Malicious Node Detection on Routing Via Certificate Authority and Optimal Fuzzy for Wireless Ad-Hoc Network

Rajkumar. K, M. K. Jeyakumar

Abstract**:** ***Wireless Ad-Hoc network has a set of nodes which designed with wireless transceivers. These nodes communicate with each other by accessing the common channel. In the ad-hoc network, security is one of the main challenges. Due to the behavior of malicious nodes, the security of the network is compromised. So, the major objective of this paper is to improve the security of the network by combining both malicious node detection and cryptography techniques. In this paper, an optimized fuzzy system is presented for the detection of malicious nodes which are malfunctioning in the routing path between source and destination. To optimize the performance of the fuzzy system, Particle Swarm Optimization (PSO) algorithm is presented. After the detection of malicious nodes, each normal behavior node in the network is authenticated by the Certificate Authority (CA). Then the authenticated nodes transmit the data packets to the destination with the Elliptic Curve Cryptography (ECC) algorithm. Simulation results show that the performance of the optimized fuzzy system is improved than that of the conventional fuzzy system for malicious node detection in terms of delivery ratio, detection time and energy efficiency.***

Keywords: Wireless Ad-Hoc network, optimized fuzzy system, Particle Swarm Optimization (PSO), Certificate Authority (CA) and Elliptic Curve Cryptography (ECC).

I. INTRODUCTION

During the most recent years, we have all seen relentlessly expanding development in the deployment of wireless and mobile communication networks [1]. Wireless ad hoc networks comprise of nodes that can communicate using remote mediums and structure dynamic topologies [2]. The fundamental characteristic for these systems is the complete lack of any sort of foundation and in this way the absence of devoted nodes that give network management tasks as do the conventional routers in fixed networks. So as to keep up connectivity in ad hoc network every taking deployment nodes need to perform routing of network traffic. The participation of nodes can't be implemented by a centralized administrative authority since one doesn't exist. In this way, a network-layer protocol intended for such self-sorted out networks must uphold connectivity and security necessities so as to ensure the undisrupted activity of the higher layer protocols [3]. Tragically the majority of the broadly utilized ad hoc routing protocols have no security contemplation and trust every one of the members to effectively forward routing and information traffic [4] [5]. This supposition can demonstrate to be terrible for an ad hoc network that depends on intermediate nodes for packet sending. Along these lines, the nodes that take part in an ad hoc network perform malicious tasks, and afterward the normal throughput will be corrupted. A few attacks like a wormhole, rushing, black hole and so on [6] [8] have come into the image under which a genuine node carries on in a malicious way. It is very hard to characterize and distinguish such behavior of a node. In this way, it becomes obligatory to characterize the typical and malicious behavior of a node.

[9]. An intruder exploits the vulnerabilities displays in the ad hoc network and attacks the node which breaks the security standards. Other than the previously mentioned challenges, the resources in the ad-hoc network additionally fill in as the real limitations. The reason is that they make difficulties while conveying security processes. So, we were motivated to detect the malicious nodes in the wireless ad-hoc network for secure communication.

Contributions of this proposed approach are described as follows:

- A routing path is established between source and destination using the AODV routing protocol.
- Any of the intermediate nodes in the routing path is behave as a malicious node. So, for malicious node detection, an *optimized Fuzzy* based system is presented. By optimizing the membership function of the input variables such as delivery ratio, delay, and energy consumption with the *Particle Swarm Optimization (PSO)*, the performance of the Fuzzy system is improved. Using this improved or optimized fuzzy system, malicious nodes are detected.
- After the malicious nodes detection, the members or nodes in the network are authenticated using *Certificate Authority* (CA). After the authentication process, the source node transmits the data securely with the *Elliptic Curve Cryptography (ECC)* algorithm.

Manuscript published on 30 September 2019
* Correspondence Author

Rajkumar.K*, Research Scholar, Dept. of Computer Science and Engineering , Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamilnad,India.rajkumarkpillai@gmail.com

Dr. M. K. Jeyakumar, Professor, Dept. of Computer Applications, Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamilnadu. India. Jeyakumarmk@yahoo.com

Remaining sections of the paper are organized as follows. Section 2 surveys some previous literature which focused research on malicious node detection and secure communication in a wireless ad-hoc network. Section 3 states the problems in the network and solutions to that. Section 4 proposes optimized fuzzy based malicious node detection on routing and certificate authority based secure communication in a wireless ad-hoc network. Results of this proposed approach are discussed in section 5. Finally, section 6 concludes this paper.

II. RELATED WORKS

In this section, some previous literatures are survived that focused research on malicious node detection and secure communication in the ad-hoc network. J. Sathiamoorthya, B. Ramakrishnan and Usha. M [10] had proposed a novel protocol which provides an efficient route discovery technique along with a competent Three Fish algorithm. The authors had aimed to enhance the safety of the data during transmission. To achieve their aim, they had presented an enhanced three fish Algorithm. The proposed protocol was used to determine the forwarding order and exploit the neighbour coverage knowledge more effectively. By presenting this approach, they had achieved data security in an ad-hoc network.

Muhammad Usman *et al* [11] had presented a Secured Data Communication Scheme for Mobile Ad-hoc Networks. The objective of the authors was to achieve better throughput in MANET. The objective had been attained by presenting QoS-Aware Secured End-to-End data Communication which was abbreviated as QASEC. The proposed mechanism relied on symmetric encryption using shared secret keys and identity of each device for authentication. Because of the proposed approach, the authors had achieved better packet-loss rate, jitter and end-to-end delay in the network.

