Designing of Fuzzy Logic-Based Intrusion Detection System (FIDS) for Detection of Blackhole Attack in AODV for MANETs

Ruchi Makani and B. V. R. Reddy

Abstract Mobile Ad hoc networks (MANETs) are wireless/infrastructure-less and resource-constraint, having collection of nodes with high mobility feature (Ramanathan and Redi in IEEE Commun Magaz 40(5) 2002). It is a challenge to have efficient intrusion detection system (IDS) for such wireless and mobile architecture of systems. Researchers have presented in their research that the fuzzy logic-based intrusion detection systems are more adoptable to MANET's application because behavior of any mobile node may be visualized in fuzziness characteristics. It is required to design robust IDS system which can sustain and can work efficiently in MANET environments. The work presents the selection of suitable protocol features and fuzzy rules generation which exhibits substantial role for precision of the fuzzy logic-based intrusion detection system (FIDS). Here, set of fuzzy rules have been proposed to protect network against blackhole attack. These set of rules are created using three AODV critical attribute which are rate of *RREQ*, *RREP* and *Sequence number* value. The proposed FIDS, thereafter, evaluated using ns2 simulator and are found efficient to detect and isolate the attacker node from the network. The deployment of FIDS has resulted in increase of throughput of the network.

Keywords AODV · MANET · Fuzzy-logic · Intrusion detection · Blackhole

1 Introduction

Aim of an intrusion detection system (IDS) is to ascertain attack or malicious activities in a standalone system or in networked systems, by continuously monitoring the audit trail of traffic. IDS largely use soft-computing techniques to monitor the 'arriving at' and 'passing by' of traffic packets to detect intrusion. Fuzzy

R. Makani (✉) · B. V. R. Reddy
University School of Information, Communication & Technology,
Guru Gobind Singh Indraprastha University, Delhi, India
e-mail: ruchichaudhary@nic.in

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_11

logic-based intrusion detection model uses fuzzy rules or fuzzy classifiers to detect various intrusive behaviors by creating more abstract and flexible patterns for intrusion detection and provides significant advantages over other techniques [2, 3]. The use of fuzziness helps to understand the abrupt separation in normal and abnormal behavior of the node distinctly and also provides a measure of the degree of normality or abnormality of an event. Section 2 of this paper has presented general overview of fuzzy logic-based intrusion detection systems. Section 3 covers the critical filed of AdHoc on-demand distance vector (AODV) protocol used in MANETs. Section 4 is presenting proposed fuzzy rules for IDS designing in detail. Sect. 5 covering the simulation of FIDS for MANETs, and the performance of AODV has been recorded with and without blackhole attack. Section 6 concludes the finding of the work.

2 Overview of Fuzzy Logic-Based Intrusion Detection

Only fuzzy logic is a computational paradigm that builds a set of user-defined rules which are converted into mathematical equivalents [4–6]. Moreover, it has the advantage to offer valuable flexibility for reasoning that considers inaccuracies and uncertainties [7–10]. It can also manage approximate reasoning instead of fixed reasoning and able to handle imprecise and incomplete data. In standard set theory, each element is either completely a member of a category or not a member at all. In contrast, fuzzy set theory allows partial membership in sets or categories. In fuzzy logic, the truth value of any event can be termed between ‘0’ and ‘1’. Fuzzy logic-based intrusion detection (FLID) classifies the nodes into ‘trusted nodes’ and ‘malicious nodes’ after evaluating the nodes’ behavior (i.e., degree of reliability) by utilizing user-defined fuzzy inference rules [11–13]. Primarily, an FLID consists of three processing steps: fuzzification, inference system and defuzzification.

Fuzzification: In fuzzification, input data values are obtained and converted into fuzzy set by using fuzzy linguistic variables and membership functions. In inference processing system, a set of fuzzy rules are created (*in form of ‘IF–THEN’ decision statements to encode an expert’s knowledge of known patterns of attack and system vulnerabilities*) by the user, depending on the application environment/requirement.

Inferences System: Inferences are established after the processing of inputs based on fuzzy rules. The inferences are then combined to compute the fuzzy output distribution.

Defuzzification: In defuzzification, the resulting fuzzy output distribution is mapped back to a crisp output value using the membership functions. The detailed processing involved in each step of fuzzy-based intrusion system is available in [14, 15]. However, a broad flow chart of the FLID is shown in Fig. 1.

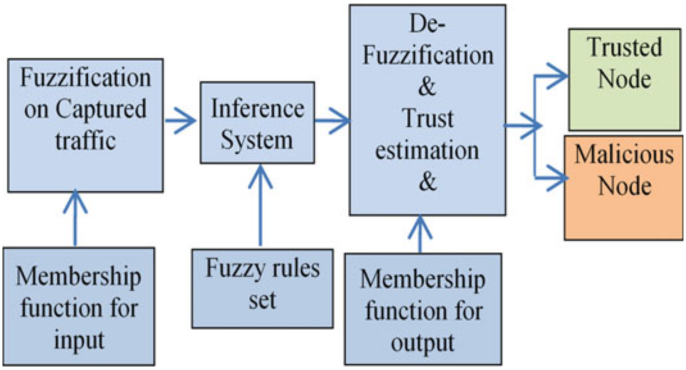

Fuzzification on Captured traffic
Inference System
De-Fuzzification & Trust estimation &
Trusted Node
Malicious Node
Membership function for input
Fuzzy rules set
Membership function for output

Fig. 1 Flow chart of fuzzy-logic-based IDS

3 Critical Fields of AODV Routing Protocol

AODV [16] is one of the most popular and widely used reactive routing protocols in MANETs. AODV ensures loop-free, single path and hop-by-hop distance vector routing [17]. AODV operates in two sub phases: *Route discovery* and *Route maintenance*. It uses four types of message packets to communicate among each other—route request (RREQ) and route reply (RREP) messages are needed in route discovery subphase, and route error (RERR) messages and HELLO messages are needed in route maintenance subphase. In each AODV routing packet, some critical fields such as control packet ID, type, hop count, sequence numbers of source and destination, IP addresses of source and destination, flags, lifetime are essential for correct protocol execution and routing [18, 19]. However, attackers may launch attack by advertising altered routing information to mislead correct routes (*known as route logic compromising attacks*) or by intently dropping the packets (*known as packet distortion attacks*). Any misuse or alteration of these critical fields by the attacker can cause AODV routing protocol to malfunction resulting in network performance degradation. Various publications relating to attacks of AODV and its effect on the network are available in [18, 19].

