Defending Jellyfish Attack in Mobile Ad hoc Networks via Novel Fuzzy System Rule: Proceedings of ICDMAI 2018, Volume 2

Chapter *in* Advances in Intelligent Systems and Computing · January 2019

DOI: 10.1007/978-981-13-1274-8_33

CITATIONS
13

READS
207

3 authors:

Suseendran G.
VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES (VISTAS), CHE…
149 PUBLICATIONS **1,039** CITATIONS
SEE PROFILE

Chandrasekaran Ekambaram
Veltech .Rangarajan Dr.Sakunthala R&D Institute of Science and technologe, Avad…
39 PUBLICATIONS **168** CITATIONS
SEE PROFILE

Anand Nayyar
Duy Tan University
581 PUBLICATIONS **12,403** CITATIONS
SEE PROFILE

Defending Jellyfish Attack in Mobile Ad hoc Networks via Novel Fuzzy System Rule

G. Suseendran, E. Chandrasekaran and Anand Nayyar

Abstract Security in mobile ad hoc environment is the most concerned research issue which is focused in the proposed research methodology by introducing authenticated routing based attack injection and detection framework using genetic fuzzy rule based system (AR-AIDF-GFRS). This assures both the successful detections of attacks present in the environment and secured routing by using trusted nodes. Here, initially, jellyfish attack is injected into the MANET environment. This attack is detected by genetic fuzzy based rule system which would generate rules based on which attack would be identified. And then to ensure the secured routing, trust evaluation of nodes is done by ant colony based trust evaluation method (ACTEM). This method selects the optimal nodes which are trusted in nature for establishing the route path. The overall evaluation of the proposed research method is done in NS2 simulation environment which proves that AR-AIDF-GFRS can outperform the existing research method by accurately identifying attacker nodes.

Keywords Jellyfish attack · Fuzzy rule · Secured routing · Trust value
Fuzzy rules · Quality of service

G. Suseendran (✉)
Department of Information Technology, School of Computing Sciences,
VELS Institute of Science, Technology & Advanced Studies (VISTAS),
Chennai 600117, Tamil Nadu, India
e-mail: suseendar_1234@yahoo.co.in

E. Chandrasekaran
Department of Mathematics, Veltech Dr. RR & Dr. SR University,
Chennai, India
e-mail: e_chandrasekaran@yahoo.com

A. Nayyar
Graduate School, Duy Tan University, Da Nang, Vietnam
e-mail: anandnayyar@duytan.edu.vn

V. E. Balas et al. (eds.), *Data Management, Analytics and Innovation*,
Advances in Intelligent Systems and Computing 839,
https://doi.org/10.1007/978-981-13-1274-8_33

1 Introduction

The 21st century of advancements and innovations open for everybody, where there no evident limits between the usefulness of the gadgets the portable specially appointed systems administration (MANETs) assume huge part. MANETs have turned out to be a standout among the most predominant zones of research in the current years and as a result of the difficulties, it postures to the related calculations. MANET is an arrangement of remote versatile hubs that progressively self-compose in the subjective and transitory system topologies.

MANET has become a rising research area with many practical applications. Its technology provides a flexible way to set up communications in situations with geographical constraints that demand distributed networks without any centralized authority or fixed base station, such as disaster relief, emergency situations (rescue team), battlefield communications, conference rooms, and military applications [1]. Compared to the traditional wireless and wired networks, MANET is prone to varied security vulnerabilities and attacks because of its features in terms of no centralized authorities, distribution cooperation, open and shared network wireless medium, severe resource restriction, and high dynamic nature of network topology. The factors that attracted attraction of researchers around MANETs are: Self-configuration and Self-maintenance. Another unique feature of MANETs that poses security threats is its unclear defense line, i.e., no built-in security.

MANETs doesnt have committed switches, and its hubs generally work by sending the bundles to each other accordingly having no security in the correspondence, giving access to both true blue clients and aggressors [2]. For instance, hub S can speak with hub D by utilizing the most brief way S–A–BD as appeared in Fig. 1 (the dashed lines demonstrate the immediate connections between the hubs). In the event that hub A moves out of hub S range, hub A needs to locate an option course to hub D (S–C–EB–D). Accordingly, security in MANETs is the most essential worry for the fundamental usefulness of the system. The accessibility of system administrations, privacy, and trustworthiness of the information can be accomplished by guaranteeing that security issues have been met. MANETs regularly experience the ill effects of security assaults in view of its highlights like

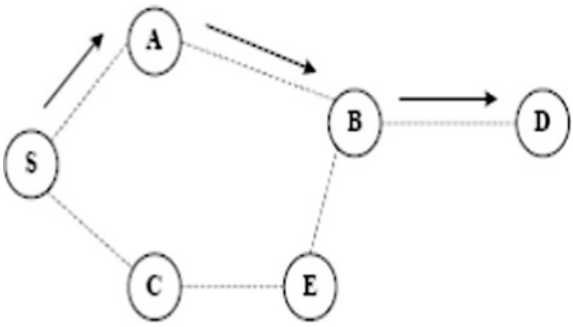

Fig. 1 Communication between nodes in MANETs

open medium, progressive topology change, absence of focal checking and administration, helpful calculations, and no unmistakable barrier system. These elements change the combat zone circumstances for MANETs against all sorts of security dangers [3].