A. R. Rajeswari *et al* [12] had proposed a secure routing algorithm for effective communication in mobile ad-hoc networks. The authors had aimed to reduce additional overhead in dynamic nature of mobile ad-hoc networks. proposed a secure routing algorithm for effective communication in mobile ad-hoc networks. The authors had aimed to reduce additional overhead in dynamic nature of mobile ad-hoc networks Fuzzy Inference System which was used to handle uncertainty in the selection of trusted nodes and to identify the stable routes. By presenting these proposed approaches, they had increased packet delivery ratio and had reduced delay in the network.

S. B. Geetha, Venkanagouda and C. Patil [13] had presented a novel routing protocol in Mobile Adhoc Network. Aim of the authors was to enhance the security of MANET against wormhole attack. They had attained their aim by presenting Graph-Based Energy Supportive Routing Protocol. This protocol offered s higher degree of energy conservation when exchanging routing information and established faster communication. Besides, this proposed approach offered better conservation of energy and satisfactory communication performance in MANET.

Jarupula Rajeshwar and Gugulotu Narasimha [14] had proposed a secure way routing protocol for MANET. The authors aimed to evade specific type of attacks or malicious behavior of the nodes or networks. To achieve their aim, they had presented a novel secure way routing protocol. This protocol provided a unique session key for each route to secure the data communication using two-way asymmetric cryptography. Security of the MANET had been improved by presenting this secure routing protocol.

Tejpreet Singh, Jaswinder Singh and Sandeep Sharma [15] had proposed Energy efficient secured routing protocol for MANETs. The objective of this literature was to enhance security and energy efficiency of MANET. To achieve this aim, they had presented security to the protocol by choosing a secure link for routing using Secure Optimized Link State Routing Protocol. Also, they had presented the Secure Source Anonymous Message Authentication Scheme for communication privacy. This proposed approach had enhanced energy efficiency in MANET.

From the above literature, we inferred that the researchers seemed to enhance the security in the wireless ad-hoc network. Although they have presented efficient routing protocols, malicious nodes in the routing path are to be detected efficiently within a less time period of detection. So, before transmitting the data packet, the source node should detect the malicious nodes with an optimized classifier. Also, some researchers have presented secure routing protocol while others have presented secure communication with cryptography only so that this research work focuses to present both malicious node detection and cryptography techniques for enhancing the security of ad-hoc network further.

III. PROBLEM STATEMENT AND SOLUTIONS

Security is one of the main challenges in the wireless ad-hoc network. Generally, a source node forwards the data packet to the destination through the optimal path. For routing the data packets in the optimal path, few routing protocol techniques have been used in a wireless ad-hoc network. Ad-hoc On-Demand Distance Vector Routing Protocol (AODV) is one of them. In AODV, during the route discovery process, any of the intermediate nodes between source and destination may act as a malicious node. This malicious node provides false route information to the source node and also it becomes vulnerable to the data packet. So, before the transmission of data packets, malicious nodes in the routing path are to be detected efficiently. Although many malicious node detection methods have been presented before, an efficient and optimized malicious node detection method is to be proposed. Although the vulnerable malicious nodes in the network have been detected, the network should be aware of malicious node entry to the network without authentication. So, each user or nodes in the network should be authenticated.

IV. SYSTEM MODEL

Figure 1 shows the system model of the Wireless Ad-Hoc network. As shown in the figure, the network includes mobile devices such as mobile phones, laptops and etc.

Every device in the network directly communicates with each other. The communication link between these devices is wireless. In this system, a source device and a destination device are considered. Before transmitting the data packet, the source node establishes a routing path to the destination by selecting the intermediate nodes with normal behavior. After the establishment of the routing path, each node in the network is authenticated by issuing a signed certificate from the Certificate Authority (CA). This CA registers the information about the nodes such as node's id, certificate validity and the public key of the node. If the nodes in the network corrupted or they act as a malicious node, certificates are revoked to the corresponding nodes. Identities of the malicious node in the network are maintained in the certificate revocation list (CRL). After the verification of authentication, the source node starts to send the data packet securely.

