as Malicious Node
Yes
No
Monitoring node broadcasts malicious node id in the network
Stop

Fig. 10 Flowchart for Anti-Flooding Attack (AFA) scheme against flooding attack in MANET

the AODV-based network sending fake data packets. The network is first tested under route request flooding attack and then under data flooding attack at different mobility speeds i.e. from 1 m/s to 5 m/s for 100 seconds of simulation time. Four number of IDS nodes are taken in the network and positioned in such a way to cover the maximum network area. The evaluation of the performance of the proposed scheme is done on different performance metrics such as packet delivery rate, throughput, routing overhead, and normalized routing load and also compared with an existing F-IDS scheme [23]. The main parameters used in the experiment are mentioned in Table 2.



```
Pseudocode: AFA Scheme
Blacklist[N];− > An array to store the ID of malicious nodes
n=0; − > To increase the counter of malicious node
if $PACKET == REQUEST$ or $PACKET == DATA$ then
    $x_i + +$− > Increase Request Packets of Source node i count by 1
    $d_j + +$− > Increase Data Packets of source node j count by 1
    $Avg = \sum_{i=1}^{n} \frac{x_i}{n}$;
    $Threshold = \sqrt{\sum_{i=1}^{n} \frac{(x_i - A)^2}{n}}$; − > Calculate threshold for request
     flooding attack where n is total number of source nodes
    $Avg = \sum_{j=1}^{n} \frac{d_j}{n}$ ;
    $Threshold = \sqrt{\sum_{j=1}^{n} \frac{(d_j - A)^2}{n}}$ − > Calculate threshold for data
     flooding attack where n is total number of source nodes
    if $x_i > Threshold$ then
        SendDummyReply(i); − > Sending Dummy Reply to source
         node i
        if no data transmission within preset timer then
            Blacklist[n]=i; − >Source node i is added as Malicious in
             Blacklist
            n++;− > To increment n value by 1 to add other malicious
             node in an Blacklist[N] array
            BroadcastALERTPACKET($x_i$, i) − > Monitoring node
             broadcasts request count and malicious id through ALERT
             packet in the network to alert other nodes ;
        else
            SendRourtErrorMessage(i) ;− > Error message is sent to
             source node to find the destination node again
        end if
    else
        if $d_j > Threshold$ then
            Blacklist[n]=j; − >Source node j is added as Malicious in
             Blacklist ;
            n++; − > To increment n value by 1 to add other malicious
             node in an Blacklist[N] array
            BroadcastALERTPACKET($d_j$, j); − > Monitoring node
             broadcasts data count and malicious id through ALERT
             packet in the network to alert other nodes ;
        end if
    end if
end if
```

Fig. 11 Pseudocode for AFA Scheme

6 Performance Metrics

Following performance metrics are used and the meaning of notations used in the equations is provided in Table 3.

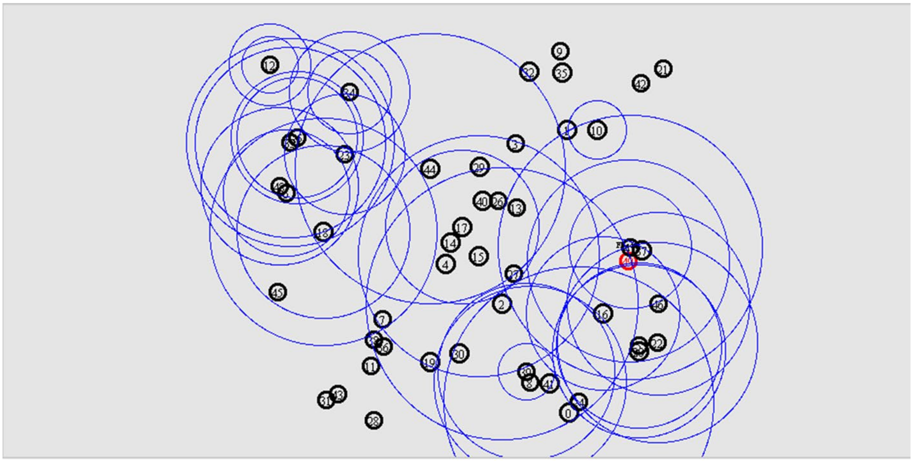


Fig. 12 Flooding attack in NS-2

Table 2 Parameters value taken in simulation

Parameter	Value
Number of nodes	50
Dimension	750×750 m^2
Number of monitoring nodes	4
Simulation time (seconds)	100 s
Mobility speeds	0,1,2,3,4 and 5
Number of nodes	10,20,30,40 and 50
Route request flooding rate	0.01 s
Traffic type	CBR
Propagation radio model	Two Ray Ground
Mobility model	Random Waypoint
Packet size	512 bytes
Number of connections	2
Number of IDS node	4
Connection	UDP
MAC layer	IEEE 802.11
Protocols/Schemes	AODV, F-IDS, AFA

6.1 Packet Delivery Rate

It is computed as total number of data packets received divided by total number of data packets sent × 100%.

$$PDR = \frac{\sum_{=1}^{n} \mathrm{DPR_K}}{\sum_{K=1}^{n} \mathrm{DPS_K}} \times 100\%$$

Table 3 Notation Meaning

Notations	Meaning
PDR	Packet delivery rate
T	Average throughput
RO	Routing overhead
NRL	Normalized routing load
$\mathrm{DPS_K}$	Number of packets sent by node K
$\mathrm{DPR_K}$	Number of packets received by node K
$\mathrm{CP_K}$	Number of control packets by node K
PS	Packet size
$\mathrm{S_P}$	Simulation STOP time
$\mathrm{S_T}$	Simulation START time

