Detection of RREQ Flooding Attacks in MANETs

B. Nithya, Aishwarya Nair and A. S. Sreelakshmi

Abstract Mobile Ad hoc Networks (MANETs) are prone to vulnerabilities as a result of lack of centralized management, dynamic topologies, and predefined boundary. There are many attacks that affect the performance of MANETs. Flooding attack is a Denial of Service attack, also known as DoS attack that brings down the network by flooding with a huge amount of route request (RREQ) packets, routed to a destination that does not exist. This paper proposes a robust detection system; a Fuzzy-based Flooding Attack Detection System (FFADS) using a first-order Mamdani-type fuzzy inference system to detect RREQ flooding attacks. This proposed system uses network-specific parameters rather than node-specific factors. Comprehensive simulations are carried out to observe the variations of input parameters with respect to the flooding level of the system. The simulation results reveal that any deviation from the normal behavior of nodes is immediately detected by the proposed system.

Keywords MANET · Flooding attacks · Fuzzy logic · RREQ flooding · AODV Network traffic

1 Introduction

Distributed DoS attack is an attack which makes a service unobtainable to users, usually by interrupting or suspending the services temporarily. In an RREQ flooding attack, a malevolent node floods the network by transmitting fake RREQs to non-existent nodes. This leads to congestion, thus resulting in a Denial of Service. It is very

B. Nithya (✉) · A. Nair · A. S. Sreelakshmi
Department of Computer Science and Engineering, National Institute of Technology,
Tiruchirappalli, Tiruchirappalli, India
e-mail: nithya@nitt.edu

A. Nair
e-mail: aishwarya05nair@gmail.com

A. S. Sreelakshmi
e-mail: sreelakshmias97@gmail.com

L. C. Jain et al. (eds.), *Data and Communication Networks*, Advances in Intelligent
Systems and Computing 847, https://doi.org/10.1007/978-981-13-2254-9_10

important to catch and prevent flooding attacks as these attacks result in congestion of the network. Overflow of routing table in the intermediate nodes is caused by RREQ flooding attacks which disable the nodes from receiving new RREQ packets, resulting in Denial of Service attack. Furthermore, forwarding these bogus RREQ packets consumes valuable node resources like energy and bandwidth.

Many solutions have been put forward to detect and avert flooding attacks in a network including behavioral approach which uses machine learning to classify nodes as malicious, statistical approach to prevent flooding in AODV networks, game theory-based approach, dynamic-based profile approach, and fuzzy logic. The main drawback faced by many of these approaches is that they restrict the number of attacker nodes and detect the maliciousness of the node, fix other parameters in the network, or work effectively only for smaller networks. Many surveys have also been conducted that analyze the effect of this attack on the different network parameters. Most of this research focuses on the nodes of the network and on classifying them as malicious and non-malicious, rather than on how the communication within the network is affected. Also, the dynamic nature of MANETs is often ignored in the development of solutions to detect the attacks on the network.

This paper introduces a system called Fuzzy-based Flooding Attack Detection System (FFADS), to catch RREQ flooding attacks especially in AODV-based networks using the first-order Mamdani-type fuzzy inference system. The solution focuses on the use of parameters that are specific to the network rather than the nodes. To detect the level of flooding attack in the system, the proposed system uses the dynamic input parameters, which are the properties of the network such as throughput, packet loss ratio, and routing overhead. While detecting the level of flooding attack, the proposed FFADS also detects abnormalities in communication within the network which may or may not be due to RREQ flooding. By stopping the malicious node from sending packets, the network can be restored to its previous state with increased throughput and reduced congestion.

This paper is organized into five sections. Section 2 deals with related works besides their detailed comparison. Section 3 deals with our proposed system for detection of flooding attacks. This includes an analysis of the different input parameters, the structure of the fuzzy inference system, and the conversion of the output value of the fuzzy system to the level of flooding in the network. Section 4 deals with performance analysis. It explains the simulation setup, the metrics involved in calculations, and graphs depicting the variations of input parameters with the number of flooding nodes. Section 5 presents the conclusion of this paper.