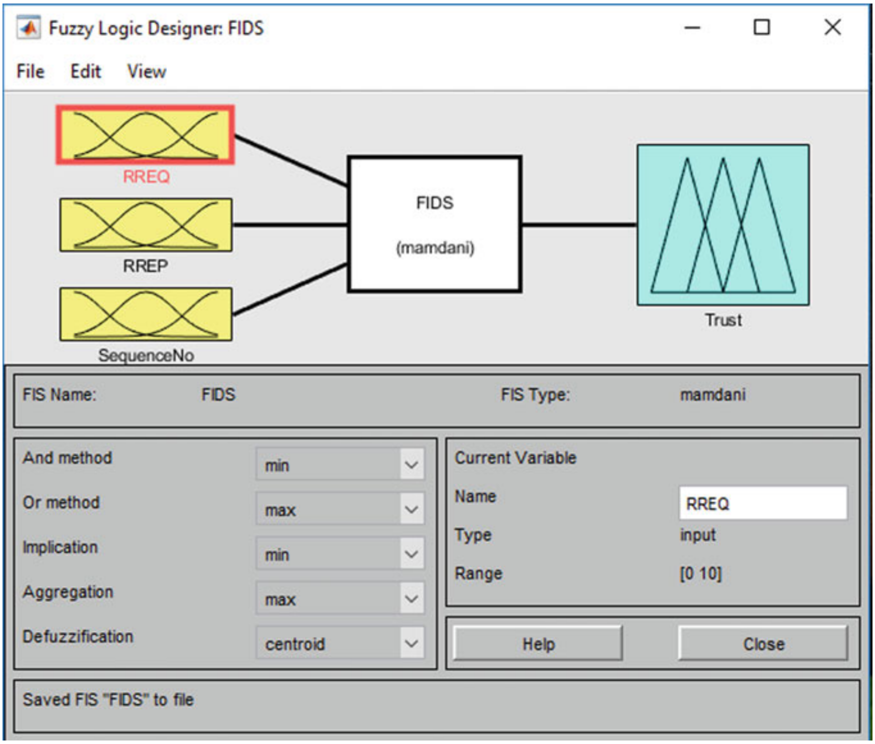
4 Proposed Fuzzy Rules for IDS Designing

In the above Sect. 3, the critical field of AODV protocols have been discussed which may be modified by attackers to deteriorate network performance. Here, efforts have been made to design a robust fuzzy logic-based intrusion detection (FIDS) system which is capable of detecting a blackhole attacker node in a network. For this, three attributes have been used to build up the fuzzy rules for fuzzification: (i) rate of forwarding RREQ control packet, (ii) rate of forwarding the RREP packets and (iii) value of sequence number. For the development of robust and effective FIDS, three following steps have been taken for designing.

4.1 Fuzzification

For the designing of FDIS, the fuzzy logic designer MATLAB (version 9.7) toolbox has been used. The three inputs, i.e., RREQ, RREP and sequence number, have been taken. The RREQ input have been divided into three categories, viz., very high (*reqVH*), high (*reqH*) and low (*reqL*). RREP is divided into two datasets, viz., high (*repH*), low (*repL*), and the sequence number is divided into three datasets, viz., high (*nauH*), medium (*nauM*), low (*nauL*). The designed FIDS's block diagram is shown in Fig. 2. The output value (*named as 'trust'*) has been estimated from the FIDS.

The membership function for output 'trust' has been divided in five sets ranging from 0 to 1 as very high (*VH*), high (*H*), medium (*M*), low (*L*) and very low (*VL*), as depicted in Fig. 3. Data is converted into fuzzy set by using fuzzy linguistic



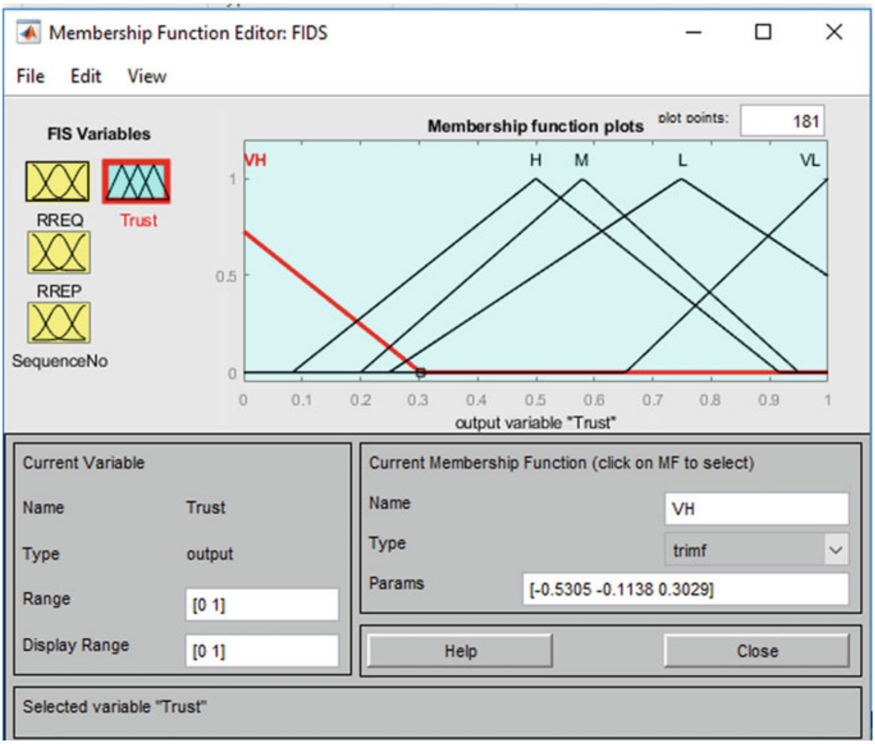
FIS Name: FIDS
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: RREQ
Type: input
Range: [0 10]

Saved FIS "FIDS" to file

Fig. 2 FIDS designer



Current Variable

Name Trust

Type output

Range [0 1]

Display Range [0 1]

Current Membership Function (click on MF to select)

Name VH

Type trimf

Params [-0.5305 -0.1138 0.3029]

Selected variable "Trust"

Fig. 3 Output fuzzy membership function plot

variables and membership functions. Here, triangular function (*trimf*) have been used for fuzzification. For the evaluation of the proposed FIDS, an input data value is obtained using simulations of MANET network in network simulator software (version ns 2.35) and has been discussed in the next section.