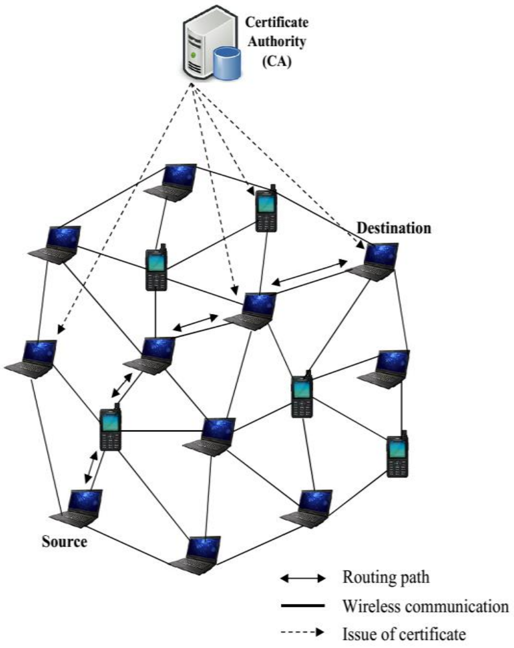

Fig. 1. System model of a wireless ad-hoc network

A. Overview

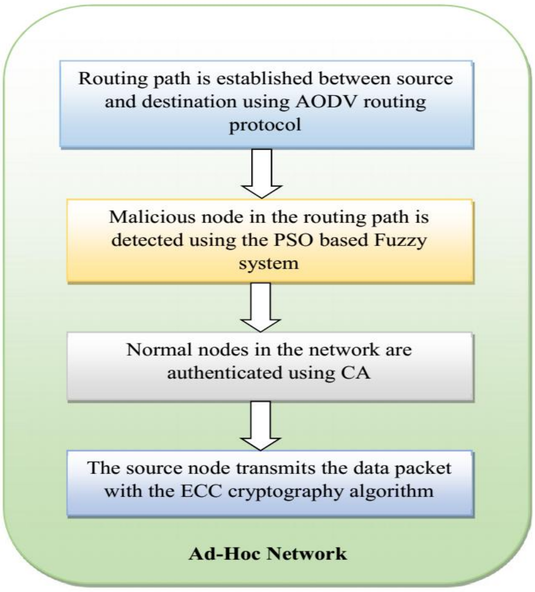
Routing path is established between source and destination using AODV routing protocol
Malicious node in the routing path is detected using the PSO based Fuzzy system
Normal nodes in the network are authenticated using CA
The source node transmits the data packet with the ECC cryptography algorithm
Ad-Hoc Network

Fig. 2. Workflow diagram

In this approach, a routing path is established between source and destination using the AODV routing protocol. In AODV, during the route discovery process, any of the intermediate nodes between source and destination may act as a malicious node. This malicious node provides false route information to the source node and also it becomes vulnerable to the data packet. So, to detect malicious nodes on AODV, PSO based Fuzzy logic system is presented. After the detection of malicious nodes, intermediate nodes on AODV are authenticated using CA. Then the authenticated nodes forward the data packet to the destination securely with the ECC cryptography. Figure 2 shows the workflow diagram.

B. Routing based on AODV protocol

AODV is a routing protocol which is used to overcome the routing issues in a wireless ad-hoc network. This protocol supports mobile nodes for reliable communication. In this protocol, initially, a node creates Route Request (RREQ) Packet and it sets the time for receiving Route Reply (RREP) message from the neighbor node. After the reception of RREQ, each node maintains the source IP address and the RREQ broadcast ID pair. This information is stored in the node for a finite period of time. After receiving the RREQ within the finite time period, the node establishes the reverse route in its routing table. This reverse route includes source IP address, count of hops to reach the destination and the sequence number. The routing table of intermediate nodes is updated during the RREQ transmission. Then the destination node forwards the RREP to the intermediate nodes through the reverse route. From the neighbor nodes, each intermediate node can receive more than one RREP. Among the received RREPs, the intermediate node selects the RREP with smaller hop count which means the shortest routing path is established between source and destination.

During the process of route discovery, a node forwards the RREQ packet to the neighbor nodes. After receiving the RREQ, any of the intermediate nodes shows that it has the shortest path to the destination. These nodes are known as malicious nodes. This malicious node provides false route information to the source node. Due to this fake route which is established between the malicious node and neighboring node, the forwarded data packet will be corrupted and the destination never receives even a single packet. So, before the transmission of data packets, malicious nodes in the routing path are to be detected efficiently. Thus, for the detection of malicious nodes on the routing path, Particle Swarm Optimization (PSO) based Fuzzy system is presented and is described in the following section.

C. Optimized Fuzzy based Malicious Node Detection on Routing

In this section, malicious nodes in the ad-hoc network are detected with the optimized Fuzzy system. In this proposed method, the membership function of the fuzzy system is optimized using Particle Swarm Optimization (PSO) algorithm.

Fuzzy system based malicious node detection

The proposed fuzzy system is shown in Figure 3. This system includes following four levels that are as fuzzification, generation of the fuzzy rule base, fuzzy inference system, and defuzzification. To detect malicious nodes, Message success rate (MSR), Residual Energy (RE) and Elapsed time (ET) are given as input to the fuzzy system. Based on these input variables, input crisp values of the fuzzy system are processed.

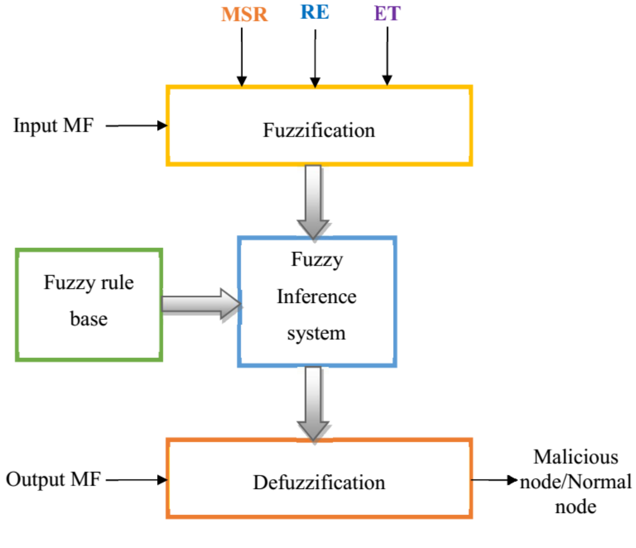

Fig. 3. The proposed fuzzy system

Fuzzification**:** In this level, input crisp values of MSR, RE, and ET are processed in the system in the form of fuzzy variables. The behavior of the node is the output of this system. For MSR, fuzzy variables are classified in the range [0, 1] and fuzzy variables of the MSR are Low (L), Medium (M) and High (H). Fuzzy variables of RE are Low (L), Medium (M) and High (H) and are in the range [0, 10J]. Also, membership functions of ET are considered as Low (L), Medium (M) and High (H) in the range [0, 10ms]. Fuzzy variables of the output are Malicious or normal node as shown in table I. To attain the optimum results, trapezoidal and triangular membership functions are used in this system. These triangular and trapezoidal membership functions are utilized for intermediate and boundary variables. The membership functions of fuzzy variables for the input values MSR, RE, and ET are shown in Figure 4, 5 and 6 respectively. Membership function of the output variable is shown in Figure 7.