A MANET is more open to these sorts of assaults as correspondence depends on shared trust between the hubs; there is no essential issue for arranging administration, no approval office, energetically changing topology, and restricted assets.

The main objective of the proposed method is to implement flexible network structure for MANETs environment by accurately detecting the attacks and preventing the unwanted packet dropouts. This is ensured by injecting jellyfish attack into the environment which is detected via genetic fuzzy rule based system which identifies the attack presence. The prevention of attack is done via trust-aware routing in which routing is performed via trustworthy nodes in the environment by proper means of authentication before establishing the routing path.

1.1 Structure of the paper

The rest of the paper is organized as follows: Section 2 outlines literature review of varied proposed methodologies by other researchers. Section 3 highlights the proposed research method along with suitable examples. Section 4 covers simulation based performance evaluation of proposed method and compares the novel proposed method with existing techniques. Section 5 concludes the paper with future scope.

2 Related Works

In this segment, shifting-related research strategies have been examined in detail in light of their working methodology regarding assault identification. Andel et al. [4] have characterized the undetectable hub assault and turned out to be not quite the same as the current assaults (man in the center, disguising, and wormhole) and set up its uniqueness. The authors characterized it as, in any convention that relies upon recognizable proof for any usefulness, any hub that successfully takes an interest in that convention without uncovering its personality is an imperceptible hub, and the activity and convention effect is named as INA. Considering the impacts of INA on various directing conventions, authors demonstrated it as unsolvable assault until now.

SAODV directing convention is utilized to avert against dark gap assault; however, it requires overwhelming weight encryption calculation [5]. SAR can be utilized to safeguard against dark gap assaults. In SAR, it needs intemperate encryption and decoding at each jump. ARAN can be utilized to guard against pantomime and renouncement assaults. It may not protect against validated egotistical hubs. Security convention SEAD is utilized against change assaults [6].

Di Crescenzo et al. [7] secure the administration disclosure stage by utilizing a safe different ruling set creation convention and the administration arrangement stage by utilizing a novel sort of edge signature plot. The two conventions address novel security objectives and are of free enthusiasm as they can discover applications to different ranges, most strikingly, the development of a conveyed and survivable open key framework in MANET.

Kim et al. [8] utilized the transmission control convention (TCP) to give solid information regarding transmission that has been performed with the end goal of smooth mix with the wired web. The creators propose their TCP-Vegas-impromptu convention, which is made mindful of RCs and utilizes the right BaseRTT esteems. Lee et al. [9] concluded that system coding in mix with single-bounce correspondence permits P2P document sharing frameworks in MANET to work in a more effective way and cause the frameworks to run without any hiccup. For example, dynamic topology and irregular network and in addition different issues that have been ignored in past MANET P2P explores, for example, tending to, hub/client thickness, non-helpfulness, and temperamental channel.

El Defrawy et al. [10] address various issues emerging in suspicious area-based MANET settings by planning and breaking down a protection saving and secure connection state based steering convention (Caution). Alert uses hubs' present areas to safely disperse and develop topology depictions and forward information. With the guide of cutting-edge cryptographic strategies (e.g., amass marks), caution gives both security and protection highlights, including hub confirmation, information trustworthiness, secrecy, and immovability (following protection). Zhao et al. [11] proposed a hazard mindful reaction instrument to methodically adapt to the distinguished steering assaults. Our hazard mindful approach depends on a broadened Dempster–Shafer numerical hypothesis of proof presenting a thought of significance factors [13].

3 Secured Routing with the Concern of Attacks

1. Versatile specially appointed system is one of the most regular impromptu systems with part of the issues identified with blockage and steering. It is one of the answers to secure the transmission over the system. Security angles assume a critical part in application situations given the vulnerabilities innate in remote specially appointed system administration from the very truth that radio correspondence happens (e.g., in strategic applications) to steer, man in the center and expound information infusion assaults. Security has turned into an essential worry keeping in mind the end goal to give ensured correspondence between versatile hubs in a threatening domain. The proposed framework is going to plan an interruption location framework to identify the jellyfish assault infused into the framework [14].
2. This identification framework depends on fluffy rationale. An IDS framwork is proposed in which change is made via utilization of two variables, i.e., Bundle misfortune rate and information rate. The two elements utilize fluffy rationale

which is criticial thinking control framework. Fluffy rationale gives a straightforward approach to touch base at a clear conclusion in light of obscure, questionable, loud, or missing data. We proposed a calculation which depends on above elements. In this calculation, initially, we characterize the system with N number of hubs and we set source hub to S and goal hub D and after that, we let the currect hub as source hub. We rehash the means until the point when the current hub is not equivalent to goal hub. In this now, we discover the rundown of neighboring hubs of current hub. We distinguish the parameters of each neighbor hub, i.e., bundle misfortune and information rate.