4.2 *Inferences System*

A set of 16 fuzzy rules have been created (in the form of 'IF–THEN' decision statements) to discern the behavior of node for the detection of a blackhole attacker (malicious node) in a given network. The blackhole attacker node broadcasts the route reply packet against the response of route request packet send by node with high sequence number to present the freshness of the loop. Based on this theory, following 16 rules have been included in FIDS. The details of the rules are listed in Table 1, and their inclusion in the fuzzy toolbox is shown in the Fig. 4. Inferences are derived after the processing of inputs based on fuzzy rules. The inferences are

Table 1 Proposed fuzzy rules

1. (REQ == reqL) | (RREP == repL) | (SequenceNo == nauL) => (Trust∼=VH) (1)
2. (RREQ == reqH) | (RREP == repL) | (SequenceNo == nauM) => (Trust=H) (0.1)
3. (RREQ == reqL) | (RREP == repH) | (SequenceNo == nauL) => (Trust=M) (0.1)
4. (RREQ == reqH) | (RREP == repL) | (SequenceNo == nauL) => (Trust=M) (0.1)
5. (RREQ == reqH) | (RREP == repH) | (SequenceNo == nauL) => (Trust=M) (0.1)
6. (RREQ == reqVH) | (RREP == repL) | (SequenceNo == nauL) => (Trust=M) (0.1)
7. (RREQ == reqVH) | (RREP == repH) | (SequenceNo == nauM) => (Trust=M) (0.1)
8. (RREQ == reqL) | (RREP == repL) | (SequenceNo == nauM) => (Trust=M) (0.1)
9. (RREQ == reqL) | (RREP == repH) | (SequenceNo == nauM) => (Trust=L) (0.1)
10. (RREQ == reqH) | (RREP == repH) | (SequenceNo == nauM) => (Trust=L) (0.1)
11. (RREQ == reqVH) | (RREP == repL) | (SequenceNo == nauM) => (Trust=L) (0.1)
12. (RREQ == reqVH) | (RREP == repL) | (SequenceNo == nauH) => (Trust=L) (0.1)
13. (RREQ == reqL) | (RREP == repL) | (SequenceNo == nauH) => (Trust∼=VL) (0.1)
14. (RREQ == reqL) | (RREP == repH) | (SequenceNo == nauH) => (Trust∼=VL) (0.5)
15. (RREQ == reqH) | (RREP == repH) | (SequenceNo == nauH) => (Trust∼=VL) (0.5)
16. (RREQ == reqVH) | (RREP == repH) | (SequenceNo == nauH) => (Trust∼=VL) (0.5)

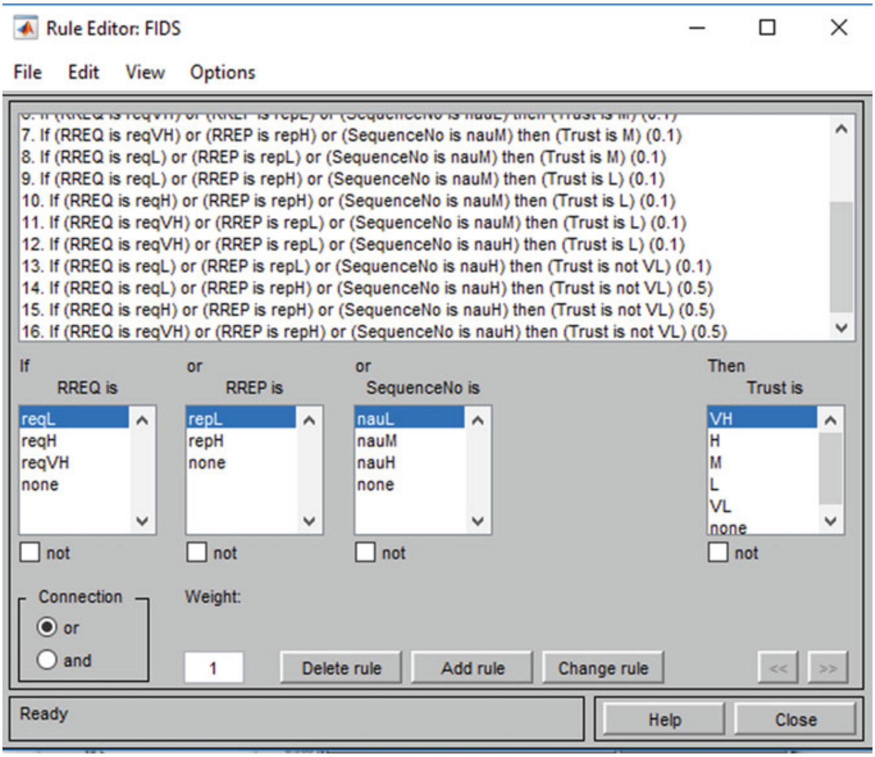
then combined to compute the fuzzy output distribution. The graphical representation of the inference obtained after the computation is depicted in Fig. 5.

4.3 *Defuzzification*

The resulting fuzzy output distribution is mapped back to output value using the same membership functions which was used during fuzzification. Here, triangular function (*trimf*) has been used. In the following Table 2 are a few test data which were used in simulation to compute the defuzzification.

5 Simulations and Result Discussion

To establish the importance of intrusion detection systems in a mobile network in Sect. 5.1, performance of AODV has been recorded with and without blackhole attack. In Sect. 5.2, performance of FIDS has been evaluated in presence of blackhole attack.