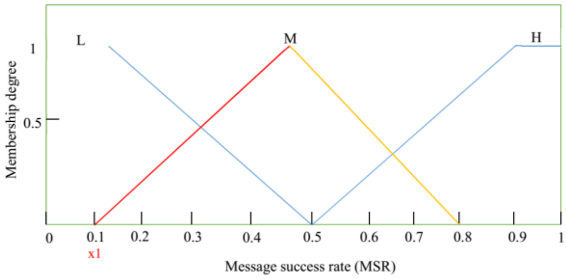

Fig. 4. Membership function of MSR

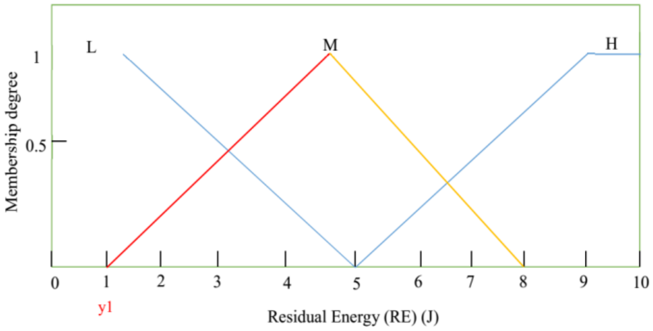

Fig. 5. Membership function of RE

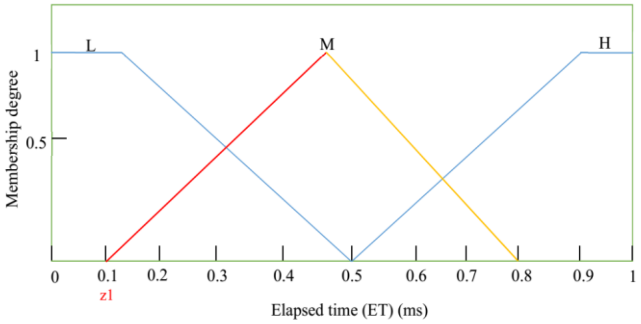

Fig. 6. Membership function of ET

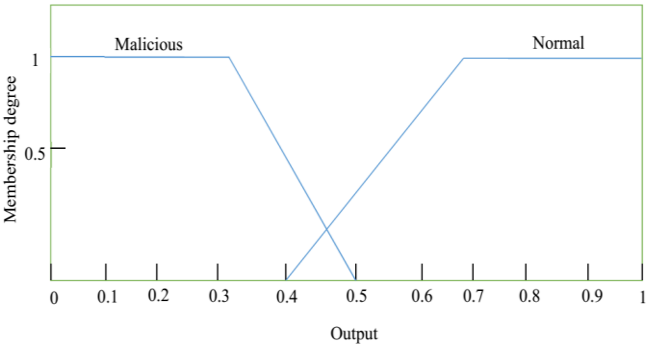

Fig. 7. Membership function of Output

Defuzzification (D)**:** In this level, fuzzy set values are converted into crisp values. For defuzzification, 5 methods [16] are suggested that are Last of Maxima Method (LOM), First of Maxima Method (FOM), Bisector of Area Method (BOA), Mean of Maxima Method (MOM) and Center of gravity (COG).

Table I: Fuzzy rule base

Rule No	MSR	RE	ET	O/P
R_1	L	M	H	Malicious
R_2	L	H	M	Normal
R_3	M	L	H	Malicious
R_4	M	H	L	Normal
R_5	H	L	M	Malicious
R_6	H	M	L	Normal

For each time, the rule base of this fuzzy system is to be balanced for each time by adapting the input and output parameters of MFs. Along these lines, it is basic to decide an optimal combination of these parameters.

In this methodology, the accompanying parameters of the fuzzy system are to be optimized. In this approach, triangular membership functions of the input variables are optimized to attain the optimal result.

Triangular MFs of the input variables are to be optimized. For instance, on the off chance that we consider a triangular shape with three peak values, for example, p, q, and s as appeared in **Figure 8**, where q and s are fixed while p-value differs. In this proposed fuzzy system, the input variables MSR, RE, and ET have triangular shapes those parameters are to be optimized. As appeared in figures 1, 2 and 3, the adjustable parameters x1, y1 and z1 are to be optimized. By changing the value of x1, y1, and z1, a fuzzy rule base also will be improved. Along with these parameters and fuzzy rule base, defuzzification methods (Z) also included finding the optimal defuzzification method.

So, the solution with 10 elements is to be selected as the optimal fuzzy system. The selection of the best possible solution will assist the network to detect malicious and normal nodes accurately or optimally. In this approach, Particle Swarm Optimization (PSO) is presented for optimizing the parameters of the fuzzy system and it is described in the following section.