2 Related Works

There are no fixed topologies in a MANET because the topologies are dynamic in nature. The number of nodes and their relative positions vary greatly, and hence, detection of the number of malicious nodes becomes difficult. Various methods are suggested to detect the presence of flooding nodes in MANET. Some of them are discussed in the following paragraphs.

A Fuzzy-Based Trust Model (FBTM) is proposed [1] to disclose selfish nodes in MANETs. The fuzzy-based analyzer is joined with a trust model to identify the non-cooperative behavior of attacker nodes from the non-attacker nodes. In this scheme, every node in the network continuously checks its nearby nodes for their activities. Every node calculates a value called the trust value of its neighbors, and these values are then passed as input to a fuzzy function. The fuzzy function calculates the net trust value, and the attacker nodes are then detected based on this value.

A Novel Intrusion Detection System (NIDS) for ad hoc network is suggested in [2] using fuzzy logic. The first-order Sugeno-type fuzzy inference system (FIS) is adopted for intrusion detection in a mobile ad hoc network. In this system, different parameters are calculated from the network and fed to the FIS. The FIS returns the verity level for each node. This method is accurate in terms of a high true positive rate and low false positive rate, but requires the number of attacker and non-attacker nodes to remain constant.

The behavioral approach is adopted in [3] to detect malicious attacks. In this system, SVM classifier is used to classify nodes as malicious and non-malicious.

The statistical approach is used in [4] to defend against RREQ flooding attacks in MANETs. The RREQ packets are monitored in real time, and the nodes are compared against their neighbors to check if they exceed default route request limit.

Alleviating route request flooding attack in MANET is suggested in [5] using node reputation scheme to abide by the impact of flooding attack in MANET. This scheme checks the status of a node intermittently and restricts its route request transmitting rate accordingly.

The detection of SYN flooding attack in AODV protocol is performed in [6] to disclose the presence of the SYN flooding attack. The scheme proposed uses game theoretical approach to form a game between the attacker node and the multimedia server node. The performance of the detection algorithm is measured by examining the several qualities of the parameters.

Ad hoc flooding attack is analyzed, and a Flooding Attack Prevention (FAP) mechanism is developed in [7]. The proposed scheme uses a trust function to record the number of route request packets and calculates the trust value. If the calculated trust value exceeds the limit, the network drops these route request packets. In [8], throughput, packet delivery ratio, and round-trip delay are compared with normal network (without attacker nodes) and a network with few attacker nodes. The performance of the network is compared in all the three scenarios.

Dynamic Profile-Based Technique (DPBT) is proposed [9] to detect the flooding attacks in MANET. The proposed scheme defines a profile value based on the performance of MANET. It recognizes the attack and tries to stop it every time the node attempts to exceed the threshold value. This value changes with respect to the request placed by the network.

A flow-based discovery mechanism against flooding attacks is developed in [10]. Two flow-based detection features are designed, and the algorithm used on them precisely detects flooding attacks.

The above-discussed methods use a number of methods to detect the presence of flooding nodes in the system. Most researches concentrate exclusively on either detecting the presence of the malicious nodes or on being aware of the presence of these nodes and mitigating the effects of the attack. The main difficulties faced are due to the unpredictable nature of a MANET, in terms of number of harmless nodes, mischievous nodes, network topology, and mobility pattern. Most studies tend to restrict one or more of the above parameters to compute the result. Motivated by these factors, our paper tries to vary as many parameters as possible, while maintaining a maximum level of accuracy. Our paper uses fuzzy-based approach to detect the level of severity of flooding attack in a network independent of the nodes in the network, topology of the network, or the percentage of flooding nodes.

3 Proposed Fuzzy-Based Flooding Attack Detection System (FFADS)

The proposed Fuzzy-based Flooding Attack Detection System (FFADS) uses fuzzy logic to detect the number of flooding nodes in a MANET. Fuzzy logic is beneficial in this situation as it can handle uncertainties and make decisions in a given range. This paper uses three-input, single-output-based first-order fuzzy Mamdani inference system for composing the decision. The fuzzy parameters are elicited from the network traffic and then passed on to the fuzzy interface. In the fuzzy interface, the fuzzy rules are applied and the number of flooding nodes is estimated.