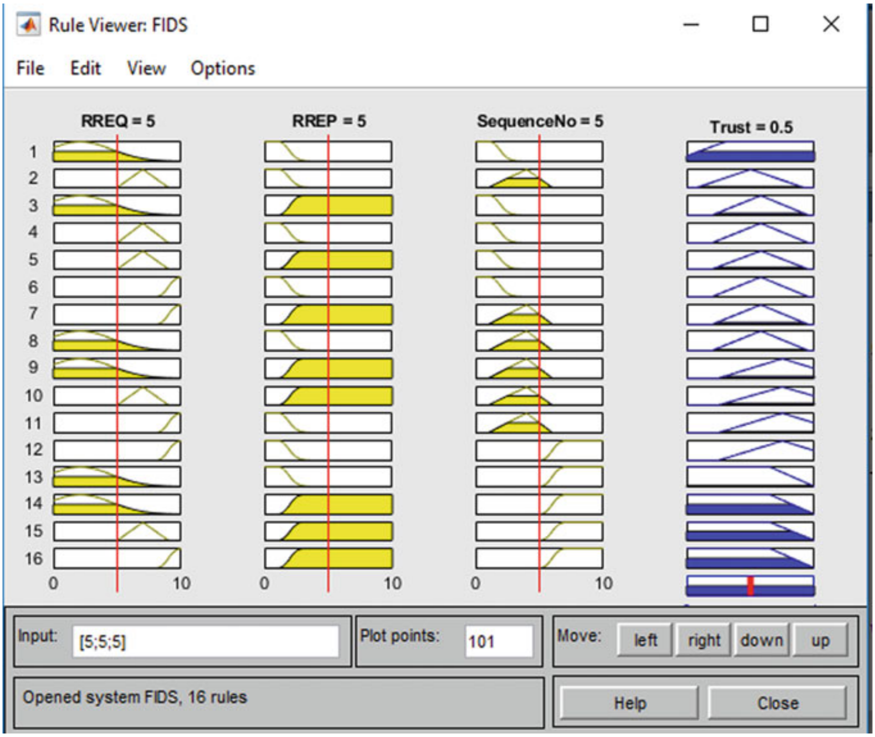
7. If (RREQ is reqVH) or (RREP is repH) or (SequenceNo is nauM) then (Trust is M) (0.1)
8. If (RREQ is reqL) or (RREP is repL) or (SequenceNo is nauM) then (Trust is M) (0.1)
9. If (RREQ is reqL) or (RREP is repH) or (SequenceNo is nauM) then (Trust is L) (0.1)
10. If (RREQ is reqH) or (RREP is repH) or (SequenceNo is nauM) then (Trust is L) (0.1)
11. If (RREQ is reqVH) or (RREP is repL) or (SequenceNo is nauM) then (Trust is L) (0.1)
12. If (RREQ is reqVH) or (RREP is repL) or (SequenceNo is nauH) then (Trust is L) (0.1)
13. If (RREQ is reqL) or (RREP is repL) or (SequenceNo is nauH) then (Trust is not VL) (0.1)
14. If (RREQ is reqL) or (RREP is repH) or (SequenceNo is nauH) then (Trust is not VL) (0.5)
15. If (RREQ is reqH) or (RREP is repH) or (SequenceNo is nauH) then (Trust is not VL) (0.5)
16. If (RREQ is reqVH) or (RREP is repH) or (SequenceNo is nauH) then (Trust is not VL) (0.5)

Fig. 4 Fuzzy rules (if-then-else form)

5.1 Performance Evaluation of AODV Protocol Under Attack

Firstly, within AODV protocol source codes, blackhole attacks have been simulated using network simulator software (ns2.35). The general simulation parameters are given in Table 3. The AODV performance is recorded in terms of packet delivery ratio, throughput, energy consumption and routing overhead in the presence of blackhole attack and without attack.

It is observed that packet delivery ratio decreases when there is a one blackhole node attack in a network. Further, this reduces by 60% when there is two blackhole node present in a network, and simulation results are shown in Fig. 6. It is observed that throughput is reduced in the presence of one blackhole node attack in a network. This reduces more significantly approximately 60% in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 7. Further, it is recorded that network energy consumption increases by 50% in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 8. Similarly, it is found that routing overhead in a given network also increases in the presence of two blackhole nodes in a network, and simulation results are shown in Fig. 9.



Input: [5;5;5]

Plot points: 101

Opened system FIDS, 16 rules

Fig. 5 Graphical representation of fuzzy rules

Table 2 Inference computation

Rate of RREQ	Rate of RREP	Sequence No	Computed trust	Inferences
5	5	5	0.5	Normal
0.301	5	5	0.544	Normal
0.301	9.46	5	0.544	Normal
0.958	9.46	9.22	0.458	Malicious
0.958	0.542	9.22	0.544	Normal
0.958	0.542	0.663	0.546	Normal
7.41	0.904	0.663	0.549	Normal
9.1	0.904	0.663	0.551	Normal
9.34	0.542	9.22	0.544	Normal
9.34	4.4	9.22	0.458	Malicious

Table 3 Simulation parameters for MANETS

Parameters	Value
Simulation tool	NS-2.35
Network nodes	20
Grid area	500 × 500
Routing protocol	AODV
Antenna	Omni directional
MAC type	802.11
Traffic type	CBR
Number of blackholes	2 nodes
Simulation time	500 s