6.2 Throughput

It is computed as the total size of packets delivered to the difference of simulation stop and start timing.

$$T[kbps] = \frac{\sum_{K=1}^{n} \mathrm{DPR_K} \times \mathrm{P_S}}{\mathrm{S_P} - \mathrm{S}_T} \times \frac{8}{1000}$$

6.3 Routing Overhead

It denotes the total number of control packets sent by nodes in the network.

$$RO = \sum_{K=1}^{n} \mathrm{CP_K}$$

6.4 Normalized Routing Load

It is computed as the total number of generated control packets divided by the total data packets received in the network.

$$NRL = \frac{\sum_{K=1}^{n} \mathrm{CP_K}}{\sum_{K=1}^{n} \mathrm{DPR_K}}$$

7 Result Analysis and Discussion

In this part, the results of different protocols on various metrics under the effect of different mobility speeds and the number of nodes are discussed and values are mentioned in Tables 4, 5, 6 and 7.

7.1 Effect of Mobility Speeds

In this section, the network is tested with varying mobility speeds.

7.1.1 Packet Delivery Rate (PDR)

In the absence of a route request flooder node, the PDR in AODV is 99.72%. In the presence of a route request flooder node, the PDR is 0%. The 0% of PDR is owing to the fake route request packets sent by the flooder node which consumes the network bandwidth and destination nodes are not able to get the data packets. When the F-IDS scheme is used, the PDR is 94.75% but in the proposed scheme, the PDR is 96.75% under route request flooding attack which is better as compared with an existing scheme as shown in Fig. 13. It has been observed that in the absence of a data flooder node, the PDR in AODV is 99.72%. In the presence of a data flooder node, the PDR is 2.38%. When the F-IDS scheme is used,

Table 4 Simulation results under route request flooding attack

S. no	Metric	AODV (without attack)	F-AODV	F-IDS	AFA
1	PDR (%)	99.72	0	94.75	96.75
2	Throughput (kbps)	19.94	0	18.81	19.31
3	Routing Overhead	182	118,458	42,257	16,350
4	Normalized Routing Load	0.77	∞	189.22	71.71

Table 5 Simulation results under Data Flooding Attack

S. no	Metric	AODV (without attack)	D-AODV	F-IDS	AFA
1	PDR (%)	99.72	2.38	2.38	98.5
2	Throughput (kbps)	19.94	0.48	0.48	19.75
3	Routing Overhead	182	372	372	202
4	Normalized Routing Load	0.77	74.5	74.5	1.15

Table 6 Simulation results under Route Request Flooding Attack

S. no	Metric	AODV (without attack)	F-AODV	F-IDS	AFA
1	PDR (%)	71.55	18.71	66.38	69.60
2	Throughput (kbps)	14.32	3.75	13.29	13.93
3	Routing Overhead	243	71,957	22,306	4183
4	Normalized Routing Load	1.16	2573.31	112.47	21.89

Table 7 Simulation results under Data Flooding Attack

S.no	Metric	AODV (without attack)	D-AODV	F-IDS	AFA
1	PDR (%)	71.55	1.46	1.46	70.05
2	Throughput (kbps)	14.32	0.29	0.29	14.02
3	Routing Overhead	243	754	754	289
4	Normalized Routing Load	1.16	431.58	431.58	1.43

the PDR is 2.38%. This low PDR in FIDS scheme is due to the lack of security mechanism against data flooding attacks but in the proposed scheme, the PDR is 98.5% under data flooding attacks which is better as compared with an existing scheme as shown in Fig. 14. From Figs. 13 and 14, it can be seen that with the increasing in the mobility speeds, the PDR is decreasing. Due to mobility, the route is broken between the communicating nodes and some packets are dropped.

7.1.2 Throughput

It has been observed that in the absence of a data flooder node, the throughput in AODV is 19.94 kbps. In the presence of a route request flooder node, throughput is 0 kbps. This is because of the fake route request packets of the flooder node which keep other nodes busy in processing the fake packets. When the F-IDS scheme is used, the throughput is 18.81 kbps but in the proposed AFA scheme, the throughput is 19.31 kbps under route request flooding attack which is better as compared with an existing scheme as shown in Fig. 15. In the absence of a data flooder node, the throughput in AODV is 19.94 kbps. In the presence of a data flooder node, throughput is 0.48 kbps. When the F-IDS scheme is used, the throughput is 0.48 kbps. This is because of the lack of a security mechanism against the data flooding attack in F-IDS scheme but in the proposed AFA scheme, the