3.1 Fuzzy Controller in the Proposed System

A MANET network is simulated with an arbitrary number of nodes and various parameters of the network—routing overhead, throughput, and packet loss ratio are extracted from the traffic. These parameters are then fed to fuzzy inference system as shown in Fig. 1, which uses a set of rules to define the output. This can be reported by the system in terms of the extent of flooding attack in the system, which is classified as low, medium, and high.

From the simulated MANET environment, the parameters—throughput, packet loss ratio, and routing overhead—to be used in the intrusion detection system are extracted. The inputs are then fed to the fuzzy controller. The fuzzification module converts input data to values of the membership functions and matches data with conditional rules in the rule base. The Mamdani-type fuzzy inference engine applies the rules and returns a fuzzy set for the defuzzification block. The output values are converted to crisp values through the defuzzification module. The output values are used to decide the extent of flooding attack in the system. The fuzzy output is

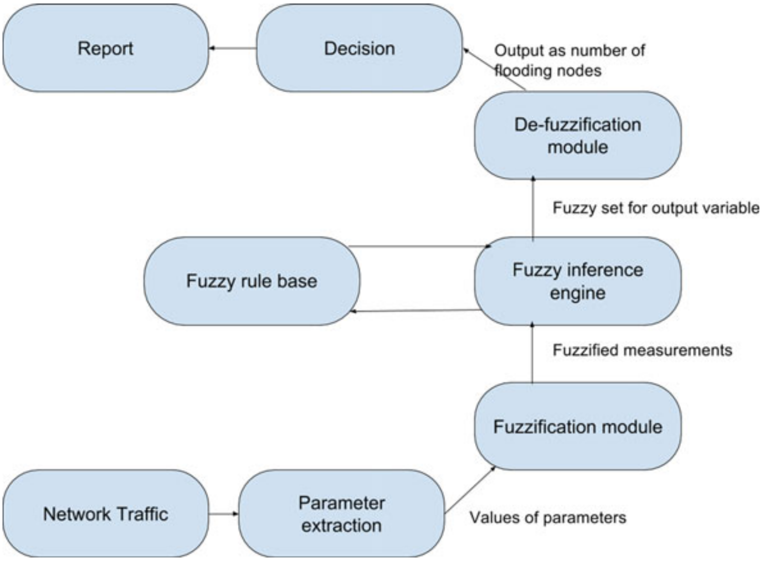

Fig. 1 Fuzzy inference system

generated within the range of [0, 1] which indicates the flooding level where 0–0.3 is classified as low, 0.3–0.7 is classified as medium, and 0.7–1 is classified as high.

3.2 Fuzzy Inputs

Routing Overhead: Routing overhead is determined as the ratio of route request packets (RREQ packets) among the total number of packets sent. It is observed that, as the number of flooding nodes increases, the number of route request packets relative to the total number of packets sent increases. Since routing overhead depends on the number of RREQ packets, the value will dynamically change depending on whether the bandwidth is utilized by RREQ packets. The membership function of this fuzzy input variable is depicted in Fig. 2.

$$\text{Routing overhead} = \frac{\text{Number of Route request packets sent}}{\text{Total number of packets sent}}$$

Packet Loss Ratio: Packet loss ratio is the ratio of the number of route request packets dropped relative to the total number of RREQ packets sent. It is observed that, as the number of flooding nodes increases, the packet loss ratio increases as the packets have to share bandwidth with the increasing number of route request packets. In a flooding attack, fake RREQs are sent to a destination that does not exist. Therefore, the fake RREQs are dropped since the node is unable to forward the