3.1 Jellyfish Attack Injection

Jellyfish assault is one of the refusals of administration assault and furthermore a kind of inactive assault which is hard to recognize. It produces delay before the transmission and gathering of information parcels in the system. Applications, for example, HTTP, FTP, and video conferencing, are given by TCP and UDP. Jellyfish assault irritates the execution of the two conventions. Jellyfish assaults are focused against shut circle streams. TCP has surely understood vulnerabilities to postponement, drop, and misarrange the parcels. Because of this, hubs can change the arrangement of the bundles likewise drop a portion of the information parcels. The jellyfish aggressor hubs completely obey convention rules, and henceforth this assault is called as uninvolved assault.

This assault which takes after all TCP rules has trademark in which jellyfish hub lessens the throughput, by dropping some of the bundles or deferring a few parcels or reordering a few parcels. At the point when a malignant hubs dispatch sending dismissal assaults, it likewise may follow all steering systems. A malevolent hub propelling jellyfish assaults may keep dynamic in both course finding and bundle sending with a specific end goal to keep it from identification and conclusion, yet the pernicious hub can assault the movement by means of itself by reordering parcels, dropping parcels intermittently, or expanding nerves. The jellyfish assault is particularly destructive to the TCP movement in that agreeable hubs can scarcely separate these assaults from the system blockage. It focuses on TCP's blockage control component.

As appeared in Fig. 2, hub JF is a jellyfish, and hub S begins to speak with hub D after a way by means of the jellyfish hub is built up. At that point, the dissent of administration assaults propelled by hub JF will cause bundle misfortune and sever the correspondences between hubs S and D at the end. In our work, jellyfish occasional assault has been infused into the MANET condition for the enhanced system execution.

Intermittent dropping is conceivable due to snidely picked period by the evil hub. This sort of occasional dropping is conceivable at hand-off hubs. Assume that blockage misfortunes drive a hub to drop $\alpha\%$ of bundles. Presently, consider that

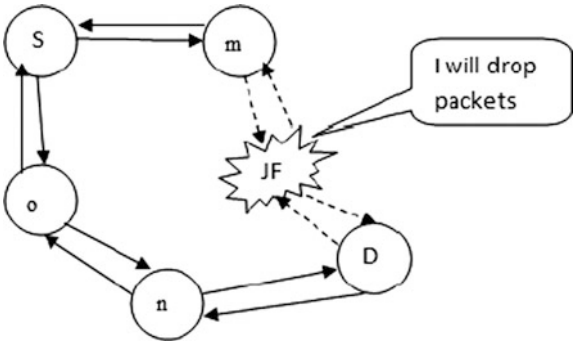

Fig. 2 Jellyfish attack scenario

the hub drops $\alpha\%$ of parcels intermittently, then TCP's throughput might be lessened to almost zero notwithstanding for little esteems.

3.2 Genetic Fuzzy Based Attack Detection

This technique involves the detection of attacker levels in the network layers using fuzzy logic technique. The following steps determine the fuzzy rule based interference:

- Fuzzification: This involves obtaining the crisp inputs from the selected input variables and estimating the degree to which the inputs belong to each of the suitable fuzzy sets.
- Rule evaluation: The fuzzified inputs are taken and applied to the antecedents of the fuzzy rules. It is then applied to the consequent membership function.
- Aggregation of the rule outputs: This involves merging of the output of all rules.
- Defuzzification: The merged output of the aggregate output fuzzy set is the input for the defuzzification process and a single crisp number is obtained as the output.

Initially, the fuzzy logic engine analyzes each layer, namely, the MAC layer, physical layer, and routing layer for the detection of abnormal behaviors. Then, the information gathered are stored in an attack database whose format is shown in Table 1.

Table 1 Attack database

Layer	Intrusion frequency (F)	Probability of successful attack (P)	Severity (S)
MAC Layer	F_1	P_1	S_1
Physical layer	F_2	P_2	S_2
Routing layer	F_3	P_3	S_3

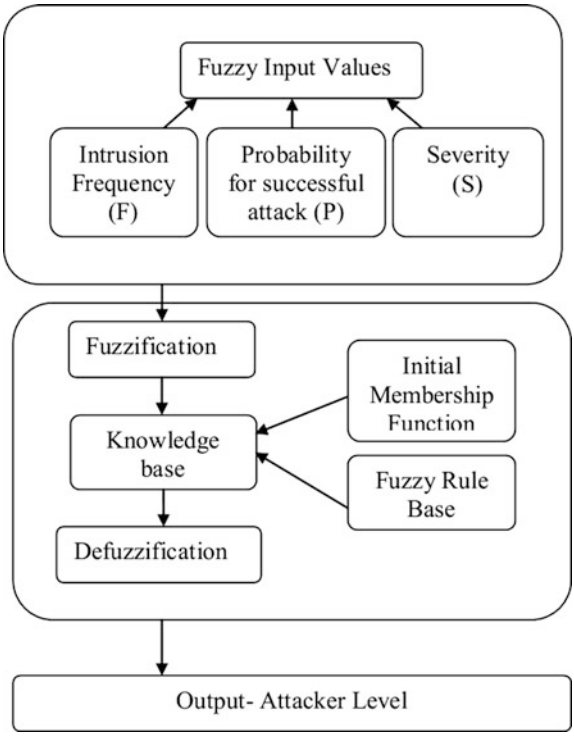

Fig. 3 Fuzzy interference system

The parameters in the table are: Interruption recurrence (*F*). It is characterized as the assault force against the layer that is liable to checking. Its unit is in assaults/unit time.