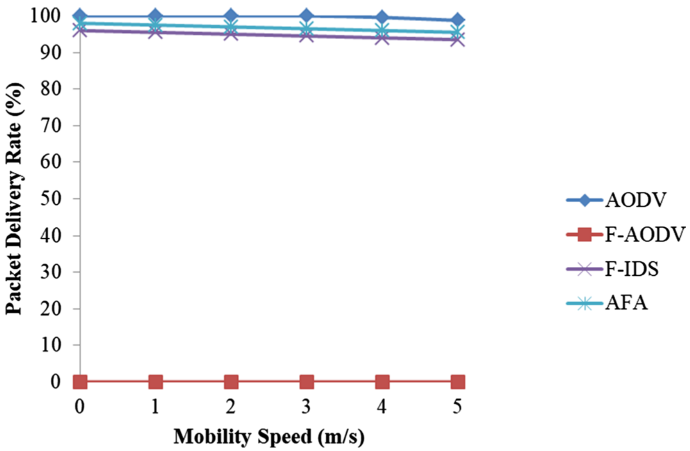


Fig. 13 Packet Delivery Rate vs Mobility under Route Request Flooding Attack

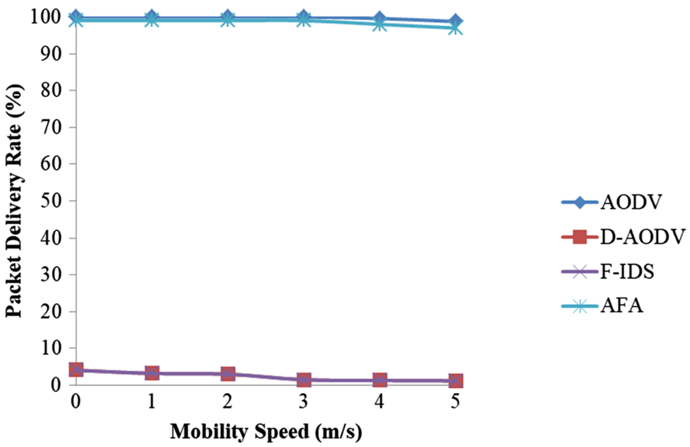


Fig. 14 Packet Delivery Rate vs Mobility under Data-Flooding Attack

throughputs are 19.75 kbps under a data flooding attack which is better compared with an existing scheme as shown in Fig. 16. From Figs. 15 and 16, it can be seen that with the increasing in the mobility speeds, the throughput is decreasing due to the reason mentioned above in case of PDR.

7.1.3 Routing Overhead

When is no route request flooder node in MANET, the routing overhead in AODV is 182 but when there is a route request flooder node in the network, the routing overhead in AODV is 118458 due to broadcasting of fake request packet in the network. The routing overhead in the F-IDS scheme under the route request flooding attack is 42257. When the

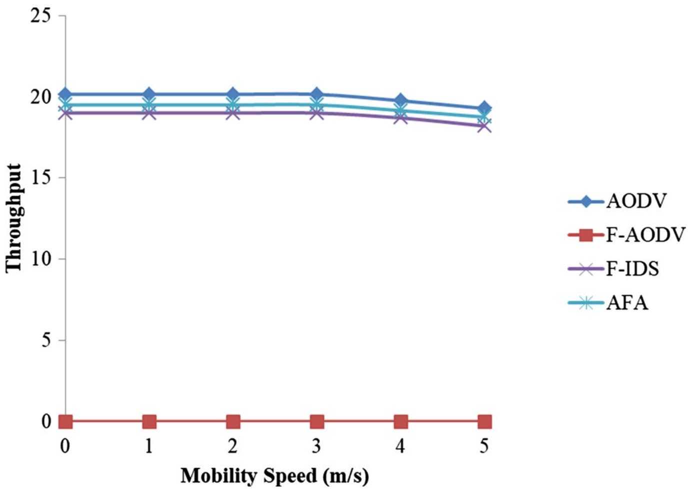


Fig. 15 Throughput vs Mobility under Route Request Flooding Attack

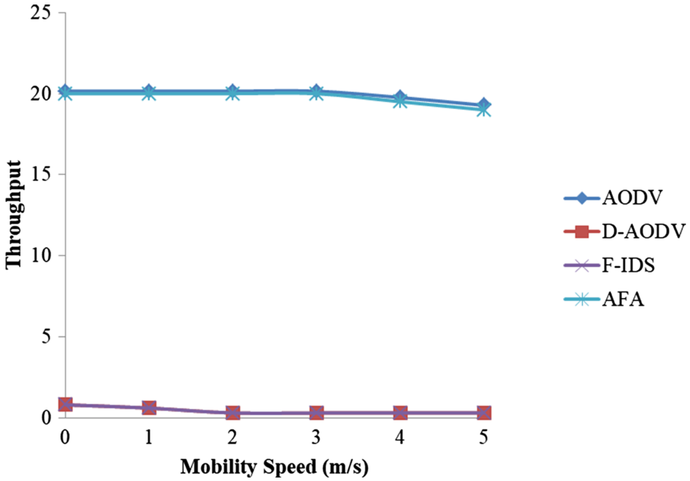


Fig. 16 Throughput vs Mobility under Data-Flooding Attack

proposed AFA scheme is employed, the routing overhead is 16350 which is better as compared with an existing scheme as shown in Fig. 17. It has been observed that when is no data flooder node in MANET, the routing overhead of AODV is 182 but when there is a data flooder node, the routing overhead of AODV is 372. The routing overhead in F-IDS under the data flooding attack is also 372 due to the lack of security mechanism against data flooding attacks. When the proposed AFA scheme is employed, the routing overhead is 202 which is low due to the incorporation of security mechanisms in AODV protocol which is better as compared with an existing scheme as shown in Fig. 18. From Figs. 17 and 18, it can be seen that with the increasing in the mobility speeds, the routing overhead is increasing. This is because of rebroadcasting of route request packets by the source nodes after route breakage due to mobility.

7.1.4 Normalized Routing Load

It is observed that when there is no route request flooder node, the normalized routing load in AODV is 0.77 but when there is a route request flooder node, the normalized routing load in AODV is infinity (∞) because of 0% of Packet Delivery Rate (PDR) as mentioned in Table 4 during route request flooding attack. It is computed by the total number of routing overhead divided by the number of data packets received. The normalized routing load in F-IDS under the flooding attack is 189.22 which is very high due to the low packet delivery rate. When the proposed AFA scheme is employed, the normalized routing load is 71.71 which is better as compared with an existing scheme as depicted in Fig. 19. When there is no data flooder node in MANET, the normalized routing load in AODV is 0.77 but when there is a data flooder node, the normalized routing load in AODV is 74.5. The normalized routing load in F-IDS under the data flooding attack is 74.5. When the proposed AFA scheme is employed, the normalized routing load is 1.15 which is better as compared with an existing scheme as depicted in Fig. 20. The low NRL in the proposed scheme is due to more number of data packets