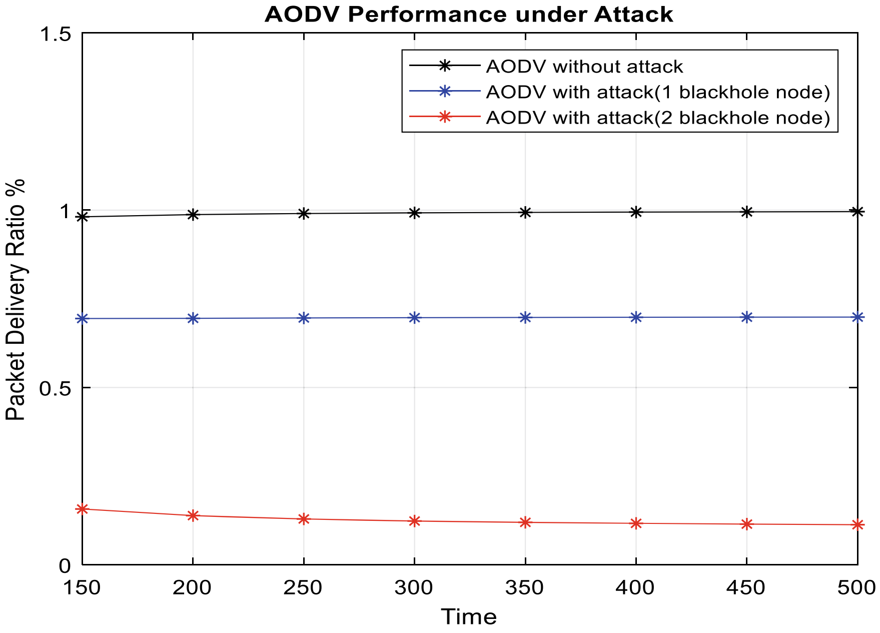


Fig. 6 AODV under attack—PDR versus simulation time

5.2 *Performance Evaluation of Proposed FIDS in AODV Protocol*

For the evaluation of the proposed FIDS, AODV source codes in ns 2.35 software have been modified and fuzzy-based intrusion detection module has been added. Further, the multiple blackhole attacks have been simulated in a given network.

It is observed that the performance of the network increases on the incorporation of proposed FIDS, as shown in the Figs. 10 and 11. Both PDR and throughput of the network are found to increase when FIDS has been included in AODV protocol.