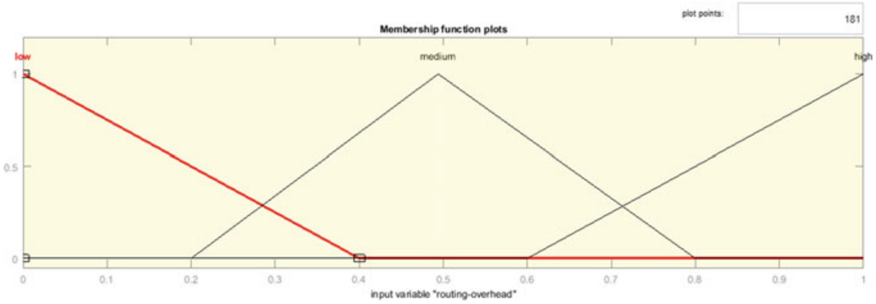

Fig. 2 Routing overhead membership function

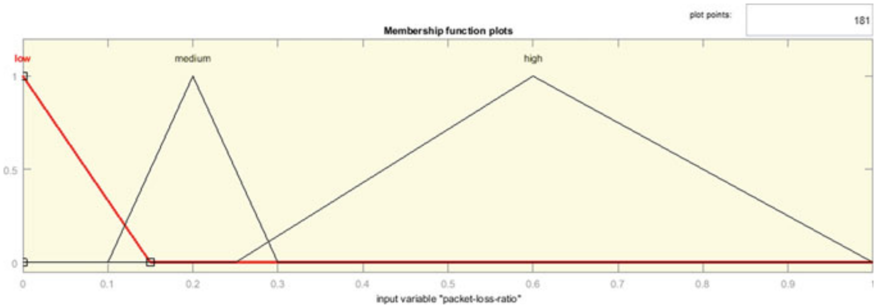

Fig. 3 Packet loss ratio membership function

RREQ packet. This increases packet loss ratio. The membership function is depicted in Fig. 3.

$$\text{Packet loss ratio} = \frac{\text{Number of RREQ packets dropped}}{\text{Number of RREQ packets sent}}$$

Throughput: In this simulation, throughput is determined as the fraction of TCP/UDP packets received at the destination to the sent packets. It is observed that, as the number of flooding nodes increases, the throughput decreases as the TCP/UDP packets are forced to share bandwidth with the increasing route request packets. As the number of fake RREQ increases, the channel experiences congestion and throughput gradually reduces. The membership function of this fuzzy input variable is depicted in Fig. 4.

$$\text{Throughput} = \frac{\text{Number of data packets}}{\text{Time}}$$

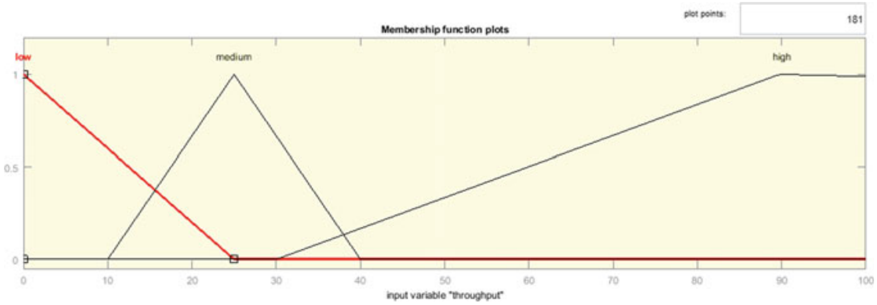

Fig. 4 Throughput membership function

Table 1 Fuzzy inference rules

Rule number	Routing overhead	Packet loss ratio	Throughput	Flooding level
1	Low	Low	High	Low
2	High	High	Low	High
3	Medium	Medium	Medium	Medium
4	High	High	Medium	High
5	Low	Low	Medium	Low
6	Low	Medium	High	Low
7	High	Medium	Medium	High
8	Medium	Medium	High	Medium
9	High	Medium	Low	High

3.3 Fuzzy Inference Rules

This detection system uses Mamdani-type inference system and takes in three parameters as input values—routing overhead, packet loss ratio, and throughput. The rule base considered in the proposed FFADS is given in Table 1.