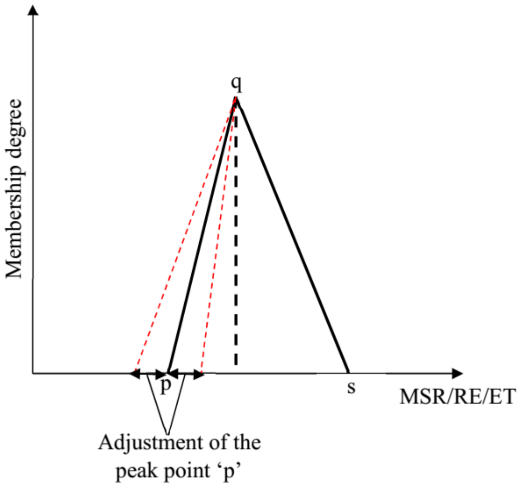

Fig. 8. Position of peak points of triangular MF

D. PSO based Fuzzy system for malicious node detection

By optimizing the membership function of the fuzzy variables along with the fuzzy rule and defuzzification, an optimal fuzzy system is selected. With the optimal fuzzy system, malicious and normal nodes in the ad-hoc network are detected accurately. For the selection of the optimal fuzzy system, PSO is presented. It was developed by James Kennedy and Russ Eberhart in 1995. This algorithm imitates the behavior of animal groups such as fish schooling and bird flocking. These animals searching for a food source and reach closest to the position of food source with have no leaders. The procedure of the PSO algorithm in obtaining optimal values follows the behavior of this animal group. In PSO, particle describes an optimal solution. Phases of this algorithm are explained as follows:

***Initialization*:** Initially, particles (P) or candidate solutions are initialized in the swarm. In this approach, the candidate solution this approach is 10 elements of the fuzzy system. The structure of each solution is shown in Figure 9.

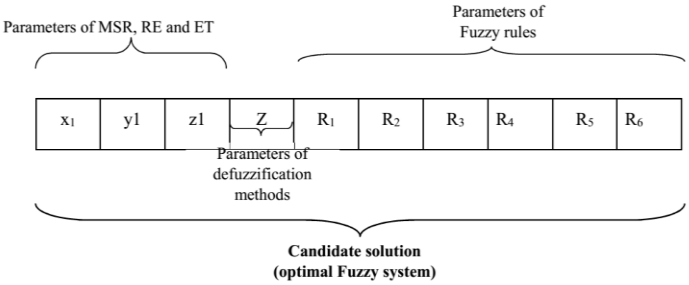

Fig. 9. Initialization of optimal solutions

Let artificial fishes or candidate solutions are initialized in *d* dimensional space as follows:

$$Y = \{F_1, F_2, \ldots\ldots, F_d\} \qquad (1)$$

Where, F_d represents the position of the artificial fish or optimal fuzzy system in d^{th} dimension. Constraints of the input parameters are given as follows:

$$\begin{cases} p_n \le x_n \le s_n \ (or)\ x_n \le p_n \quad n = 1 \\ p_n \le y_n \le s_n \ (or)\ y_n \le p_n \quad n = 1 \\ p_n \le z_n \le s_n \ (or)\ z_n \le p_n \quad n = 1 \end{cases} \qquad (2)$$

Order of MFs of two input parameters x_n, y_n, and z_n are given in equations (3).

$$p_n < q_n < s_n \qquad for\ x_n, y_n and\ z_n \qquad (3)$$

***Fitness*:** After the initialization, fitness is calculated for each solution. The fitness is calculated based on the delivery ratio of the network. The system with the maximum delivery ratio is selected as an optimal fuzzy system. It can be represented as follows:

$$Fit_i = Max\{Del\ Rat_i\} \qquad (4)$$

Where, $Del\ Rat_i$ represents the delivery ratio of the i^{th} and it can be defined as follows:

$$Del\ Rat_i = \frac{No.of\ Received\ Packets}{No.of\ Transmitted\ packets} \qquad (5)$$

Updating Procedure: After Calculating the fitness value of each particle best value (P_{best}) and global best (G_{best}) are determined , here P-best is lower error of each particle and G-best is optimal solution is obtained using the updating procedure that is position and velocity , it mathmatically represented in equation (6) and (7).

$$v_{t+1} = \omega * v_t + c_1 * r_1 (p_{best} - x_t) + c_2 * r_2 ((g_{best} - x_t)) \qquad (6)$$

$$y_{t+1} = y_t + v_{t+1} \qquad (7)$$

Where, v_{t+1} and x_{t+1} is the current velocity and current) position of each particle respectively, r_1 and r_2 are two random values with the range [0, 1]. c_1 and c_2 are the acceleration constants varying in the range [0, 2], ω denotes the inertia weight varying in the range [0, 1]. This inertia weight value is decreasing while increasing the iteration *t*. This can be calculated as follows,

$$w = w_{\max imum} - \frac{w_{\max imum} - w_{\min imum}}{t_{\max imum}} \times t \quad (8)$$

Where, $w_{\max imum}$ and $w_{\min imum}$ represent the maximum and minimum inertia weight respectively. $t_{\max imum}$ represents the maximum number of iterations.

After the particle is updated to the new position, the fitness value of the particle *P* is compared with the fitness of previous *P_{best}*. If the fitness value of *P* is greater than that of *P_{best}*, then the particle *P* is updated as the *P_{best}*. Besides, if the fitness value of *P* is greater than that of *g_{best}*, then the particle *P* is updated as the *g_{best}*.

$$P_{best}\ (t+1) = \begin{cases} P(t) & if\ F(P(t+1)) \geq F\left(P_{best}\ (t)\right) \\ P(t+1) & otherwise \end{cases} \quad (9)$$

$$G_{best}\ (t+1) = \begin{cases} P(t) & if\ F(P(t+1)) \geq F\left(G_{best}\ (t)\right) \\ P(t+1) & otherwise \end{cases} \quad (10)$$

Termination: The above phases are continued if the algorithm doesn't satisfy the stop criteria or doesn't obtain the optimal solution or optimal fuzzy system. Otherwise, the algorithm is terminated.