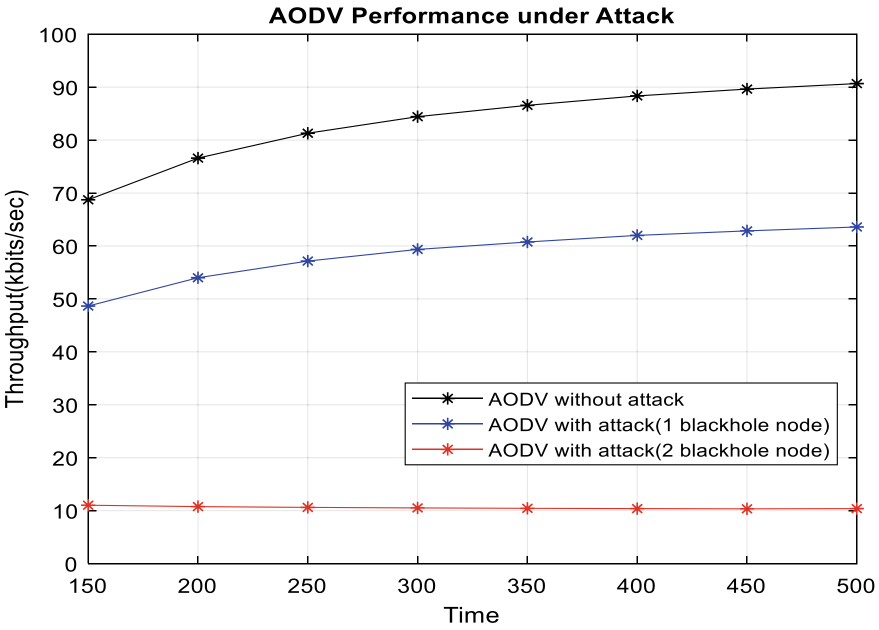


Fig. 7 AODV under attack—throughput versus simulation time

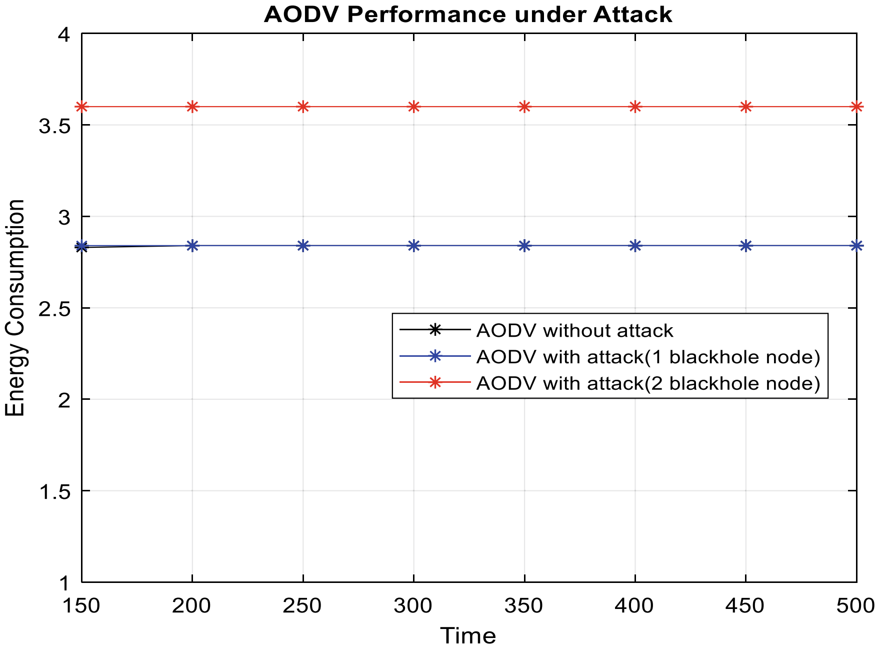


Fig. 8 AODV under attack—energy consumption versus simulation time

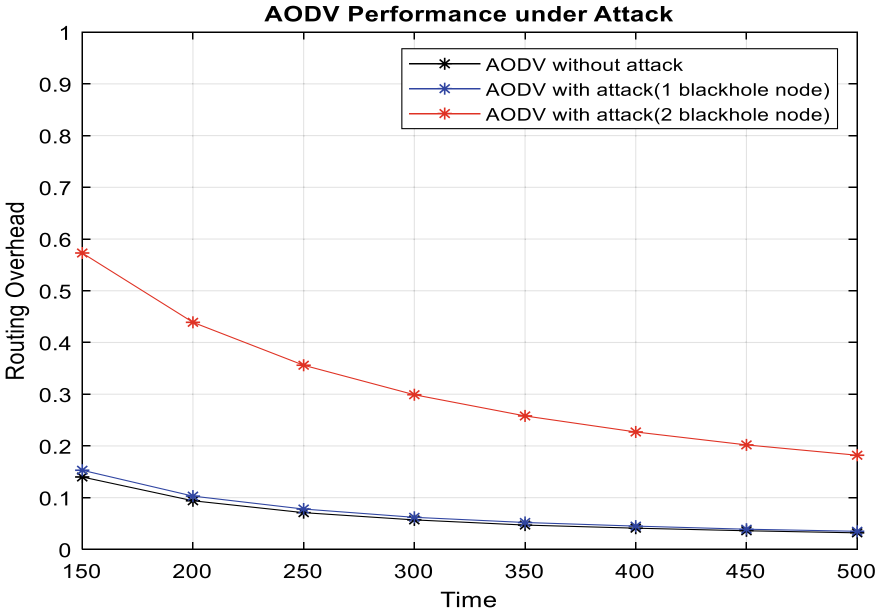


Fig. 9 AODV under attack—routing overhead versus simulation time

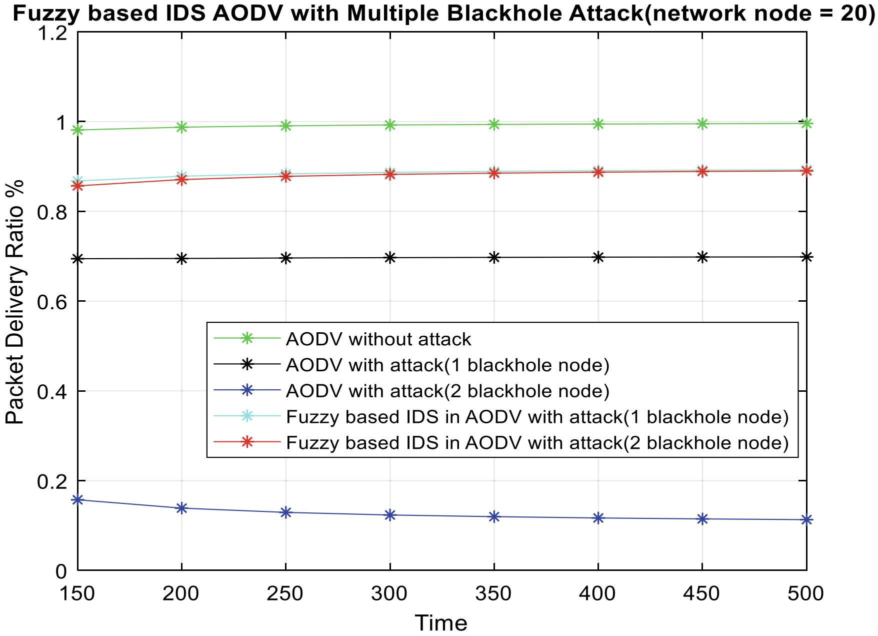


Fig. 10 FIDS performance under attack—PDR versus simulation time

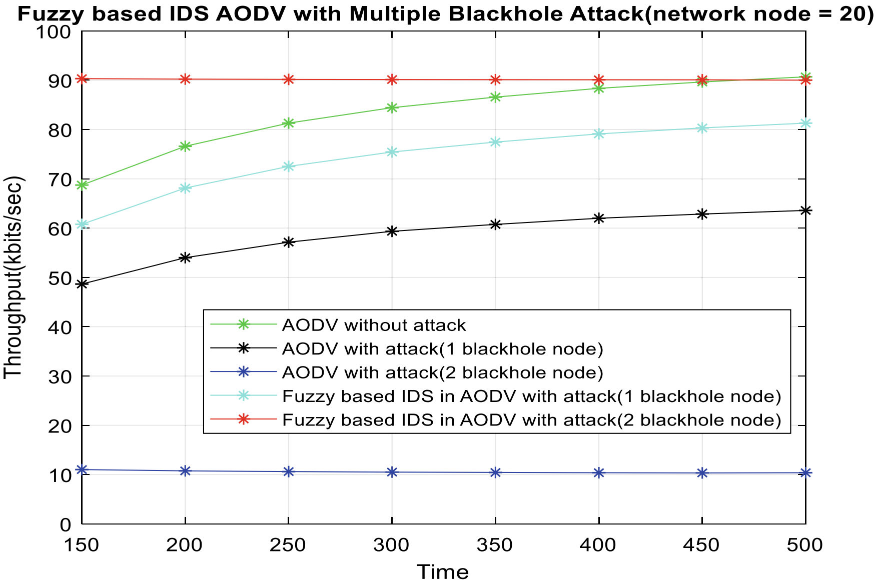


Fig. 11 FIDS performance under attack—throughput versus simulation time

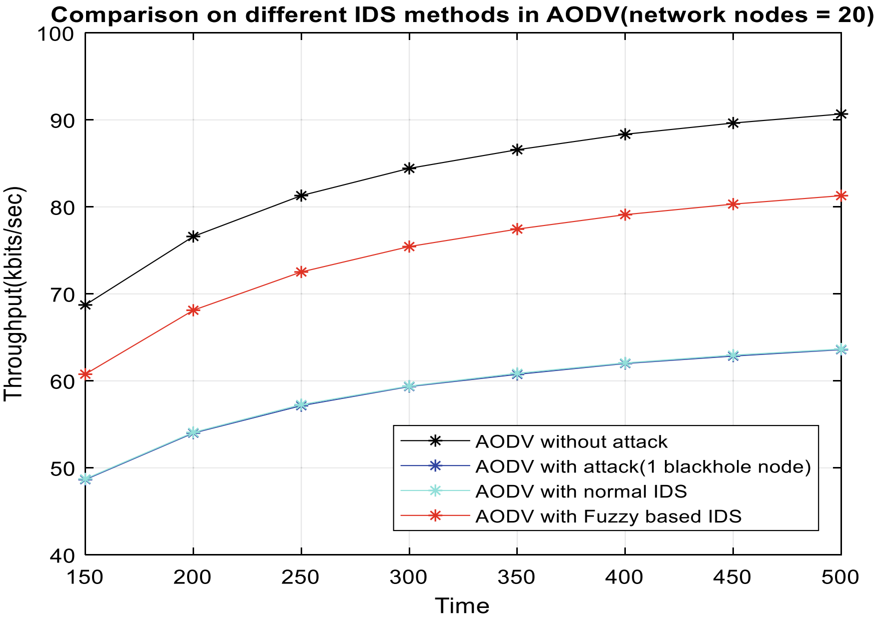


Fig. 12 Comparison on different IDS—throughput versus simulation time

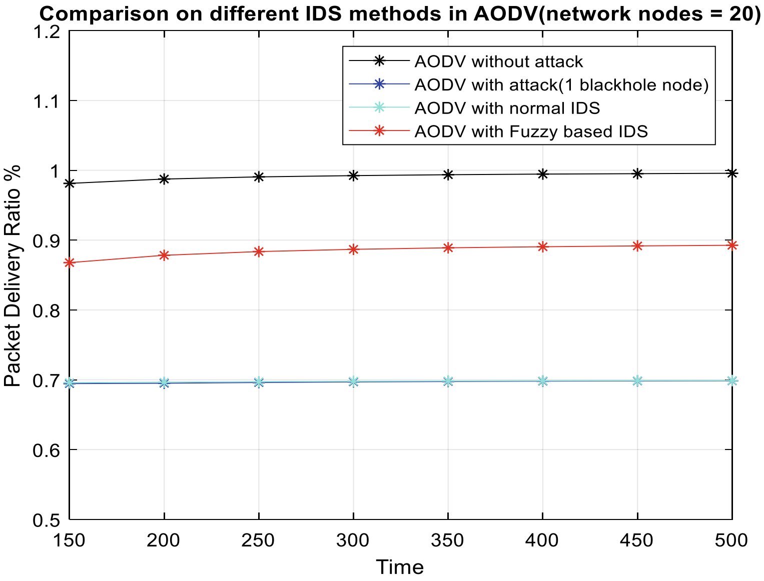


Fig. 13 Comparison on different IDS—PDR versus simulation time

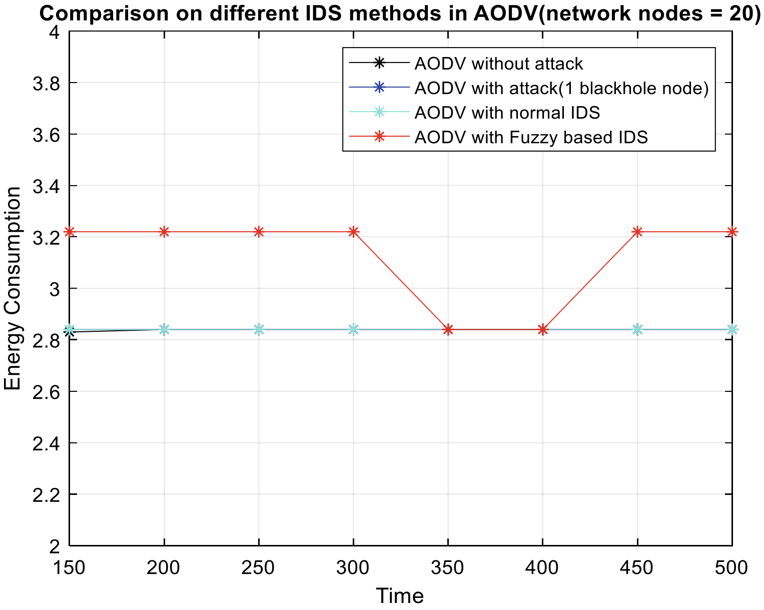