3.4 Fuzzy Surface View

The surface view between two input parameters and the output parameter (flooding level) is shown in Figs. 5, 6, and 7. Different colors represent the severity of flooding. Figure 5 shows the output surface (flooding level) versus the two parameters—routing overhead and packet loss ratio. Figure 6 depicts the output surface (flooding level) versus the two parameters—routing overhead and throughput. The output surface (flooding level) versus the two parameters—throughput and packet loss ratio—is plotted in Fig. 7. The different colors of the surface graph—blue, green

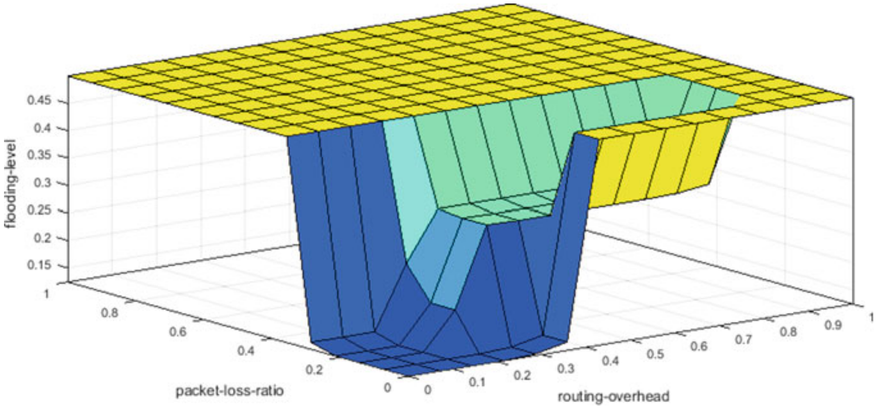

Fig. 5 Routing overhead, packet loss ratio

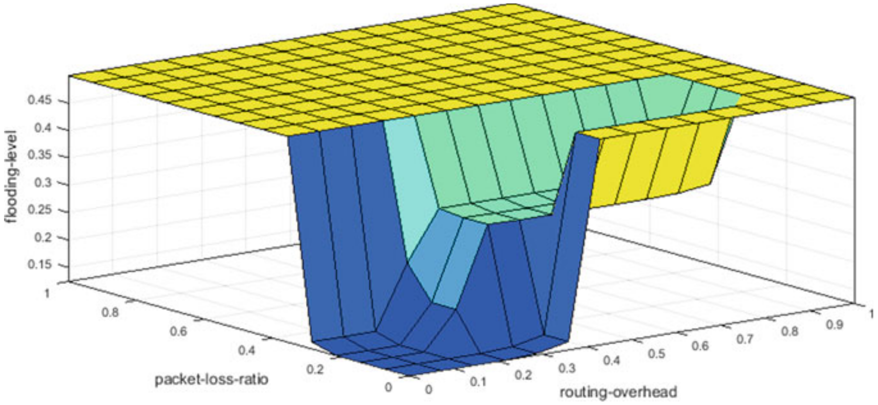

Fig. 6 Packet loss ratio, routing overhead

and yellow—represent the different levels of the output for the two given inputs, that is, the different intensities of flooding attack.

3.5 Fuzzy Output

The controller takes in the above-mentioned fuzzy inputs and maps them to their membership functions. This is then fed to the fuzzy rules. The obtained truth values are then defuzzified. The output values represent the extent of flooding attack in the system as shown in Fig. 8.