Algorithm: PSO based optimal fuzzy system selection for malicious node detection

Input: Candidate solutions or optimal fuzzy systems (*F_i*)

Output: Optimized fuzzy system

```
1. Initialize candidate solutions or optimal fuzzy systems ($F_i$).
2. Update the values of $r_1$, $r_2$, $c_1$, $c_2$ and $\omega$.
3. Calculate fitness for each solution.
4. Update velocity and position of the solution using equations (6) and (7).
5.If
        $F(P(t+1)) \geq F\left(P_{best}\ (t)\right)$
        $F(P(t+1)) \geq F\left(G_{best}\ (t)\right)$
6.Then
        $P_{best}\ (t+1) = P(t)$
        $G_{best}\ (t+1) = P(t)$
7.Else
        $P_{best}\ (t+1) = P(t+1)$
        $G_{best}\ (t+1) = P(t+1)$
8. End
9. Steps 3-8 are continued until finding optimal solutions.
10. An optimized fuzzy system is obtained.
```

E. Certificate Authority Based Secure Communication

After the detection of malicious nodes, the normal nodes in the ad-hoc network are authenticated using Certification Authority (CA). The CA registers all nodes in the network. It updates the information of each node that is the node's id, certificate validity and the public key of the node. After updating the information from the node, the CA issues certificate to the corresponding authenticated node. This issued certificate will be renewed if the validity period of the certificate is expired. When the node is identifying as a malicious node, a certificate of the node is revoked. Identities of the malicious node in the network are maintained in the certificate revocation list (CRL). Besides, the CA maintains a list of normal nodes with their keying details for secure communication.

After the authentication of normal nodes and the revocation of the certificate to the malicious nodes, the source node forwards the data packet on AODV routing to the destination. For secure communication, the data packet is transmitted with the Elliptic Curve Cryptography (ECC) algorithm. The following section describes the function of this algorithm.

Secure communication using the ECC algorithm

ECC is a public key encryption process based on the hypothesis of the elliptic curve that can be utilized to create cryptographic keys which are increasingly capable, snappier and progressively small. Circular bend cryptography makes keys by methods for the characteristics of the state of the elliptic curve rather than the standard technique of generation as the result of expanding prime numbers.

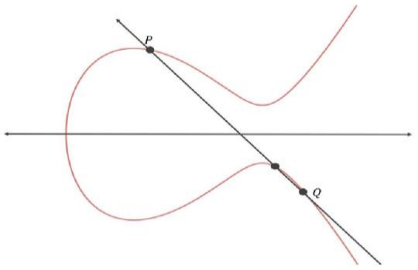

Fig. 9. Point "P" of Elliptic Curve

Figure 10: Point 'P' on the elliptic curve

The ECC approach has the ability to generate private keys and public keys which makes the distributed information more secure. The general condition of the elliptic curve is provided underneath,

$$y^2 = x^3 + ax + b \quad (11)$$

Using the public key of the destination, the source node is e

$$K_{Pu} = K * P \quad (12)$$

Here K_{pu} represents the receiver public key, K denotes the random prime number in range [1, n-1] and iot receiver private key. Finally, P is elliptic curve point shows in figure 10.

V. RESULTS AND DISCUSSIONS

In this section, the proposed optimized fuzzy system and CA-based ECC algorithm are implemented in the Network Simulator (NS2). Table II shows the simulation parameters of the proposed approach. In this simulation, 250 mobile nodes and one CA node are used. These nodes perform in the simulation area 1000m X 1000m. Constant bit rate (CBR) traffic source is utilized for this simulation. IEEE 802.11 based MAC protocol is used. Size of the packet is 512 byte and the packet is transmitted in the rate of 500kbps. For establishing an efficient routing path between source node and destination, AODV routing protocol is utilized. For malicious node detection, PSO based fuzzy system is presented. After the detection of a malicious node, the source node transmits the data packet with the ECC cryptography.

Table II: Simulation settings

Parameters	Assumptions
No. of Nodes	250 mobile nodes and one CA node
Area	1000m X 1000m
MAC	802.11
Simulation Time	200 secs
Traffic Source	CBR
Rate	500Kbps
Propagation	Two Ray Ground
Antenna	Omni Antenna
Packet size	512 byte
Routing protocol	AODV
Cryptography	ECC

A. Performance Analysis

In this section, the performance of the proposed PSO-Fuzzy system is evaluated in terms of delivery ratio, delay, energy consumption, routing overhead and detection time by varying malicious nodes. Also, the performance of the proposed PSO-Fuzzy system is compared with that of the conventional fuzzy system.

B. Performance-based on malicious nodes

Figures 11-16 show the comparison of performance metrics for different approaches by varying malicious nodes. Figure 11 shows the comparison between the delay of the proposed PSO-Fuzzy and that of the conventional fuzzy system by varying malicious nodes. As shown in the figure, the delivery of the packet to the destination is delayed when the number of malicious nodes increases. However, the delay of the proposed PSO-Fuzzy system is reduced to 36% than that of the conventional fuzzy system. As the proposed fuzzy system is optimized using PSO, the detection of malicious nodes is improved than the conventional fuzzy system.

Figure 12 shows the comparison of the delivery ratio of the proposed PSO-Fuzzy system with that of the conventional fuzzy system. When the number of malicious nodes increases, the delivery ratio of the network is decreased. By presenting the optimal fuzzy based malicious node detection with the CA-based ECC cryptography, the delivery ratio of the proposed PSO-Fuzzy system is increased to 40% than that of the conventional fuzzy system. The trade-off between malicious nodes and energy consumption for different approaches is shown in Figure 13. As shown in the figure, the presence of malicious nodes in the network may consume more energy so that these malicious are to be ignored. By presenting the proposed malicious nodes detection, energy consumption of PSO-Fuzzy system is reduced to 54% than that of the conventional fuzzy system.

