Optimal Secure Routing Protocol for Ad-Hoc Networks using Adaptive Fuzzy Petri Nets

S. Ananthakumaran[1], A. Praneeth Kumar[2], N. Anjani Satya Santoshi[3],
Sadhana Pamulapati[4], Kothapalli Tharun[5]
[1,2,3,4,5]Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur - 522502, Andhra Pradesh, India
[1]bhashkumaran@gmail.com, [2]saipraneeth005@gmail.com, [3]anjanisatyasantoshi@gmail.com,
[4]sadhanapamulapati7@gmail.com, [5]tarunkothapalli18@gmail.com

Abstract

Optimal Secure Routing Protocol (OSRP) uses the Fuzzy Inference System (FIS) for dynamically evaluating the route lifetime, shortest path and the trustworthiness. This protocol chooses more than one path and enhances the robust transmission against unreliability. The multicasting is done via multiple paths to multiple receivers in the group. The security threats in the network are periodically recognized and OSRP resist against attack in the self preventing and self adjusting fashion, as well as the recovery mechanism enhances the attack tolerance of the network. A special expert system called Adaptive Fuzzy Petri Net Agent is introduced at each node, which has the ability to learn and adjust to fit in to the dynamic environment. So the proposed protocol produces secure and optimal communication path with minimum delay, less routing overhead and higher packet delivery ratio.

Key Words: *Routing, Multicast, Multipath, Fuzzy Petri Nets, Route Lifetime, Energy, Security*

1. Introduction

In the modern era, the networks are everywhere. The proliferation of Internet leads to various advancements in the field of networking. So this paved the way for wireless networking. A routing path from one node to another node consists of number of wireless links, which can be frequently blocked or moved. And along with this fading channel and inference from other communication also led for re-establishment of routes takes place during the transmission. Hence guarantee for the delivery of packets and delay is a complex task in ad-hoc routing, which is an intensive area of research for more than decades.

Numerous routing protocols for ad-hoc networks have been proposed but these protocols are lacks to balance the performance and the security threats. Multipath routing is preferred in-order to provide better fault tolerance in case of path breaks. These kind of protocols are designed for good performance by improving the delivery ratio, reduced the end-to-end delay, reduced routing overhead etc., but they are less concerned about security. Security issues needs to be addressed are, to protect the data transmission and to make the routing protocol secure. Routing protocols are mostly based on the encryption and the authentication algorithms, which addresses the first issue. In order to make a secure routing protocol, the security level of autonomous mobile nodes should be considered.

Fuzzy logic is a multi-valued logic for solving the hard optimization problems with conflicting objective. It is introduced in routing algorithms for optimizing the route selection process considering more than one constrains. These constrains are the route metrics which are used for making decisions and to obtain different number of disjoint routes with maximum life time and stability. Fuzzy inference rule bases are used to calculate the fuzzy cost with the help of the fuzzy rules. These rules express the knowledge to be exploited. The routing protocols designed with the fuzzy logic are accurate and shows improvement in their performance when compared with the protocol which is not using fuzzy.

In general the network is more vulnerable to attacks, when routing is considered the attacks such as unauthorized routing update, sink hole, gray hole and black hole are possible. Only few protocols exist for defending against these attacks but they are compromised in the performance aspect. When fuzzy logic is used in routing it is possible to achieve optimality in routing as well there are possibilities to achieve security also. So, there is always a need for a protocol to achieve the above two goals.

The rest of the paper is organized as follows: section2 gives a detailed literature review of routing protocol and fuzzy Petri Nets, sectin3 focus on the proposed Optimal Secure Routing Protocol and its structure, section4 describes results and discussions, and section5 concludes the paper.