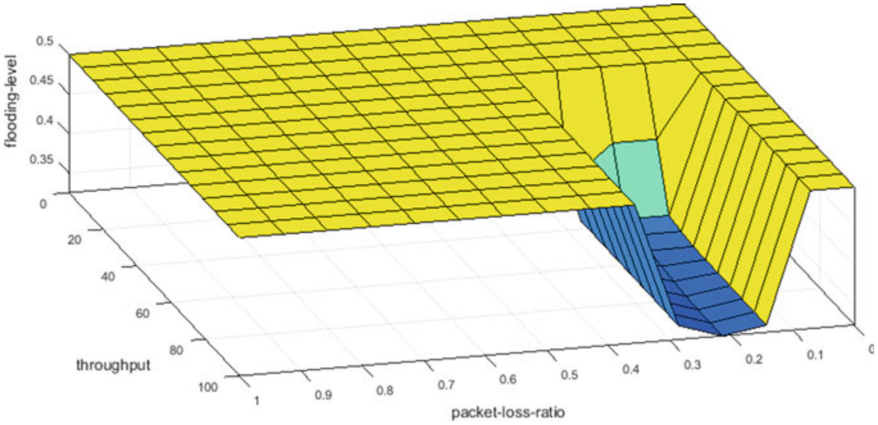

Fig. 7 Throughput, packet loss ratio

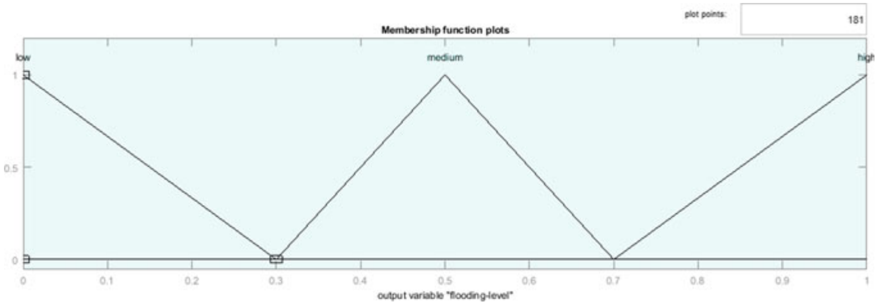

Fig. 8 Fuzzy output

4 Performance Analysis

This section briefs about the simulation setup and the performance analysis depending on the routing overhead, packet loss ratio, and throughput.

4.1 Simulation Setup

For this system, Ns2 simulator is used to simulate MANET. The simulation parameters are shown in Table 2. The parameters are extracted from the trace files and are fed to the Fuzzy Toolbox in MATLAB.

Table 2 Simulation parameters

Parameter	Value
Mac type	IEEE 802.11
Routing protocol	AODV
Antenna	Omni-directional
Simulation time	20 s
Traffic type	FTP
Topology	Random
Simulation area	500 m × 500 m
Number of nodes	Random

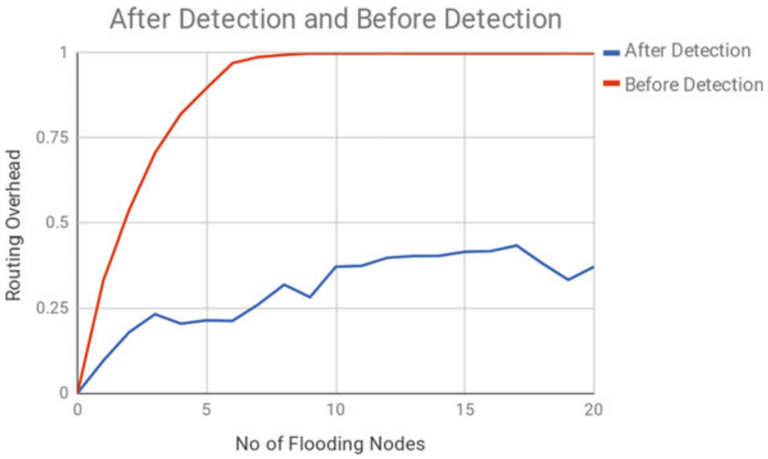

Fig. 9 Routing overhead versus number of flooding nodes

4.2 Metrics

In the proposed system, the following three parameters are considered to affect the level of flooding attack in the system.

Routing Overhead: Routing overhead is observed to increase with the extent of flooding attack in the system. The graph plotted in Fig. 9 shows a setup consisting of 25 nodes and different number of flooding nodes ranging from 0 to 20. It is observed that routing overhead increases linearly till a certain point beyond which it is observed to be constant. After detection of flooding attack, if the flooding node is correctly identified and the RREQ packets sent by the flooding node are ignored by all the other nodes, the effect of flooding attack is greatly reduced.