Likelihood for effective assault (*P*): It portrays the strategy by which the aggressor handles to defeat the proactive controls. It varies in the range of (0–1).

Severity (*S*): It depicts the effect of an assault on the layer. The fluffy derivation framework is represented utilizing Fig. 3.

3.2.1 Fuzzification

This includes fuzzification of information factors, for example, interruption recurrence (*F*), likelihood of effective assault (*P*), and seriousness (*S*), and these data sources are given a degree to suitable fluffy sets. The fresh information sources are blend of *F*, *P,* and *S*. We take two potential outcomes, high and low for *F*, *P,* and *S*. Figures 4, 5, 6, and 7 demonstrate the participation work for the information and yield factors. Because of the computational proficiency and uncomplicated recipes, the triangulation capacities are used which are generally used for progressive applications. Likewise, a positive effect is offered by this outline of enrollment work.

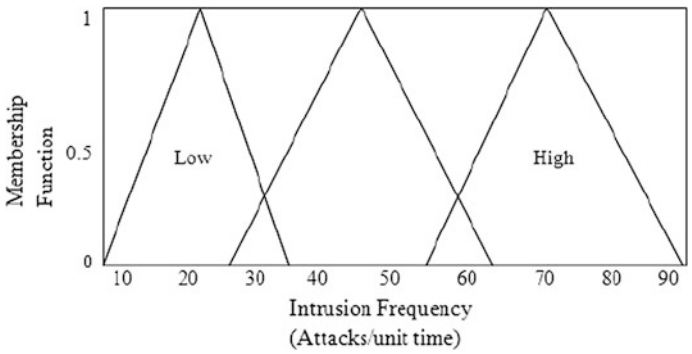

Fig. 4 Membership function of intrusion frequency

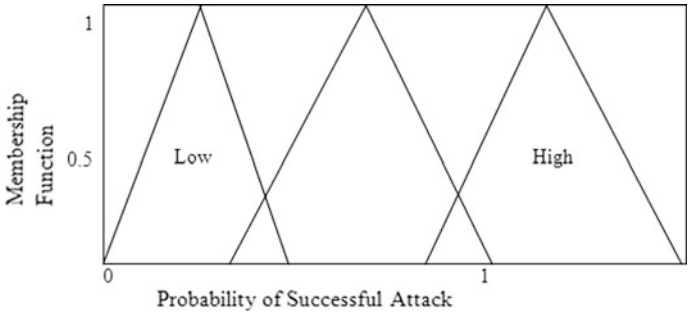

Fig. 5 Membership function of successful attack probability

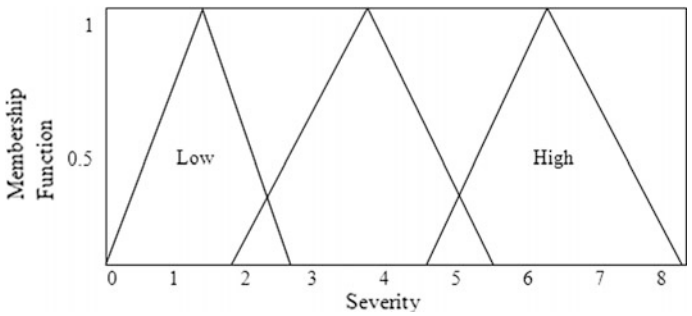

Fig. 6 Membership function of severity

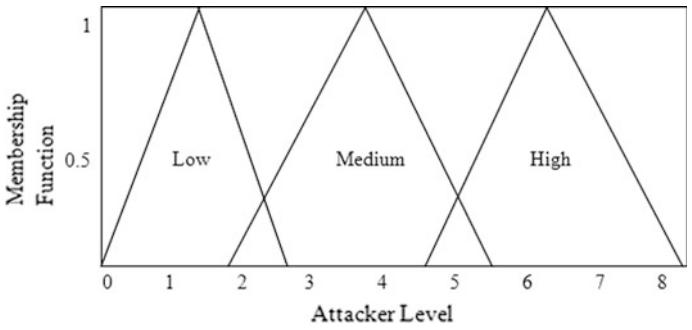

Fig. 7 Membership function of attacker level

Table 2 Fuzzy rules for the determining output

S. No	*F*	*P*	*S*	AL
1.	Low	Low	Low	Low
2.	Low	Low	High	Medium
3.	Low	High	Low	Medium
4.	Low	High	High	High
5.	High	Low	Low	Medium
6.	High	Low	High	High
7.	High	High	Low	High
8.	High	High	High	High

In Table 2, *F*, *P,* and *S* are given as sources of info and the yield speaks to the level of aggressor (AL) in every hub in the individual layer. In light of the aggressor level, the trust estimation of noxious hub is decreased (Clarified in Sect. 3.1). The eight fluffy sets are characterized with the blends introduced in Table 2.

Table 2 shows the composed fluffy induction framework. This outlines the capacity of the deduction motor and strategy by which the yields of each manage are consolidated to create the fluffy choice.