2. Related Work

Ad-Hoc routing protocols are designed, for routing the data among the nodes and based on the source routing or distance vector routing protocols. In general the routing protocols are classified – reactive, proactive, hybrid [5, 6, 16] - based on the routing information updating mechanism. Ad-Hoc On-demand Distance Vector routing protocol (AODV) [1, 3, 7, 10, 12] a reactive routing mechanism, is designed and it follows hop-by-hop routing with the help of the sequence number technique. An Intelligence method - fuzzy logic - can be applied to the Ad-Hoc networks to improve the efficiency of the routing algorithms. Fuzzy Logic is chosen because there are uncertainties associated with nodes’ mobility and the estimation of the link crash. In general the fuzzy system is used in routing algorithms for making decisions for the path selection strategy.

In ad-hoc network the black-hole attack [1, 2, 7, 13] the malicious node, acts as an intermediate node and sends advertisement, that it has the shortest path to reach the destination, to the sender. When the sender starts sending data through this malicious node it simply drops all the packets. Secure Ad-Hoc On-demand Distance Vector routing (SAODV) [15] and Fuzzy logic based detection schemes using AODV [1, 7] are proposed for efficient prevention and detection of black-hole attack. Moreover the SAODV is good enough to solve black-hole problem.

Security and reliable routing is achieved in Security Aware Ad-Hoc Routing (SAR) [15] using the trust levels and in Reliable Routing Algorithm based on Fuzzy-Logic (RRAF) [5] along with the trust-level the battery capacity is also considered. The trust-level is measured by considering the length of association, response time of the node and number of packets forwarded. In RRAF and AODV protocols, Packet Delivery Ratio (PDR) and throughput are decreased when mobility of the nodes increases. When results are analyzed at different pause time, RRAF produces 70% of PDR whereas AODV has produced only 58%. But When End-to-End Delay (E2ED) is considered AODV produces 0.34 seconds, whereas RRAF produces 0.36 seconds.

The energy level of each node in the selected route is helpful for estimating the lifetime of the route [3, 6, 8, 12, 14]. AODV with fuzzy ART predicts the route lifetime [14] using the path length and the node mobility. Fuzzy Stable Route Selection (FSRS) and Fuzzy Route Lifetime Prediction (FRLP) [8] which modifies the AODV, are used to select the stable route and to predict the lifetime of the route based on the fuzzy cost. The PDR for AODV with Fuzzy ART is higher than AODV, where as the Routing Overhead (RO) is decreased by 20.6% and E2ED is also reduced by 45.6% than AODV. FSRS shows improvement than, AODV about 6.087%, 10.113%, 44.36% in terms of PDR, RO and E2ED. In FRLP, PDR, E2ED and RO are increased about 7.18%, 53.247% and 22.499% respectively than AODV. In case of Fuzzy Ad-Hoc On-demand Distance Vector protocol (FAODV) [6], the memory overhead is reduced and the PDR is increased by 5.015%, E2ED is improved by 47.4215%

over normal AODV.

In multicast routing environment [3, 5, 11] to overcome sudden breaks in the path, multipath mechanism is adapted. Fuzzy Modified AODV Multiple Routing (FMAR) [3, 12], selects stable route with maximum route lifetime based on fuzzy logic weight. When using multipath in the multicasting environment, FMAR achieves better performance than AODV. The PDR of FMAR is 98.7% whereas AODV produces 97%, RO and E2ED are reduced in FMAR than AODV. Average Route Acquisition latency for FMAR is 45.5% whereas AODV latency is 49.6%. The enhanced FMAR [3] - for quick maintenance and route repairing with dynamic route lifetime - has produced better results than the FMAR and AODV.

In [4], the topological detection of wormhole is discussed. Wormhole Avoidance Routing Protocol (WARP) [10] avoids wormhole as well it provides load balancing, recovery from isolation of nodes and safety as well. A special expert system called Fuzzy Petri net agent [11] is used in the multicast ad-hoc network to learn and adapt itself in the dynamic changing environment. The packet loss in Knowledge-based Inference Multicast Protocol (KIMP) is around 24% and Bandwidth Efficient Multicast Routing Protocol (BEMRP) produces 35.8%.