Packet Loss Ratio: It is observed from Fig. 10 that there is gradual increase in packet loss ratio with the increase in number of flooding nodes. Detection of flooding attacks is simulated by dropping any RREQ packets with unknown destination. The number of RREQ packets dropped is the same in both cases. Since packet loss ratio

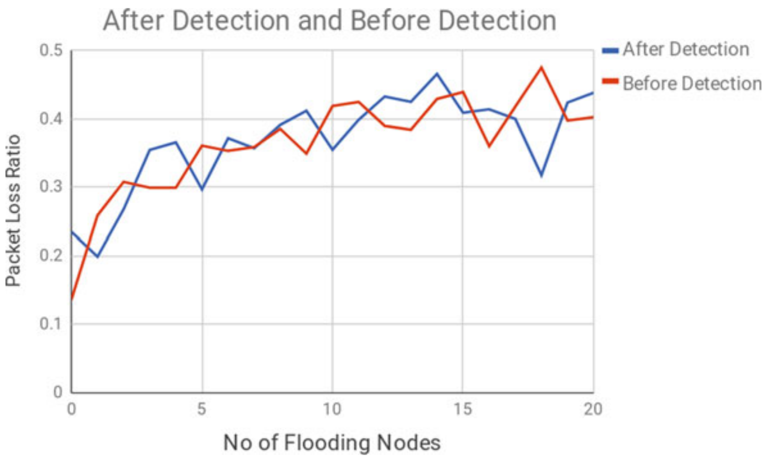

Fig. 10 Packet loss ratio versus number of flooding nodes

is the number of RREQ packets dropped, the packet loss ratio remains almost the same. Figure 10 shows that the RREQ packet loss ratio before and after detection.

Throughput: It is inferred from Fig. 11 that the throughput decreases as the number of flooding nodes increases. Since the fake RREQ packets utilize the bandwidth, the overall throughput decreases. It is observed that throughput increases significantly after detection of flooding attack as the entire bandwidth can now be used by the data communication taking place. The RREQ packets sent by the flooding node are dropped by all other nodes as long as it continues flooding the medium. Figure 11 depicts the variation of throughput with number of flooding nodes before and after detection of the flooding attack.

Predicted Flooding Level: The graph plotted in Fig. 12 depicts the flooding level of the network which consists of nodes ranging from 0 to 30. We have taken different setups with different number of nodes and measured the input parameters. It is observed that the predicted flooding level increases with the increase in number of flooding nodes. It is also observed that the predicted flooding level is independent of number of nodes, simulation time, and number of connections.

5 Conclusion

In this paper, a detection system—Fuzzy-based Flooding Attack Detection System (FFADS)—is proposed for detecting flooding attacks using fuzzy logic. The proposed system predicts the flooding level using three input parameters—routing overhead, throughput, and packet loss ratio. The flooding level is independent of the number of nodes, simulation time, and number of connections and depends only on the externally measured parameters. The system has an edge over existing systems that