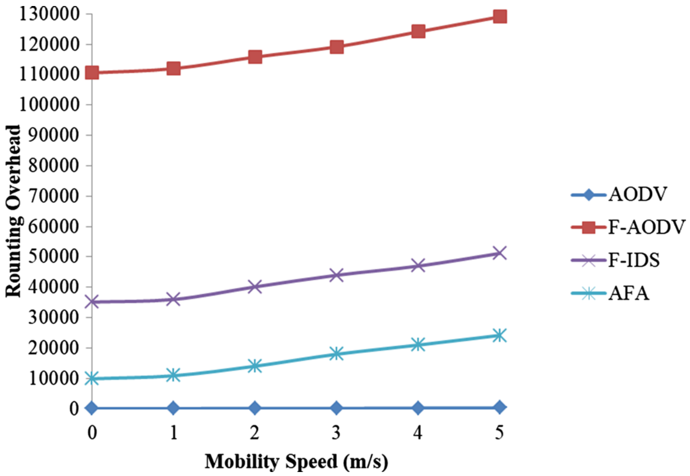


Fig. 17 Routing Overhead vs Mobility under Route Request Flooding Attack

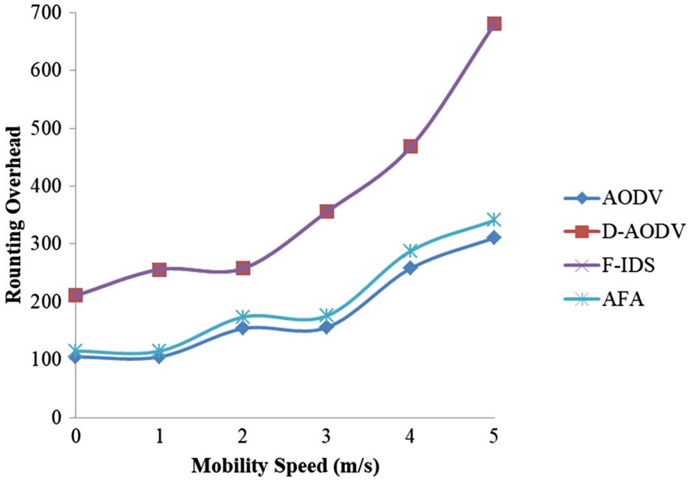


Fig. 18 Routing Overhead vs Mobility under Data-Flooding Attack

delivered. From Figs. 19 and 20, it can be seen that with the increasing in the mobility speeds, the normalized routing load is increasing. It is observed that with the increase in mobility speeds, the routing overhead is increasing and PDR is decreasing, therefore, the NRL will increase with the increase in mobility speeds as it is ratio of the number of control packets generated to the number of packets delivered.

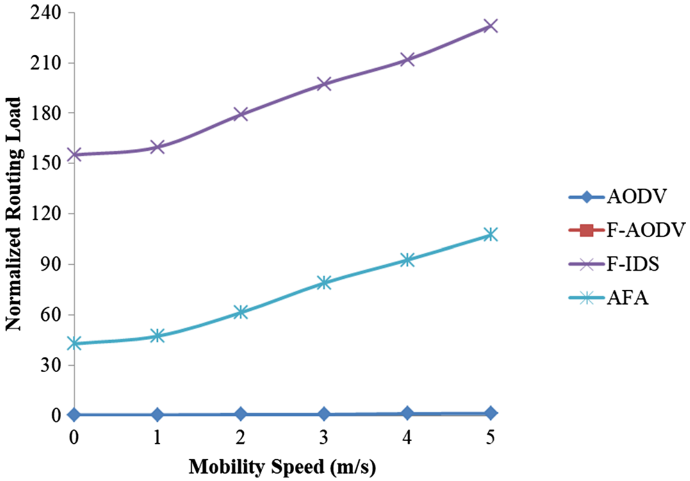


Fig. 19 NRL vs Mobility under Route Request Flooding Attack

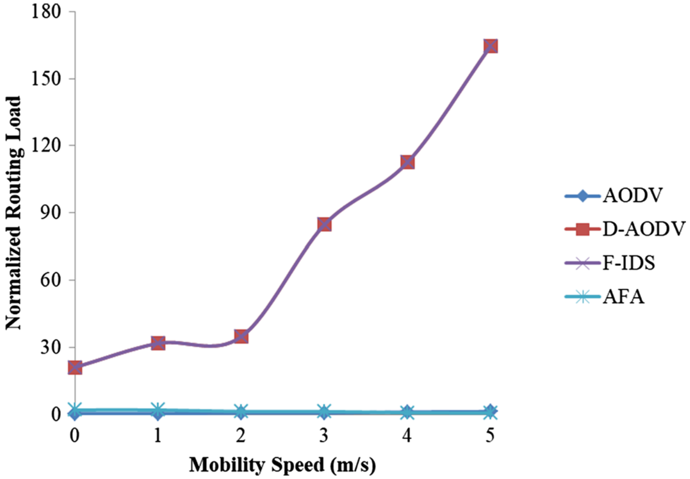


Fig. 20 NRL vs Mobility under Data-Flooding Attack

7.2 Effect of Number of Nodes

In this section, the network is tested with a varying number of nodes with a maximum speed of 20 m/s and random movement.