Fuzzy Logic based Security Level (FLSL) [15] uses the AODV as the base protocol, concentrates on secure and shortest route selection process. In this protocol, the keys are used along with the fuzzy logic for finding the secure route. The average security level of the FLSL is around 3.35% where as AODV is around 2.6% but in case of PDR, FLSL achieves around 94% where AODV achieves around 95%. Fuzzy Logic Wireless Multipath Routing (FLWMR) [9] considered hop count only for selecting the optimal path whereas the Fuzzy Logic Load Aware Multipath Routing (FLWLAR) [9] considered the traffic load along the link and calculates the optimal path, but both of these protocols are using the fuzzy controller.

3. The proposed optimal Secure Routing Protocol

3.1 Basic Idea

The OSRP routing protocol is the source initiated on-demand secure routing protocol. The objective of this protocol is to find out multiple paths which are optimal and secured. The optimality of the route is decided by two important metrics. The first one is the hop count, which is the number of nodes in between the source and the destination. The second metric is the lifetime of the node. This is calculated based on the consumed energy and remaining energy available in each and every node. The optimal path should be a route with maximum expiry time and should be substituted when one path link is broken. The security level of the route is decided by the trustworthiness of each and every node in the routing path.

3.2 System Model and Assumptions

This section presents a detailed sketch about assumptions and the security threats possessed by the network and security models for handling the threats to achieve a secure and optimal route.

Network Model:

The proposed work addresses multi-hop wireless ad-hoc networks composed of mobile and stationary nodes. All the nodes in this Wireless Ad-Hoc NETwork (WANET) are connected through bidirectional wireless links. Each node is equipped with IEEE 803.11 radios. Any two nodes can be one hop neighbours, if they stay within the transmission range of the other node. The existence of multiple paths increases the routing tolerance in between the source and destination node.

Attack Model:

This work focuses on the different types of attacks that compromise the availability of the network and its operations. The malicious nodes can perform deny or delay operation in the services. In this work such scenarios are considered, and it handles the attacks such as black hole, gray hole, worm hole, and flooding attacks. Other attacks are considered to be out of scope of this work.

Security Model:

In this work, it is assumed that the above mentioned attacks can be identified and can be prevented. The system is designed with one preventive – to prevent attacks, reactive – reacting against malicious nodes and tolerant security mechanism – to mitigate the damages and recover the compromised services.

3.3 System Architecture

The OSRP focuses on supporting the development of essential services such as, routing and end-to-end connectivity. It is established by three integrated modules: input collection module, pre-processing module and processing module. Figure1 illustrates these modules. Each node is the network implements and performs these three modules independently.

Input Collection Module:

A source node in the ad-hoc network consists of multiple paths to reach a destination node. Hop count is described as the number rating nodes along the route between the source and the destination. When the hop count is high the probability of link breakage in the route is high, due to the node mobility. Smaller the hop count means the shortest distance and less overhead.

Trustiness of each node is measured by various parameters such as length of the association, ratio of number of packets forwarded successfully and average time taken to respond to a route request. Based on these parameters the trust worthiness of node i to node j is found. Three types of trust worthiness are Stranger, acquaintance, friend. When node i have never send/receive messages to/from node j, then the trust level between these two nodes will be considered as low. Hence they are called as strangers. Every new node that is entering the existing network will be the stranger node to all its neigbours. If node i frequently send/receive messages to/from node j, then the trust level is high and they are said to be friends. If node i have send/receive few messages to/from node j, then the trust level is medium, hence they are called as acquaintance.

Initially each node is deployed with some amount of energy. Based on the energy of each and every node that node lifetime can be evaluated. For sending and receiving event some amount of energy is consumed.