Fig. 14 Comparison on different IDS—energy consumption versus simulation time

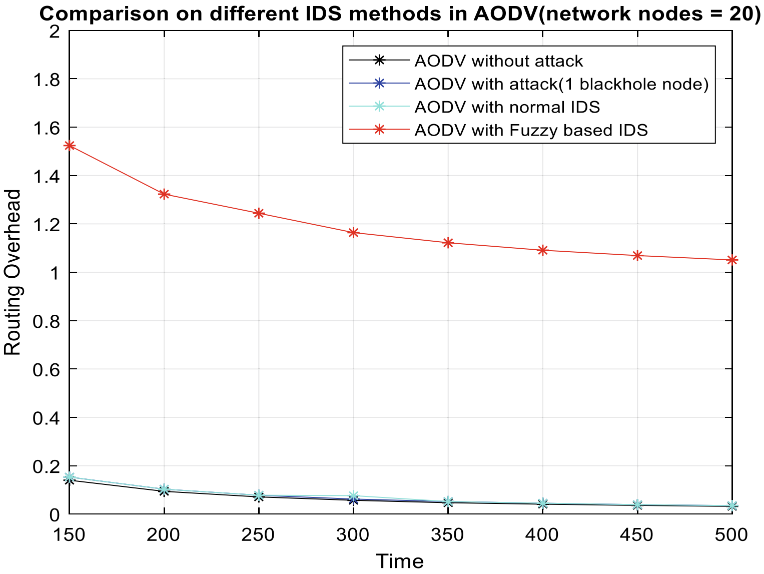


Fig. 15 Comparison on different IDS—routing overhead versus simulation time

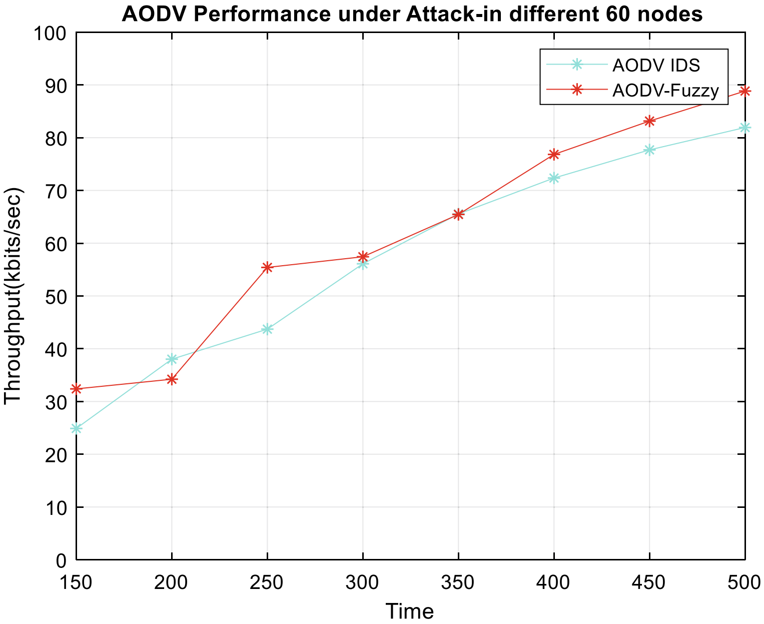


Fig. 16 Comparison on IDS with different node numbers—throughput versus simulation time

Moreover, in the presence of multiple blackhole attacks, similar results have been observed. In addition to this, the performance of FIDS is compared with the another IDS which was proposed by author Dokurer [20]; here, it is named as normal IDS which works on the principle of ignoring the first established route to reduce the effects of the blackhole attack because blackhole node always responds with a fake reply without making delay.