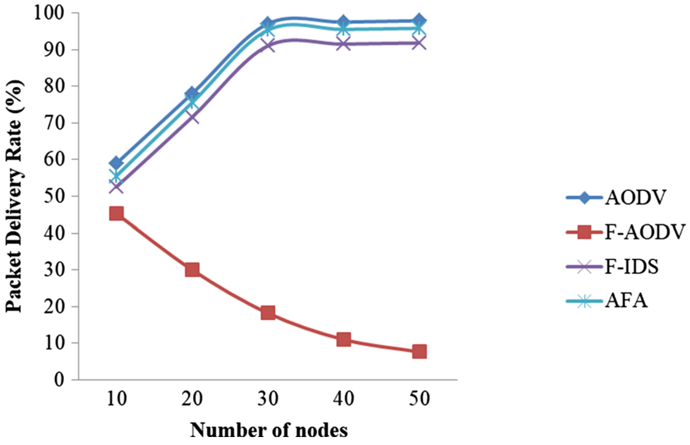


Fig. 21 Packet Delivery Rate vs Number of nodes under Route Request Flooding Attack

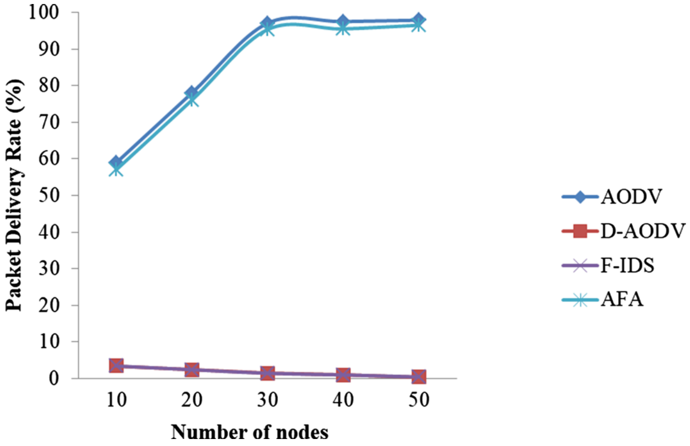


Fig. 22 Packet Delivery Rate vs Number of nodes under Data-Flooding Attack

7.2.1 Packet Delivery Rate (PDR)

In the absence of a route request flooder node, the PDR in AODV is 71.55%. In the presence of a route request flooder node, the PDR is 18.71% due to the broadcasting of fake route request packets sent by the flooder node which consumes the network bandwidth and destination nodes are not able to get the data packets. When the F-IDS scheme is used, the PDR is 66.38% but in the proposed scheme, the PDR is 69.60% under route request flooding attack which is better as compared with an existing scheme. It has been observed that in the absence of a data flooder node, the PDR in AODV is 71.55%. In the presence of a data flooder node, the PDR is 1.46%. When the F-IDS scheme is used, the PDR is 1.46%. This low PDR in the FIDS scheme is due to the lack of security mechanism against data flooding attacks but in the proposed scheme, the PDR is 70.05% under data flooding attacks which is better as compared with an existing scheme. From Figs. 21 and 22, it can be seen that with the increasing number of nodes, the PDR of AODV, F-IDS, and AFA is increasing due to the easy availability of a path towards the destination which is not easy if the number of nodes is low. Under route request flooding attack and data flooding attack, the PDR is decreasing. This is due to the reason that with more numbers of nodes, all nodes in the network are able to get the route request packets from the neighbouring nodes whereas if the number of nodes is low, the far-away nodes do not get the route request packet from the other node due to out of their range.

7.2.2 Throughput

It has been observed that in the absence of a data flooder node, the throughput in AODV is 14.32 kbps. In the presence of a route request flooder node, throughput is 3.75 kbps. This is because of the fake route request packets of the flooder node which keep other nodes busy in processing the fake packets. When the F-IDS scheme is used, the throughput is 13.29 kbps but in the proposed AFA scheme, the throughput is 13.93 kbps under route request flooding attack which is better as compared with an existing scheme. In the absence of a data flooder node, the throughput in AODV is 14.32 kbps. In the presence of a data flooder node, throughput is 0.29 kbps. When the F-IDS scheme is used, the throughput is 0.29 kbps. This is because of the lack of a security mechanism against the data flooding attack in F-IDS scheme but in the proposed AFA scheme, the throughputs are 14.02 kbps under a data flooding attack which is better compared with an existing scheme. From Figs. 23 and 24, it can be seen that the throughput of AODV, F-IDS, and AFA are increasing with the increase in the number of nodes and it is decreasing with the increase in the numbers of nodes under route request flooding attack and data flooding attack due to same reason as mentioned above in case of PDR.