The nodes which are continuously involving in the process of send and receive will lose considerable amount of energy. The power consumption rate of a node *i* is calculated by considering the power consumed by the node for sending, receiving and the overhead packet and the packets send received and over headed.

$$Power\ Consumption\ (PCi) = \frac{Pr*Nr+Ps*Ns+Po*No}{T} \tag{1}$$

$$Residual\ Energy\ (RE) = \frac{Remaining\ Energy\ of\ node\ i}{PCi} \tag{2}$$

$$Residual\ Time\ (RTi) = \begin{pmatrix} Residual\ Time\ of\ node\ i\ to \\ consume\ its\ Residual\ Energy \end{pmatrix} \tag{3}$$

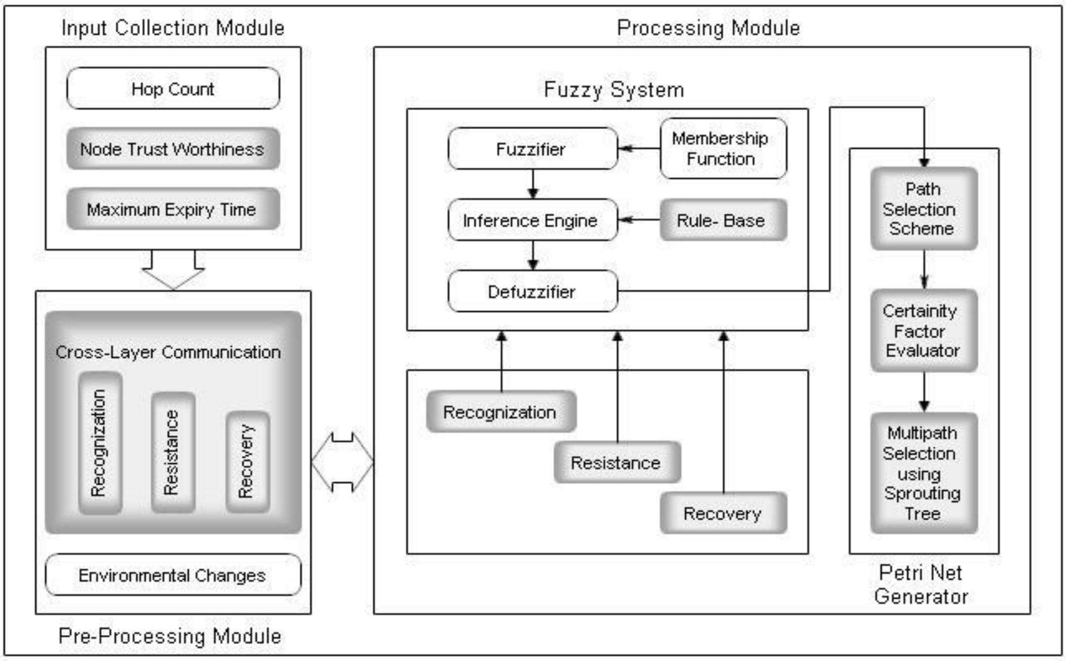

Fig. 1 OSRP Architecture

Where, Pr, Ps and Po are the power consumed by the network interface when the node i receive, send or overhears the packet; Nr, Ns and No are the amount of three types of packet respectively; T is the time period during which the node i consumes its energy. Hence PCi is the average energy consumption rate of node *i*. The residual energy of the node i is calculated as the energy currently available at node *i* divide by the PCi. The residual time of node i to consume its residual energy is considered as the residual time of node *i*. When the residual time of a node increases this in turn increases the expiry time of that node.

Pre-Processing Module:

This module is composed of the cross-layer communication and the environmental change information. The cross layer communication is designed to exchange the information about the network capability of repelling the attacks, detecting the attacks and evaluating the damages, restoring the disrupted information and functionalities. Also it is capable of quickly incorporating the lesson learned from previous failures and thus adapting to emerging threats.

Recognition comprehends reactive mechanisms to identify the threats and the malicious behavior such as intrusion and compromised nodes. Resistance is the preventive mechanism. This component works in self protection and self adjusting fashion. Based on the trustiness of the node, the path is selected for forwarding the data packets. Recovery mechanism is to enhance the attack tolerance of the network. It is used to restore the disrupted information or functionality in case of attacks.