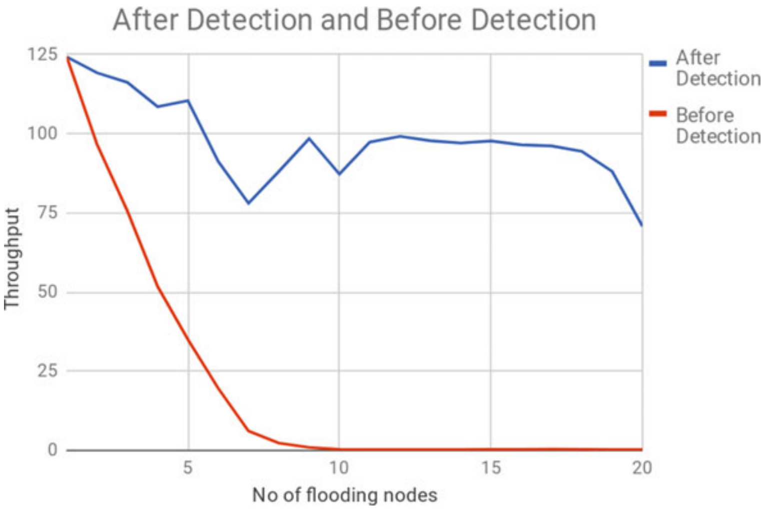

Fig. 11 Throughput versus number of flooding nodes

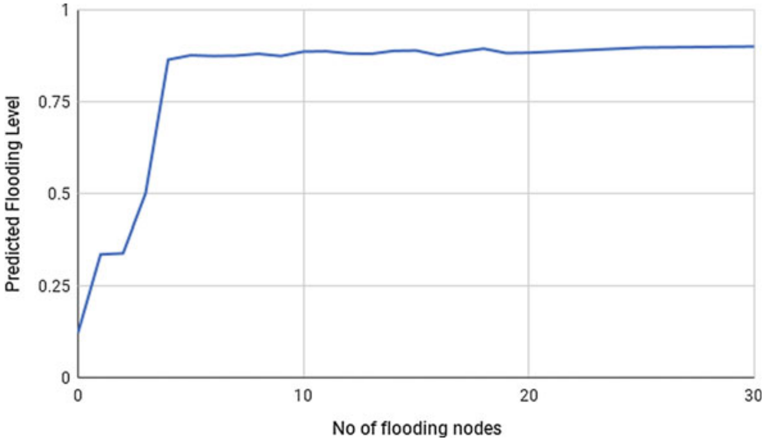

Fig. 12 Predicted flooding level versus number of flooding nodes

detect intrusions as it is dynamic in nature and the predicted flooding level changes with the performance of the network. Also since the system does not restrict the size or topology of the network, it can be applied on real-world networks to detect flooding attacks.

References

1. Ullah, Z., Khan, M.S., Ahmed, I., Javaid, N., Khan, M.I.: Fuzzy-based trust model for detection of selfish nodes in MANETs. In: 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, pp. 965–972 (2016)
2. Chaudhary, A., Tiwari, V., Kumar, A.: A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks. In: International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, pp. 1–4 (2014)
3. Patel, M., Sharma, S.: Detection of malicious attack in MANET a behavioral approach. In: 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, pp. 388–393 (2013)
4. Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., Gaiti, D.: Flooding attacks detection in MANETs. In: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, pp. 1–6 (2015)
5. Choudhury, P., Nandi, S., Pal, A., Debnath, N.C.: Mitigating route request flooding attack in MANET using node reputation. In: IEEE 10th International Conference on Industrial Informatics, Beijing, pp. 1010–1015 (2012)
6. Geetha, K., Sreenath, N.: Detection of SYN flooding attack in mobile ad hoc networks with AODV protocol. Arab. J. Sci. Eng. **41**, 1161 (2016)
7. Chouhan, N.S., Yadav, S.: Flooding attacks prevention in MANET. Int. J. Comput. Technol. Electron. Eng. (IJCTEE) **1**(3) (2013)
8. Bhalodiya, S., Balakrishnan, V., Chauhan, R., Chouhan, N.S., Fitri, M.H., Ghonge, M.M., Hong, F., Jawandhiya, P.M., Joshi, K., Lomte, V., Murthy, S.R., Pushpalatha, M., Rai, M.K., Song, J., Tupakula, U., Vaghela, K., Varadharajan, V., Venkataraman, R.: Enhanced detection and recovery from flooding attack in MANETs using AODV routing protocol (2015)
9. Sathish, T., Sasikala, E.: Dynamic profile based technique to detect flooding attack in MANET. Int. J. Innov. Res. Comput. Commun. Eng. **2**(1) (2014)
10. Guo, Y., Gordon, S., Perreau, S.: A flow based detection mechanism against flooding attacks in mobile ad hoc networks. In: 2007 IEEE Wireless Communications and Networking Conference, Kowloon, pp. 3105–3110 (2007)