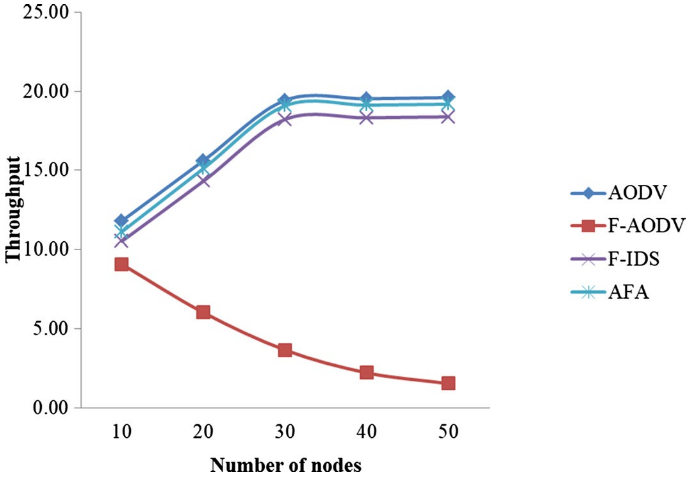


Fig. 23 Throughput vs Number of nodes under Route Request Flooding Attack

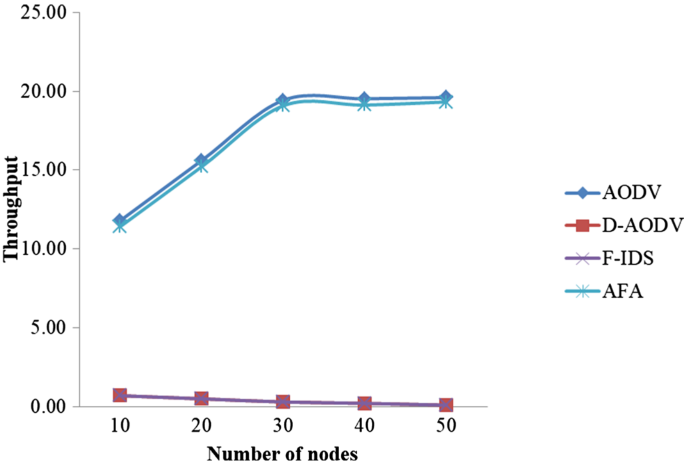


Fig. 24 Throughput vs Number of nodes under Data-Flooding Attack

7.2.3 Routing Overhead

When is no route request flooder node in MANET, the routing overhead in AODV is 243 but when there is a route request flooder node in the network, the routing overhead in AODV is 71957 due to the broadcasting of the fake request packet in the network. The routing overhead in the F-IDS scheme under the route request flooding attack is 22306. When the proposed AFA scheme is employed, the routing overhead is 4183 which is better as compared with an existing scheme. It has been observed that when is no data flooder node in MANET, the routing overhead of AODV is 243 but when there is a data flooder node, the routing overhead of AODV is 754. The routing overhead in F-IDS under the data flooding attack is also 754 due to the lack of security mechanisms against data flooding

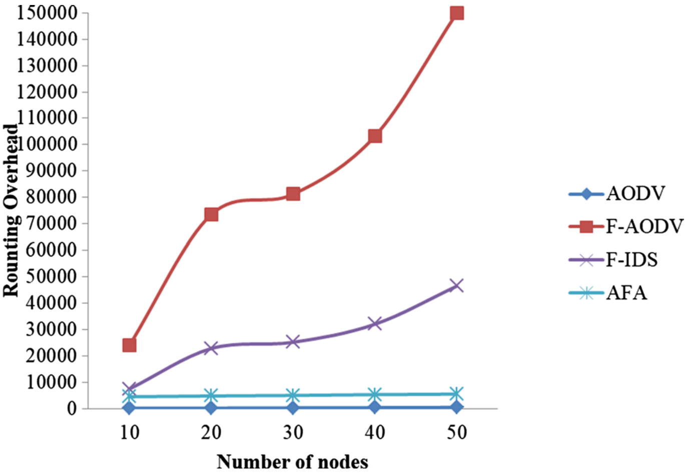


Fig. 25 Routing Overhead vs Number of nodes under Route Request Flooding Attack

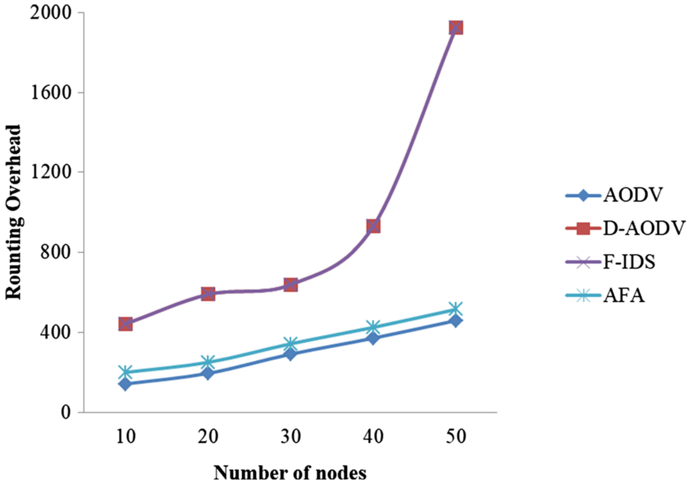


Fig. 26 Routing Overhead vs Number of nodes under Data-Flooding Attack

attacks. When the proposed AFA scheme is employed, the routing overhead is 289 which is low due to our proposed security mechanism which is better as compared with an existing scheme. From Figs. 25 and 26, it can be seen that with increasing numbers of nodes, the routing overhead is increasing. This is due to the generation of more control packets due to the high number of nodes in the network.

7.2.4 Normalized Routing Load

It is observed that when there is no route request flooder node, the normalized routing load in AODV is 1.16 but when there is a route request flooder node, the normalized routing load in AODV is 2573.31 which is very high due to fake request packets by flooder node.