Figure 14 shows the comparison between the network lifetime of the PSO-Fuzzy system and that of the conventional fuzzy system by varying malicious nodes. Because of the detection of malicious nodes and CA-based ECC communication, the network lifetime of the proposed approach is increased to 50% than that of the existing approach. As shown in Figure 15, routing overhead is increased when the number of malicious nodes increases. However, compared to the conventional fuzzy system, routing overhead of the proposed PSO-Fuzzy system is reduced to 23%. As the proposed PSO-Fuzzy system detects the malicious nodes in the network, the performance of the AODV routing protocol is improved. Thus, the routing overhead of the proposed approach is reduced.

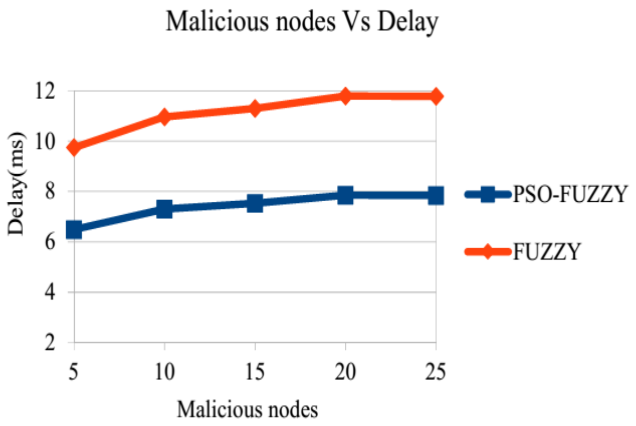

Fig. 11. Malicious nodes Vs Delay

Comparison of the detection time of the PSO-Fuzzy system and that of the conventional fuzzy system by varying malicious nodes is shown in Figure 16. As the proposed fuzzy system is enhanced with the PSO algorithm, the performance of malicious node detection is improved. Thus, the time of malicious nodes detection is decreased to 35% using PSO-Fuzzy system than using the conventional fuzzy system.