Processing Module:

Processing module consists of fuzzy system, security system and Petri net generator. Fuzzy logic is a tool for modeling the uncertainty of the natural language. It is a form of multi-valued logic, where the variables may have a truth value that ranges in degree between 0 and 1. Fuzzifier is responsible for the fuzzification process. It is defined as a mapping from real valued inputs to a fuzzy set using set of membership functions. The knowledge base or the rule-base is expressed with natural language. The rule base is a collection of IF-Then rules. Here for this system, 81 rules are framed. Table1 illustrates the sample rule base. Figure 2 a) illustrates the network topology graph.

Table 1. Fuzzy Rule-Base

Input			Output
Hop Count	Trust Worthiness	Expiry Time	Certainty Factor
Large	High	Long	Strong
Large	Medium	Long	Normal
Large	Low	Long	Average
Large	High	Medium	Normal
Large	High	Short	Average
Large	Medium	Medium	Average
Large	Medium	Short	Weak
Large	Low	Medium	Weak
Large	Low	Short	Weakest
Normal	High	Long	Strong
Normal	Medium	Long	Strong
Normal	Low	Long	Normal
Normal	High	Medium	Strong
Normal	High	Short	Normal
Normal	Medium	Medium	Normal
Normal	Medium	Short	Average
Normal	Low	Medium	Average
Normal	Low	Short	Weak
Short	High	Long	Strongest
Short	Medium	Long	Strong
Short	Low	Long	Strong
Short	High	Medium	Strong
Short	High	Short	Strong
Short	Medium	Medium	Strong
Short	Medium	Short	Normal
Short	Low	Medium	Normal
Short	Low	Short	Average

The security system comprises recognition, resistance and recovery. This security system is included in order to ensure the system is secured and as well as the path selected is secured. This system is developed to give a hard core security in case of path selection. Henceforth it re-uses the recognition, resistance and recovery mechanism used in cross layer communication.

The fuzzy system output is given to this Petri net generator for the path evaluation. Figure 2 b) illustrates the petri net graph generated for the given network topology. In the path selection scheme, after collecting the reply message from all the forwarding nodes the source node constructs the marked fuzzy Petri net model using fuzzy protection rules. The certainty factor is evaluated based on the dynamically changing input values. Based on this, the set of transition is built for all the possible paths for more than one destination. The fuzzy production rules produce the output in terms of the linguistic variables. These variables will be mapped to the corresponding numerical values in the truth scale for certainty factor. The table 2 represents the set of truth scale for certainty factor and its corresponding numerical values. Based on the certainty factor values the route setup diagram was drawn, which is illustrated in figure 2 c) with all the optimal routes.

The multipath selection in the multicast environment is carried out by means of generating a sprouting tree. The sprouting tree is generally used for the decision making process. Here in this work, the sprouting tree is used to create an inference from the sender to the receiver node through all the forwarding nodes. The degree of truth of the nodes and the n possible routes are found which relies on m possible intermediate nodes. The sprouting tree generated contains all the possible paths and the weights and the various constrain that are specified for selecting the path.