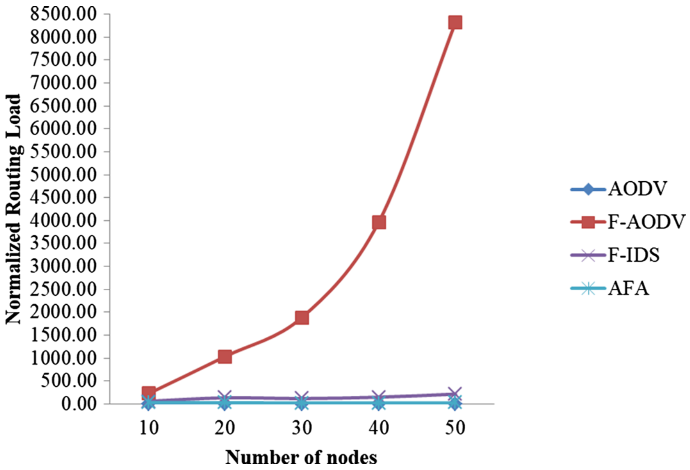


Fig. 27 NRL vs Number of nodes under Route Request Flooding Attack

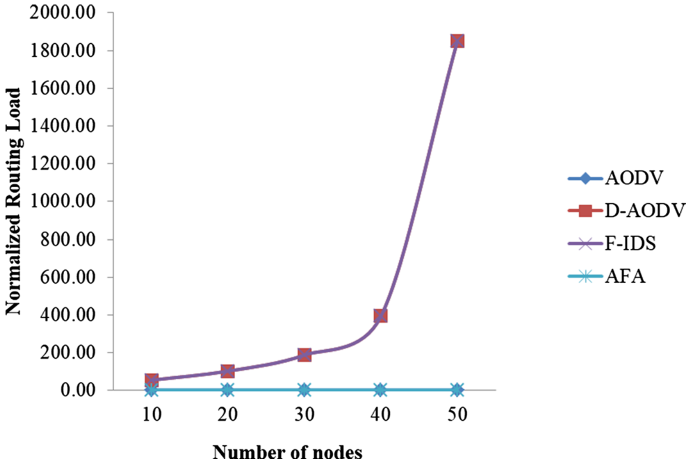


Fig. 28 NRL vs Number of nodes under Data-Flooding Attack

The normalized routing load in F-IDS under the flooding attack is 112.47. When the proposed AFA scheme is employed, the normalized routing load is 21.89 which is better as compared with an existing scheme as depicted in Fig. 27. When there is no data flooder node in MANET, the normalized routing load in AODV is 1.16 but when there is a data flooder node, the normalized routing load in AODV is 431.58. The normalized routing load in F-IDS under the data flooding attack is 431.58 due to a lack of security mechanisms against data flooding attacks. When the proposed AFA scheme is employed, the normalized routing load is 1.43 which is better as compared with an existing scheme as depicted in Fig. 28. The low NRL in the proposed scheme is due to more number of data packets delivered and it is increasing with the increase in the number of nodes due to same reason as mentioned above.

8 Conclusion

A mobile ad-hoc network is a network of autonomous mobile nodes and this network is vulnerable to many active attacks like data flooding attacks, route request flooding attacks, etc. In a flooding attack, the fake packets are sent by the flooder node due to which the network performance is degraded. Since the existing schemes deal mostly with route request flooding attacks and lack security mechanisms against data flooding attacks. To deal with both types of flooding attacks in the MANET, an Anti-Flooding Attack scheme is proposed which provides dual security mechanisms during the route discovery phase and data transmission phase. The efficiency of the AFA scheme is validated in the NS-2 simulator under different mobility speeds and the number of nodes scenario. The results obtained through the simulator tool show that the proposed AFA scheme performs better than the F-IDS scheme on various performance metrics.

Acknowledgements Not applicable.

Author Contribution All authors have contributed equally in this paper. All authors read and approved the final manuscript.

Funding The authors confirm that for this research no funding was received.

Data Availability Statement The authors confirm that the data supporting the findings of this study are available within the article.

Declarations

Conflict of interest The authors declare that they have no competing interests.

Ethical Approval Not applicable.

Consent to Participate Not applicable.

Consent for Publication Not applicable.

Human and Animal Participants Not applicable.

References

1. Murthy, C. S. R., & Manoj, B. S. (2004). *Ad hoc wireless networks: Architectures and protocols*. Upper Saddle, USA: Prentice Hall PTR.
2. Deng, H. M., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communication Magazine, 40*(10), 70–75.
3. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Elsevier Computers and Electrical Engineering, 40*(2), 530–538.
4. Medadian, M., Mebadi, A., & Shahri, E. (2009). Combat with Black Hole attack in AODV routing protocol. In *IEEE First Asian Himalayas International Conference*, pp. 530–535.
5. Su, M. Y. (2010). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Elsevier Computer Communication, 34*(1), 107–117.
6. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2014). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE System Journal, 9*(1), 65–75.
7. Ning, P., & Sun, K. (2004). How to misuse AODV: A case study of insider attacks against mobile adhoc routing protocols. *Elsevier Ad hoc Network, 3*(6), 795–819.
8. Jhaveri, R. H., Patel, S. J., & Jinwala, D.C. (2012). DoS attacks in mobile ad hoc networks: A survey. In *IEEE 2nd International Conference on Advanced Computing & Communication Technologies*, pp. 535–541.
9. Guo, Y., & Perreau, S. (2007). Trace flooding attack in mobile ad hoc networks. In *IEEE International Conference on Intelligent Sensors, Sensor Networks and Information*, pp. 329–334.
10. Yeung, D. S., Jin, S., & Wang, X. (2007). Covariance-matrix modeling and detecting Various flooding attacks. *IEEE Transaction on Systems, Man and Cybernetics, 37*(2), 157–169.
11. Yi, P., Wu, Y., & MA, J. (2009). Experimental evaluation of flooding attacks in mobile ad hoc networks. In *IEEE International Conference on Communications Workshops*, pp. 1–4.
12. Yi, P., Zhou, Y. K., Wu, Y., & Ma, J. (2009). Effects of denial of service attack in mobile ad hoc networks. *Journal of Shanghai Jiaotong University, 14*(5), 580–583. https://doi.org/10.1007/s12204-009-0580-7.19.Yu,J.,K
13. Yu, J., Kang, H., Park, D., Bang, H. C., & Kang, D. W. (2013). An in-depth analysis on traffic flooding attacks detection and system using data mining techniques. *Journal of Systems Architecture, 59*(10), 1005–1012.
14. Chouhan, N. S., & Yadav, S. (2011). Flooding attacks prevention in MANET. *International Journal of Computer Technology and Electronics Engineering (IJCTEE), 1*(3), 68–72.