In the event that *F*, *P,* and *S* are low, at that point the attack level is low.
In the event that *F* and *P* are low, *S* is high, at that point the attack level is medium.
In the event that *F* and *S* are low, *P* is high, at that point the attack level is medium.
In the event that *F* is low, *P* and *S* are high, at that point the attack level is high.
In the event that *F* is high, *P* and *S* are low, at that point the attack level is medium.
In the event that *F* and *S* are high, *P* is low, at that point the attack level is high.
In the event that *F* and *P* are high, *S* is low, at that point the attack level is high.
In the event that *F*, *P,* and *S* are high, at that point the attack level is high.

3.2.2 Genetic-Based Rule Selection to Reduce Computation Overhead

An overabundance number of standards may not deliver great execution and it makes hard to comprehend the model conduct. To choose and tune a minimized arrangement of fluffy affiliation rules with high characterization precision from the manage base, a GA is utilized, where rules depend on the semantic two-tuple portrayal. The emblematic interpretation parameter of a semantic term is a number inside the interim [− 0.5, 0.5) that communicates the area of a mark when it is moving between its two parallel names. In the event that S is set of marks speaking to a fluffy parcel, at that point, there is a couple (S_i, αi), $S_i \in S$, $\alpha i \in [-0.5, 0.5)$. The CHC approach makes utilization of an interbreeding aversion instrument and a restarting procedure to energize assorted variety in the populace, rather than the notable transformation administrator. This inbreeding aversion instrument will be considered keeping in mind the end goal to apply the hybrid administrator, i.e., two guardians are crossed if their hamming separation isolated by 2 is more than a foreordained edge L. This edge esteem is instated as the most extreme conceivable separation between two people (the quantity of non-coordinating qualities in the chromosome) isolated by 4. Following the first CHC plot, L is decremented by 1 when there are no new people in the populace in one era. Keeping in mind the end goal to make this technique free of the quantity of qualities in the chromosome, for this situation, L will be decremented by $\varphi\%$ of its underlying worth (where φ controlled by the client, typically 10%). At the point when L is beneath zero, the calculation restarts the populace. Plan of this GA is as per the following:

Codification and beginning quality pool: To consolidate the govern determination with the worldwide horizontal tuning, a twofold coding plan for both run choice CS and sidelong tuning CT is utilized. For the CS part, every chromosome is a parallel vector that decides when a govern is chosen or not (alleles "1" and "0" individually).

Chromosome assessment: To assess a decided chromosome punishing countless, arrangement rate is figured and the wellness work is expanded. This capacity must be in the agreement with the system of imbalanced datasets. Along these lines, the normal of total of effectively ordered preparing designs by the standards in the chromosome part CS is utilized as wellness work.

$$\text{Fitness}(C) = \frac{\sum_{i=1}^{N_{\text{rs}}} \text{NCP}(R_i)}{N_{\text{rs}}}$$

where N_{rs} is the number of rules in the rule set and NCP(Ri) is the number of correctly classified training. In the event that there is no less than one class without chose rules or if there are no secured designs, the wellness estimation of a chromosome will be punished with the quantity of classes without choosing rules and the quantity of revealed designs.

Hybrid administrator: The hybrid administrator will rely upon the chromosome part where it is connected. In the CS part, the half-uniform hybrid plan (HUX) is utilized. The HUX hybrid precisely trades the mid of the alleles that are diverse in the guardians (the qualities to be crossed are arbitrarily chosen from among those

that are distinctive in the guardians). This administrator guarantees the most extreme separation of the posterity to their folks (investigation).

Restarting approach: To make tracks in an opposite direction from neighborhood optima, a restarting approach has been utilized. For this situation, the best chromosome is kept up, and the remaining are created aimlessly. The restart technique is connected when the limit esteem L is beneath zero, which implies that every one of the people existing together in the populace is fundamentally the same.

3.2.3 Defuzzification

The system by which a fresh esteems are removed from a fluffy set as a portrayal esteem is alluded to as defuzzification. The centroid of region plot is mulled over for defuzzification amid fluffy basic leadership process. The recipe (1) portrays the defuzzifier strategy.

$$\text{Fuzzy\_cost} = \left[\sum_{\text{all rules}} z_i * \lambda(z_i)\right] / \left[\sum_{\text{all rules}} \lambda(z_i)\right]$$

where fuzzy_cost is utilized to determine the level of basic leadership, z_i is the fluffy all tenets, and variable $\lambda(z_i)$ is its enrollment work. The yield of the fluffy cost work is adjusted to fresh an incentive according to this defuzzification technique.

3.3 Secured Routing Using Trusted Nodes

In this system, we consider swarm insight in view of insect state enhancement (ACO) method for performing confirmed directing. This procedure includes two insect operator to be specific forward subterranean insect (FA) and in reverse insect (BA) [12]. The means associated with this calculation are as per the following.

Stage 1 When source (S) needs to transmit the information parcel to goal (D), it dispatches FA with a limit put stock in esteem (T_{th}) connected with it.

Stage 2 The versatility of FA going to every N_i depends on probabilistic choice run shown in [14].

$$P_r(N_i, S) = \begin{cases} \frac{a(N_i,S)^{\xi}.[b(N_i,S)]^{\sigma}}{\sum_{N_i \in N_n}[s(N_1,S)]^{\xi}.[b](N_i.S)^{\sigma}} & \text{if } r0, \text{otherwise} \\ 0, \text{otherwise} \end{cases}$$

where $a(N_i, S)$ i represents pheromone value.
b (N_i, S_o) represents the bandwidth related heuristic value.
N_{R} represents the receiver node.
RT (N_i) represents the routing table for N_i.