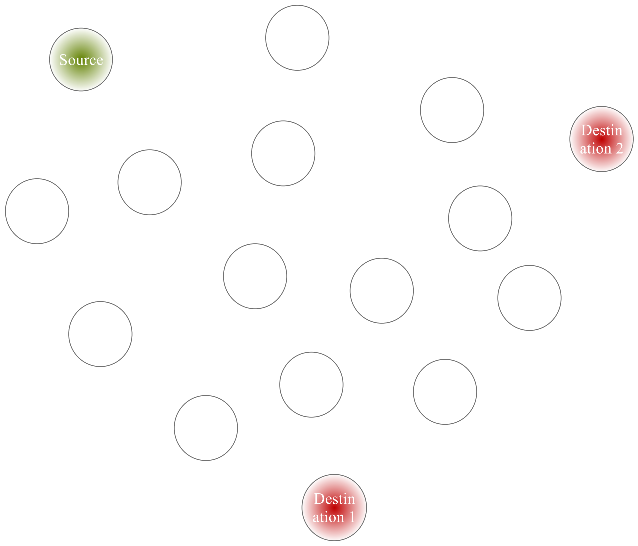

Fig. 2 (a) Topology Graph

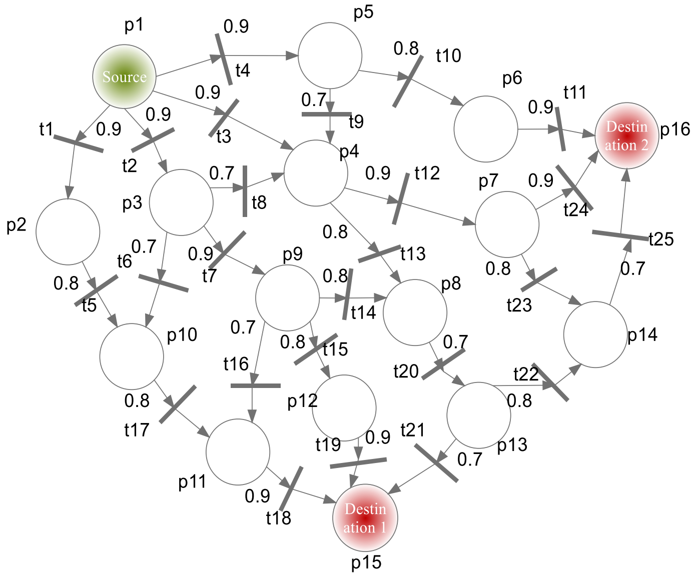

Fig. 2 (b) Marked Fuzzy petri Nets

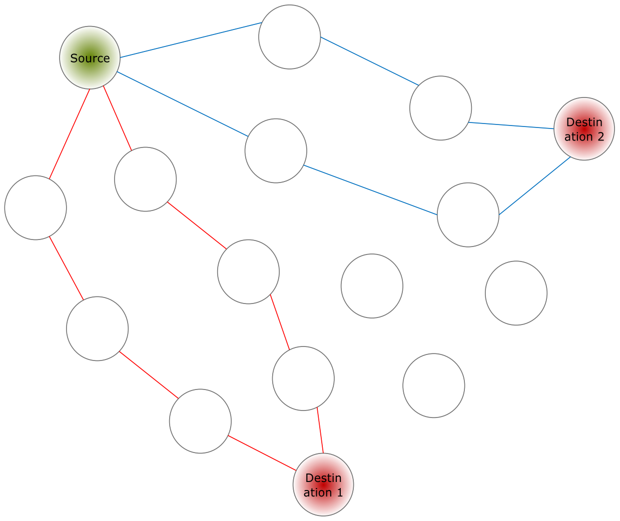

Fig. 2 (c) Selected Route

Fuzzy Reasoning Algorithm:

INPUT : Crisp Set of Input Data (Hop count, Trustworthiness, Expiry time)
OUTPUT: Certainty Factor value for path selection
STEP 1: Route Searching Step, in this step the source node floods the RouteRequest packet to the other nodes present in the multicast group and the receiver in the group re-floods the packet to others. On receiving the RouteRequest the destination sends back a RouteReply packet through the same route it received the request.
STEP 2: Membership Selection Step, in this step the source receives more than one reply through the different routes. The source constructs the different route based on three basic evaluation criteria, such as hop count, trustworthiness and the expiry time of each node. The membership function values are defined for all the three basic criteria.
STEP 3: Using the combined rule-base the final fuzzy rating index is found, i.e. the certainty factor is found, which is represented as membership function again.
STEP 4: The source selects the disjoin routes to different destination nodes. Each node will be having more than one path from source to destination. Out of these paths an optimal one and an alternate one is selected by the path selection scheme.