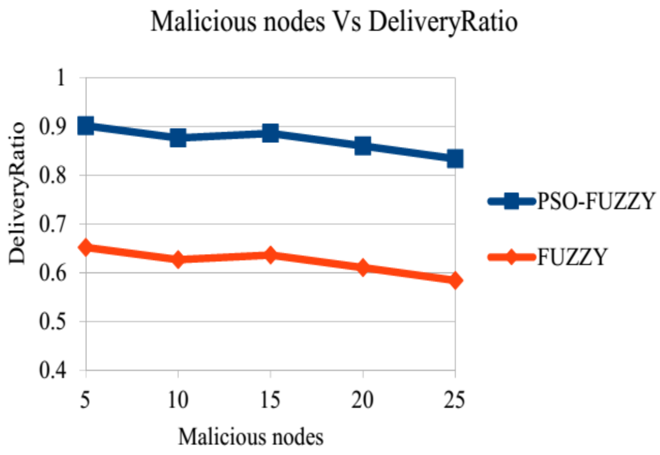

Fig. 12. Malicious nodes Vs Delivery ratio

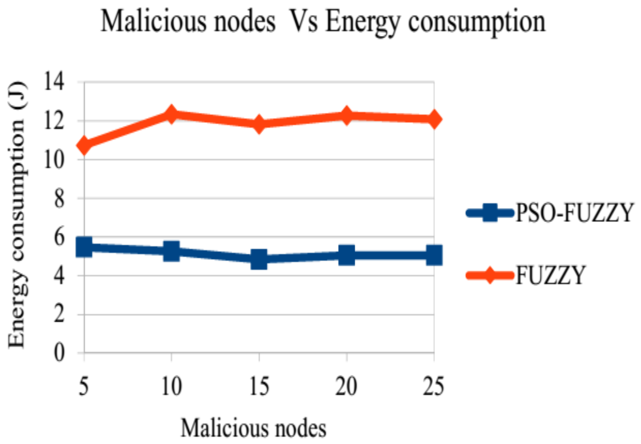

Fig. 13. Malicious nodes Vs Energy

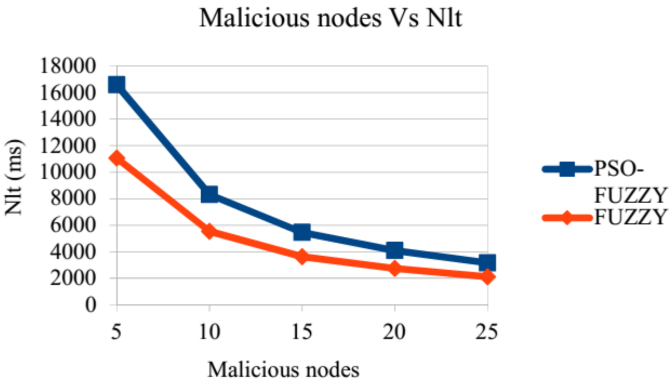

Fig.14. Malicious nodes Vs Network lifetime

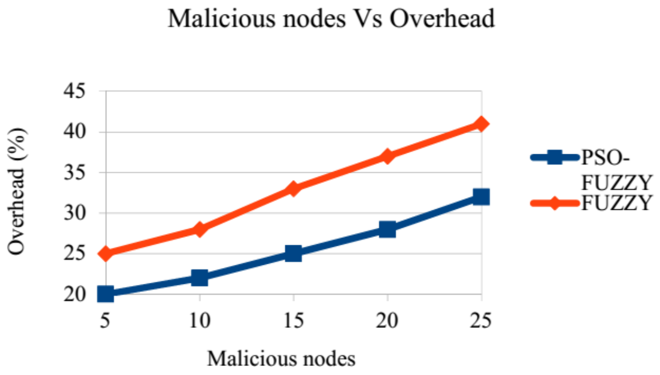

Fig.15. Malicious nodes Vs Overhead

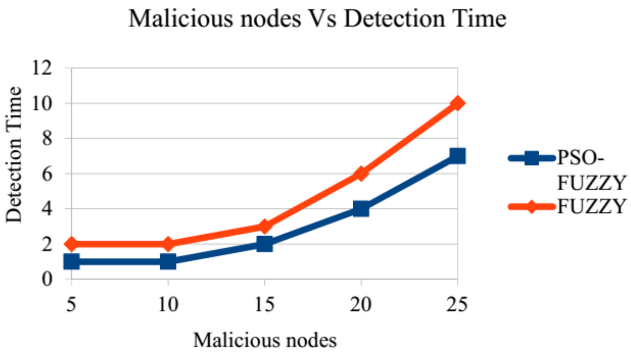

Fig.16. Malicious nodes Vs Detection time

VI. CONCLUSION

For secure communication in an ad-hoc network, optimized fuzzy based malicious nodes detection on routing and CA-based ECC have been presented in this paper. During the routing discovery process of AODV routing protocol, some intermediate nodes behave as a malicious node. These malicious nodes have been detected using the proposed PSO based fuzzy system in this paper. After the detection of malicious nodes, the normal nodes in the network have been authenticated with the CA. After the authentication, the source node has forwarded the data packet to the destination with the ECC cryptography algorithm. By presenting these approaches integrity and confidentiality of the data packets have been improved. The performance of the proposed PSO-fuzzy system is compared with that of the conventional fuzzy system.

Simulation results showed that the proposed system outperformed the existing approach in terms of delivery ratio, delay and detection time.

REFERENCES

1. Hoebeke, Jeroen, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. "An overview of mobile ad hoc networks: applications and challenges." Journal-Communications Network 3, no. 3 (2004): 60-66.
2. S. Toumpis and D. Toumpakaris, "Wireless ad hoc networks and related topologies: applications and research challenges", e & i Elektrotechnik und Informationstechnik, vol. 123, no. 6, pp. 232-241, 2006.
3. S. G. Diana, S. Janardhana, J. Jaya and K. J. Sabareesaan, "Implementation of network layer protocols in wireless networks for efficient routing," 2013 International Conference on Current Trends in Engineering and Technology (ICCTET), Coimbatore, 2013, pp. 349-352
4. S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks", Ad Hoc Networks, vol. 1, no. 1, pp. 151-174, 2003.
5. Y. Singh, Y. Chaba, M. Jain and P. Rani, "Performance Evaluation of On-demand Multicasting Routing Protocols in Mobile Adhoc Networks", 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.
6. S. Sarika, A. Pravin, A. Vijayakumar and K. Selvamani, "Security Issues in Mobile Ad Hoc Networks", Procedia Computer Science, vol. 92, pp. 329-335, 2016.
7. J. V. Ananthi and S. Vengatesan, "Detection of various attacks in wireless adhoc networks and its performance analysis," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, 2017, pp. 754-757.
8. Jangra1,A. Goel,N. Priyanka and Bhati,K. - Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering,
pp. 189-196, 2010

9. J. Karjee and S. Banerjee, "Tracing the Abnormal Behavior of Malicious Nodes in MANET," 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, 2008, pp. 1-7.
10. Sathiamoorthy, J. and Ramakrishnan, B., 2017. Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs. Journal of information security and applications, 36, pp.43-58.
11. M. Usman, M. Jan, X. He and P. Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks", Future Generation Computer Systems, 2018.
12. A. Rajeswari, K. Kulothungan, S. Ganapathy and A. Kannan, "A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks", Peer-to-Peer Networking and Applications, 2019.
13. S. Geetha and V. Patil, "Graph-Based Energy Supportive Routing Protocol to Resist Wormhole Attack in Mobile Adhoc Network", Wireless Personal Communications, vol. 97, no. 1, pp. 859-880, 2017.
14. J. Rajeshwar and G. Narsimha, "Secure way routing protocol for mobile ad hoc network", Wireless Networks, vol. 23, no. 2, pp. 345-354, 2015.
15. T. Singh, J. Singh and S. Sharma, "Energy efficient secured routing protocol for MANETs", Wireless Networks, vol. 23, no. 4, pp. 1001-1009, 2016.
16. D. Rao and S. Saraf, "Study of defuzzification methods of fuzzy logic controller for speed control of a DC motor", Proceedings of International Conference on Power Electronics, Drives and Energy Systems for Industrial Growth.

AUTHORS PROFILE

Rajkumar.K, Research Scholar, Dept. of Computer Science and Engineering , Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamilnad,India. He is working as an associate professor and head of the department in Musaliar College of engineering chirayinkeezhu. He has 21 years of teaching experience in different engineering colleges. rajkumarkpillai@gmail.com

Dr. M. K. Jeyakumar is working as Professor in the Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India. He has 25 years of teaching experience including 17 years of research experience in the field of Mobile Computing and Image Processing. He published more than 110 peer review research articles and one book chapter. Jeyakumarmk@yahoo.com