ξ and σ are the parameters that control the relative weight of the pheromone and heuristic value, respectively.

Step 3 FA travels through N_i using the control portrayed in stage 2 and confirms whether the trust estimation of the went to hub is more prominent than the trust edge esteem.

If $T_i > T_{\text{th}}$, then
FA continues its path and keeps updating the routing table until it reaches D
Else if $T_i < T_{\text{th}}$ Then
The node is omitted from getting updated in the routing table.
End if

Step 4 Each FA deposits a quantity of pheromone ($\Delta\tau^u(r)$) in the visiting N_i as per the following equation:

$$\Delta\tau^u(r) = \frac{1}{X_s^u(r)}$$

where $X_s^u(r)$ represents the total number of N_i visited by FA during its tour at iteration r and $u = 1, 2, \ldots, n$.

Step 5 At the point when FA achieves D, BA is produced and the whole data gathered by FA is exchanged for BA.

Step 6 The BA at that point takes an indistinguishable way from that of its relating forward subterranean insect, yet the other way. It refreshes the pheromone table with the confide in estimation of the separate N_i.

Step 7 Once S gets the BA, it gathers the directing data about all N_i along every way from its refreshed pheromone table.

Step 8 From the gathered data, S picks the course with dependable hubs for information correspondence.

4 Experimental Results

This section enlists all simulation paramaters utilized for creating MANET scenario for evaluating the proposed methodology for combating Jellyfish attack. Ubuntu 17.04 is utilized as the working framework since it is easy to use which makes it simple to oversee. All the testing of the proposed method is performed on NS-2.35 simulator. In Table 3, we portray MANET parameters that are utilized as a part of this reenactment to quantify its execution and contrast it and distinctive conventions over a MANET organize. In the reproduction, we examine the connection between various MANET execution parameters regarding bundles' size.

Table 3 Parameters used in simulation

Parameter	Value
Operating system	Ubuntu 17.04
NS2-2 version	2.35
Channel type	Wireless channel
Number of nodes	100
Speed	3, 5, 7, 10, 20, 25
Data type	UDP
Simulation time	160 s
MAC protocol	MAC/802.11
Data packet size	100, 300, 500, 700, 800, 1000, 1500 and 2000
Area of simulation	700 * 700
Radio propagation model	Two-ray ground
Routing protocol	AODV/DSR

The proposed authenticated routing based attack injection and detection framework using genetic fuzzy rule based system (AR-AIDF-GFRS) is compared with the existing techniques like artificial bee colony (ABC), and memetic artificial bee colony (MABC) algorithm and performance is measured in terms of throughput, packet delivery ratio (PDR), end-to-end delay (E2E), routing efficiency, routing overhead (RO), and so on. The performance and results of the routing algorithm are as follows.

4.1 Throughput

The throughput is the number of bytes transmitted or received per second. The throughput is denoted by T,

$$\text{Throughput} = \text{received node/simulation time}$$

$$T = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \times 100\%$$

where N_i^r is the average receiving node for the ith application, N_i^s = average sending node for the ith application, and n = number of applications.

Figure 8 shows throughput comparison results of the attack detection algorithms such as ABC, MABC, and AR-AIDF-GFRS. From these figures, it concludes that the proposed AR-AIDF-GFRS based AD algorithm has improved throughput as compared to ABC and MABC. Based on Fig. 8, it is observed that AR-AIDF-GFRS performs better when the number of nodes increase and provides stable path from source to destination. It demonstrates that the number of Mbps transmitted from source to destination has increased when using AR-AIDF-GFRS based AD algorithm.

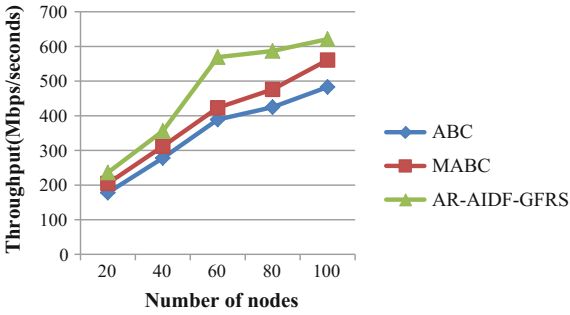

Fig. 8 Throughput comparison results of AODV protocol

Table 4 Throughput comparison results of AODV protocol

No. of nodes	Throughput (Mbps/Seconds)-AODV		
	ABC	MABC	AR-AIDF-GFRS
20	178	205	236
40	278	312	356
60	389	423	569
80	425	476	587
100	483	561	621
Avg	350.6	395.4	473.8

The values of these algorithms are tabulated in Table 4. Table 4 outlines average throughput results of AR-AIDF-GFRS based AD algorithm i.e. 473.8 Mbps/s for AODV protocol, 295.4 Mbps/s for MABC algorithm and 350.6 Mbps/s for ABC algorithm.