15. Roshan, K., Prasad, K. R., Upadhayaya, N., & Govardhan, A. (2012). New-fangled method against data flooding attacks in MANET. *International Journal of Computer Science & Information Technology (IJCSIT), 4*(3), 25.
16. S. Hakak, S., Anwar, F., Latif, S. A., Gilkar, G., & Alam, M. K. (2014). Impact of packet size and node mobility pause time on average end to end delay and jitter in MANET's. In *IEEE International Conference on Computer and Communication Engineering*.
17. Kumar, S., Alaria, S., & Kumar, V. (2015). Prevention in sleep deprivation attack in MANET. *International Journal of Latest Technology in Engineering (IJLTEMAS), 4*(2), 139–144.
18. Bhalodiya, S., & Vaghela, K. (2015). Enhanced detection and recovery from fooding attack in MANETs using AODV routing protocol. *International Journal of Computer Applications, 125*(4), 10–15.
19. Jatthap, S., & Dashore, P. (2016). Battery capacity based detection and prevention of fooding attack on MANET. *In International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS), 4*(9), 89–99.
20. Rao, D. S., & Padmanabhuni, V. (2016). An efcient RREQ fooding attack avoidance technique for adaptive wireless network. *International Journal of Applied Engineering Research (IJAER), 11*(5), 3696–3702.
21. Pandikumar, T., & Desta, H. (2017). RREQ fooding attack mitigation in MANET using dynamic profle based technique. *In International Journal of Engineering Science and Computing (IJESC), 7*(6), 12700–12705.
22. Vimal, V., & Nigam, M. J., (2017). Plummeting food based distributed-DoS attack to upsurge networks performance in ad-hoc networks using neighborhood table technique. In *Proceedings of the 2017 IEEE Region 10 Conference,* pp. 139–144.
23. Gurung, S., & Chauhan, S. (2017). A novel approach for mitigating route request fooding attack in MANET. *Wireless Networks, 23*(4), 1–16.
24. Nithya, B., Nair, A., & Sreelakshmi, A. S. (2018). *Detection of RREQ flooding attacks in MANETs data and communication networks* (pp. 109–121). Singapore: Springer.
25. Zant, M. A., & Yasin, A. (2019). Avoiding and isolating flooding attack by enhancing AODV MANET protocol (AIF_AODV). *Hindawi Security and Communication Networks*. https://doi.org/10.1155/2019/8249108
26. Mohammadi, P., & Ghafari, A. (2019). Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis. *Wireless Personal Communications, 106*, 365–376.
27. Sbai, O., & Elboukhari, M. (2020). Data flooding intrusion detection system for MANETs using deep learning approach. In *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, pp 1–5.
28. Singh, G., & Joshi, G. (2021). A novel statistical adhoc on-demand distance vector routing protocol technique is using for preventing the mobile adhoc network from flooding attack. *Turkish Journal of Turkish Journal of Computer and Mathematics Education, 12*(6), 1753–1765.
29. Nishanth, N., & Mujeeb, A. (2021). Modeling and detection of flooding-based denial of service attacks in wireless ad hoc networks using uncertain reasoning. *IEEE Transactions on Cognitive Communications and Networking, 7*(3), 893–904.
30. Nandi, M., & Anusha, K. (2021). An optimized and hybrid energy aware routing model for effective detection of flooding attacks in a manet environment. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-09079-7
31. Luong, N. T., Nguyen, A. Q., & Hoang., D. (2022). FAPDRP: A flooding attacks prevention and detection routing protocol in vehicular ad hoc network using behavior history and nonlinear median filter transformation. *Wireless Networks*. https://doi.org/10.1007/s11276-022-03174-8
32. The network simulator-ns-2. http://www.isi.edu/ nsnam/ns/.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Vivek Mankotia received the M.Tech degree in Electronics and Communication Engineering in 2013 from Thapar University Patiala, Punjab, India and B.Tech degree in Electronics and communication Engineering in 2010 from Sardar Beant Singh State University, Gurdaspur, Punjab, India. He is an Assistant Professor (ECE) in Rajiv Gandhi Government Engineering College, Kangra and currently pursuing the Ph.D. degree in Electronics and Communication Engineering at National Institute of Technology Jalandhar, Punjab, India. His research interests include mobile ad hoc network security.

Ramesh Kumar Sunkaria received the Ph.D degree in Biomedical Signal Processing from IIT Roorkee, India. He received the M.Tech degree in Electronics and Communication Engineering from Guru Nanak Dev Engg. college, Ludhiana and and the B.Tech degree in Electronics and Communication Engineering from Guru Nanak Dev University, Amritsar Punjab, India. He is an Associate Professor in the department of Electronics and Communication Engineering, National Institute of Technology, Jalandhar, Punjab. His research interests include biomedical signal processing and network security. He has various publications in reputed conferences and SCI/SCIE indexed journal.

Shashi Gurung received the Ph.D degree in Computer Science and Engineering from National Institute of Technology, Hamirpur, HP, India in 2020. He received the M.Tech degree in computer science and engineering in 2014 and the B.Tech degree in computer science and engineering in 2011 from Punjab Technical University, Jalandhar, Punjab, India. He is an Assistant Professor (Computer Engineering) in Government Hydro Engineering College, Bilaspur, H.P. His research interests include mobile ad-hoc network security. He is reviewer of SCI and SCIE indexed journals publisher like IET, Elsevier, Emerald, Springer, Wiley, Hindawi etc and has various publications in reputed conferences and SCI/SCIE indexed journal.