The evaluation of the proposed FIDS has been carried out by calculating the performance metrics, i.e., throughput, packet delivery ratio, energy consumption and routing overhead in the Figs. 12, 13, 14 and 15, respectively. At each time, it is being compared with the normal IDS. It is observed that in the proposed FIDS has increased throughput and PDR which results in better network performance. However, slight increase in energy consumption and routing overload is found because computation processing is involved in FIDS working. Further, results are also validated with different number of nodes present in a network, i.e., 60 nodes. Similar results like better throughput as compared to normal IDS are recorded and presented in the following Fig. 16.

6 Conclusion

Although MANETs are more vulnerable to inside and outside attacks than conventional wired networks, they are increasingly being used in many applications because they provide low-cost mobile connectivity solutions. Researchers are constantly focusing on developing or evolving methods for preventing, detecting and response mechanism for MANETs. Fuzzy-based intrusion detection has been identified as a suitable technique for dynamic environment (i.e., MANETs) by various researchers. It emerges that, to secure a network against the unknown attacks, the fuzzy-based intrusion detection may be the appropriate technique to tackle attacks in MANETs. Here, in this work, its applicability in MANETs has been presented. An effective set of fuzzy rules for inferences is necessary to be identified by making use of the fuzzy rule learning strategies, which would contribute more effectively for detecting intrusion in MANETs. Here, under the scope of this paper, the fuzzy rules (*set of 16 rules*) have been proposed for the detection of blackhole attack in a network. These fuzzy rules are developed on three critical attributes of AODV which are rate of RREQ, RREP and sequence number. Subsequently, the proposed FIDS has been evaluated for the detection of blackhole attack using different simulation parameters of MANETs. And it is observed that fuzzy logic-based intrusion detection systems performs better than the other method-based intrusion detection methods. However, here in the proposed solution, only limited features have been taken into account for the detection of blackhole attack ONLY, to use this model for different attacks, more features are required to be added for accuracy in detection of attack that may results in more computation processing on node which limits the operational philosophy of MANETs. As a result, IDS in MANETs remain a demanding, complex and challenging subject for researchers.

References

1. Ramanathan, R., Redi, J.: A brief overview of ad hoc networks: challenges and directions. IEEE Commun. Magaz. **40**(5) (2002)
2. Vydeki, D., Bhuvaneswaran, R.S.: Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks. J. Comput. Sci. **9**(4), 521–525, ISSN: 1549-3636 (2013)
3. Poongothai, T., Duraiswamy, K.: Cross layer intrusion detection system of mobile ad hoc networks using feature selection approach. Wseas Trans. Commun. **13** (2014)
4. Introduction to fuzzy logic. http://www.francky.me/doc/course/fuzzy-logic.pdf
5. Lectures on Fuzzy. http://ce.sharif.edu/courses/92-93/1/ce9571/resources/root/Lectures/Lecture6&7.pdf
6. Zadeh, L.A.: Fuzzy logic—computing with words. IEEE Trans. Fuzzy Syst. **4**, 103–111 (1996)
7. Ruchi, M., Reddy, B.V.R.: Taxonomy of machine leaning based anomaly detection and its suitability. In: International Conference on Computation Intelligence and Data Science (ICCIDS 2018), Procedia Computer Science, vol. 132, pp. 1842–1849, Elsevier (2018)
8. Garcia Teodora, P., Diaz Verdejo, J., MaciaFarnandez, G., Vazquez, E.: Anomaly based network intrusion detection: techniques, systems and challenges. J. Comput. Secur. **28**(1), 18–28 (2009)
9. Shelly, X.W., Wolfgang, B.: The use of computational intelligence in intrusion detection systems: a review. Appl. Soft Comput. Appl. Soft Comput. **10**, 1–35 (2010)
10. Izakian, H., Pedrycz, W.: Agreement-based fuzzy c-means for clustering data with blocks of features. Neurocomputing **127**, 266–280 (2014)
11. Animato, M.E., Kim, H., Kim, K.: Another fuzzy anomaly detection system based on ant clustering algorithm. Kumamoto, Japan (2016)
12. Mkuzangwe, N.N.P., Nelwamondo, F.V.: A fuzzy logic based network intrusion detection system for predicting the TCP SYN flooding attack. Springer International Publishing, Part II, LNAI 10192, pp. 14–22 (2017)
13. Kulbhushan, Singh, J.: Fuzzy-logic-based intrusion detection system against blackhole attack AODV in Manet. IJCA Special issue on "Network Security and Cryptography", vol. NSC, no. 2, pp. 28–35 (2011)
14. Mandal, S.N., Pal Choudhury, J., Bhadra Chaudhuri, S.R.: In search of suitable fuzzy membership function in prediction of time series data. Int. J. Comput. Sci. Issues **9**(3), 3 (2012)
15. Chaudhary, A., Kumar, A., Tiwari, V.N.: A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs. IEEE Int. Conf. Optimiz. Reliab. Inf. Technol. 178–181 (2014)
16. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Proceedings 2nd IEEE Workshop Mobile Computer System and Applications, pp. 90100 (1999)
17. Ning, P., Sun, K.: How to misuse AODV: a case study of inside attacks against mobile ad-hoc routing protocols. In: Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY (2003)
18. Rajya Lakshmi, G.V., Anusha, K.: Detection of anomaly network traffic for mobile ad-hoc network using fuzzy logic. Int. J. Emerg. Res. Manag. Technol. (2013)
19. Chaudhary, A., Tiwari, V.N., Kumar, A.: Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks. BIJIT—BVICAM s Int. J. Inf. Technol. **6**(1) (2014)
20. Dokurer, S., Ert, Y.M., Acar, C.E.: Performance analysis of adhoc networks under blackhole attacks. In: Southeast Con, 2007, Proceedings IEEE, pp. 148–153 (2007)