4.2 Packet Delivery Ratio (PDR)

It can be measured as the proportion of the received packets by the receiver node as compared to the packets transmitted by source node.

$$\text{PDR} = (\text{number of received packets / number of sent packets}) * 100$$

$$T = \frac{\sum_{i=1}^{n} \left(N_i^s - N_i^r\right)}{\sum_{i=1}^{n} N_i^s} \times 100\%$$

Figure 9 shows the packet delivery ratio of the proposed AR-AIDF-GFRS based AD algorithm, compared with existing optimization algorithms. Since the more number of the attacks has been detected, those routes are removed from original routing table. AODV increases the PDR of the proposed system and slightly decreases if the number of nodes increases. It shows that the number of packets transmitted from source to destination has increased for AR-AIDF-GFRS based AD

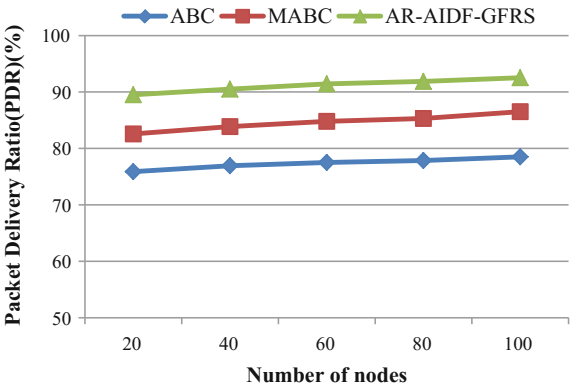

Fig. 9 PDR comparison results of AODV protocol

algorithm. The values of these algorithms are tabulated in Table 5. Table 5 shows that the proposed AR-AIDF-GFRS based AD algorithm produces average PDR results of 91.176% for AODV protocol, whereas the average PDR results of MABC and ABC are 84.61 and 77.344%, respectively.

4.3 Dropped Packets Ratio

It can be measured as the ratio of the number of packets that sent by the source node that fails to reach the destination node.

$$\text{Dropped packets} = \text{sent packets} - \text{received packets}$$

$$T = \sum_{i=1}^{n} \left(N_i^s - N_i^r\right) - \sum_{i=1}^{n} N_i^s$$

Figure 10 shows the drop packet ratio of the proposed AR-AIDF-GFRS based AD algorithm, compared with existing optimization algorithms. From the results, it concludes that the proposed AR-AIDF-GFRS based AD algorithm has less number of dropped packets as compared to other existing algorithms for both routing protocols, since the number of attacks detected in the proposed work is high. Those routes have been removed from original routing table and thereby reduces the number of dropped packets. It shows that the number of packets transmitted from source to destination has been higher. The values of these algorithms are tabulated in Table 6. Table 6 shows that the proposed AR-AIDF-GFRS based AD algorithm produces drop packets ratio results of 7.47% for 100 number of nodes in the AODV protocol, whereas the drop packets ratio results of MABC and ABC are 13.48 and 21.48%, respectively.

Table 5 PDR comparison results of AODV protocol

No. of nodes	Packet Delivery Ratio (PDR) (%)-AODV		
	ABC	MABC	AR-AIDF-GFRS
20	75.89	82.56	89.52
40	76.93	83.87	90.51
60	77.52	84.79	91.45
80	77.86	85.31	91.87
100	78.52	86.52	92.53
Avg	77.344	84.61	91.176

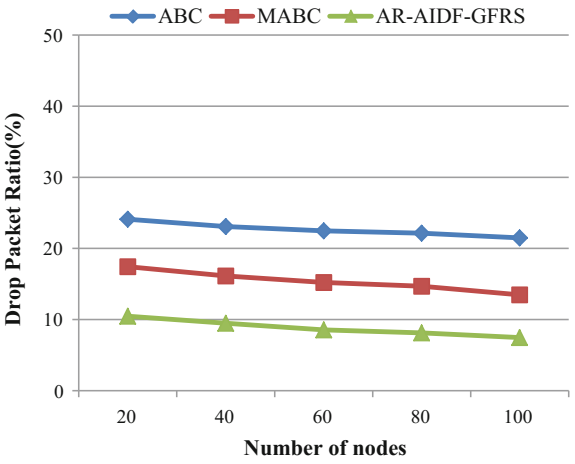

Fig. 10 Drop packets ratio comparison results of AODV protocol

4.4 End-to-End Delay (E2E)

It represents the time required to move the packet from the source node to the destination node.

$$\text{E-2-E delay [packetid]} = \text{received time [packetid]} - \text{sent time [packetid]}$$

The average E2E can be calculated by summing the times taken by all received packets divided by its total numbers

$$D = \frac{\sum_{i=1}^{n} d_i}{n}$$

where d_i = average end-to-end delay of node of ith application and n = number of application.

Figure 11 shows the E2E delay performance comparison results of proposed AR-AIDF-GFRS based AD algorithm, compared with other existing optimization algorithms. From the results, it concludes that the proposed AR-AIDF-GFRS based

Table 6 Average drop packets ratio comparison results of AODV protocol

No. of nodes	Drop packets ratio (%)-AODV		
	ABC	MABC	AR-AIDF-GFRS
20	24.11	17.44	10.48
40	23.07	16.13	9.49
60	22.48	15.21	8.55
80	22.14	14.69	8.13
100	21.48	13.48	7.47

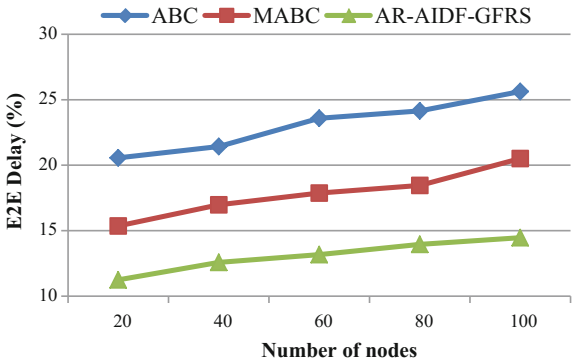

Fig. 11 End-to-end delay (E2E) comparison results of AODV protocol

Table 7 Average E2E delay comparison results of AODV protocol

No. of nodes	E2E Delay (%)-AODV		
	ABC	MABC	AR-AIDF-GFRS
20	20.56	15.36	11.25
40	21.43	16.98	12.58
60	23.58	17.87	13.17
80	24.15	18.46	13.95
100	25.63	20.51	14.47
Avg	23.07	17.836	13.084

AD algorithm has lesser E2E when compared to existing algorithms for both routing protocols. It shows that the number of packets transmitted from source to destination has been higher. The values of these algorithms are tabulated in Table 7. Table 7 shows that the proposed AR-AIDF-GFRS based AD algorithm produces average E2E delay of 13.084% for AODV protocol, whereas the average E2E delay results of MABC and ABC are 17.836 and 23.07%, respectively.

5 Conclusion

In this work, detecting a malicious node and launching new optimization algorithm may lead to serious security concerns. The proposed scheme uses new method, namely, authenticated routing based attack injection and detection framework using genetic fuzzy rule based system (AR-AIDF-GFRS). The proposed research assures successful detection of Jellyfish attack and secured routing via trusted nodes. In this work, initially, jellyfish attack would be injected into the MANET environment. This attack would be detected by introducing genetic fuzzy based rule system which would generate various number of rules based on which attack would be identified. And then to ensure the secured routing without involvement of intruders, in this work trust evaluation of nodes is done by using ant colony based trust evaluation method (ACTEM). The method select the optimal nodes from the MANET environment which is more trusted in nature for establishing the route path. The overall evaluation of the proposed method i.e. AR-AIDF-GFRS is done using NS-2.35 simulator and results state that the proposed method outshines in every aspect in terms of performance as compared to existing algorithms. In future scenario, different attacks can be considered for improving the network performance. In addition to that attacks, prevention mechanism can be introduced to avoid the network failure and unwanted computation overhead.

References

1. Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine, 40,* 70–75.
2. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications, 11,* 38–47.
3. Karpijoki, V. (2000, December). Security in ad hoc networks. In *Proceedings of the Helsinki University of Technology, Seminars on Network Security*, Helsinki, Finland.
4. Andel, T. R., & Yasinsac, A. (2007). The invisible node attack revisited. *Proceedings of IEEE SoutheastCon, 2007,* 686–691.
5. Hu, Y., Perrig, A., & Johnson, D. (2002). Ariadne: A secure on-demand routing for ad hoc networks. In *Proceedings of MobiCom 2002*, Atlanta.
6. Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. In *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM)*, Boston.
7. Di Crescenzo, G., Telcordia Technol, N. J., Ge, R., & Arce, G. R. (2006). Securing reliable server pooling in MANET against byzantine adversaries‖. *IEEE Journal on Selected Areas in Communications, 24,* 357–369.
8. Kim, D., Bae, H., & Toh, C. K. (2007). Improving TCP-Vegas performance over MANET routing protocols. *IEEE Transactions on Vehicular Technology, 56*(1), 372–377.
9. Lee, U., Park, J.-S., Lee, S.-H., Ro, W. W., Pau, G., & Gerla, M. (2008). Efficient peer-to-peer file sharing using network coding in MANET. *IEEE Journal on Communications and Networks, 10*, 422–429.
10. El Defrawy, K., & Tsudik, G. (2010). ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Journal on Mobile Computing, 10*, 1345–1358.

11. Zhao, Z. Hu, H., Ahn, G.-J., & Wu, R. (2011). Risk-aware mitigation for MANET routing attacks. *IEEE Journal on Dependable and Secure Computing, 9*, 250–260. (Security Eng. for Future Comput. Lab., Arizona State Univ., Tempe, AZ, USA).
12. Kaur, M., Sarangal, M., & Nayyar, A. (2014). Simulation of jelly fish periodic attack in mobile ad hoc networks. *International Journal of Computer Trends and Technology (IJCTT)*, *15*.
13. Kaur, M., & Nayyar, A. (2013). A comprehensive review of mobile adhoc networks (MANETS). *International journal of emerging trends & technology in computer science (IJETTCS), 2*(6), 196–210.
14. Kaur, M., Rani, M., & Nayyar, A. (2014, September). A novel defense mechanism via Genetic Algorithm for counterfeiting and combating jelly fish attack in mobile ad-hoc networks. In *2014 5th International Conference Confluence The Next Generation Information Technology Summit (Confluence)* (pp. 359–364). IEEE.