Table 2. Truth Scale for Certainty Factors

Truth Scale	Numerical Intervals
Strongest	0.91-1.0
Strong	0.71-0.90
Normal	0.61-0.70
Average	0.51-0.60
Weak	0.41-0.50
Weakest	0.30-0.40
Inconsiderable	0.00-0.29

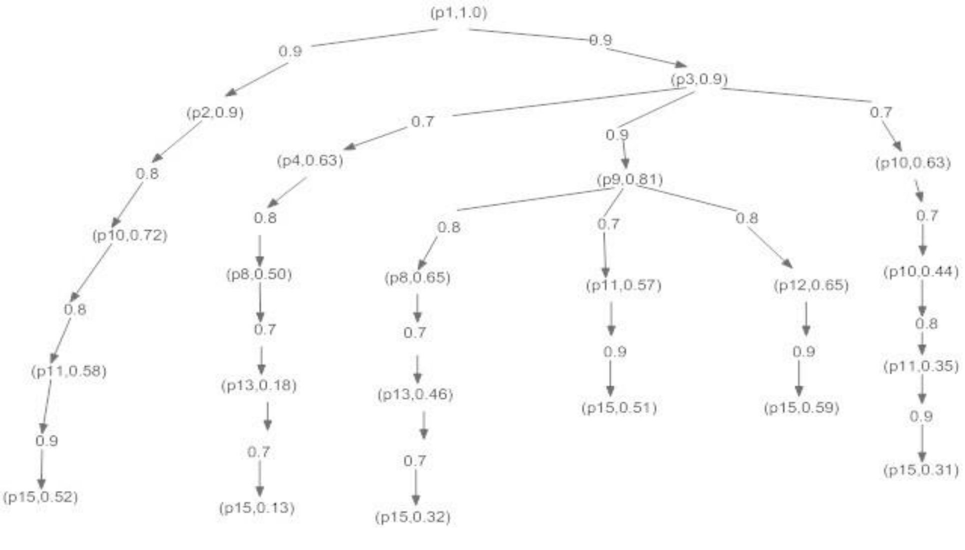

Fig. 3 Sprouting Tree

The path which is having the highest degree of truth is considered to be the optimal and the secure path for multicasting and the next path having second largest truth value is considered as the alternate path in case of path failure. Here in the network topology considered, we have to generate disjoint routes for two different destinations. For destination 1, there are 6 different routes from the source, out of which the path through p3, p9 and p12 is having highest certainty factor and the second largest is p2, p10 and p11. These two routes are stored in the routing table, when the first path is broken the second is chosen. Likewise, for the destination 2 also a sprouting tree is generated. Figure 3 illustrates the sprouting tree generated for the marked fuzzy Petri net shown in fig. 2 b).

4. Results and Discussion

Three network parameters are mainly consider for evaluating the performance of the proposed routing protocol. They are Packer Delivery Ratio (PDR), Routing Overhead (RO) and End-to-End Delay (E2ED). Each parameter is used in two different scenarios such as, by varying the simulation time and the number of attacker nodes.

Table 3. Packet Delivery Ratio (PDR) Vs No. of Attackers

Attacks	No. of Attackers					
	5	10	15	20	25	30
Blackhole	97.26	96.14	96.29	95.84	95.37	94.06
Wormhole	97.24	97.09	96.52	96.21	96.14	95.46
Sinkhole	97.82	96.15	95.82	96.73	95.89	94.35
Grayhole	97.41	95.47	95.72	95.26	95.07	94.59

In the table 3, the variations in the PDR, with varying number of attacker nodes for different attacks are listed out. In the presence of 5 Black Hole (BH) attacker nodes the PDR is 97.26%, where as it is decreased to 94.06% with 30 BH attackers. Similarly, for the wormhole attack, the PDR is decreased from 97.24% to 95.46%, and for sink hole attack the PDR is reduced from 97.82% to 94.35%. For grayhole attack the PDR varies from 97.41% to 94.59%. This is considered to high when compared to other existing routing protocols.

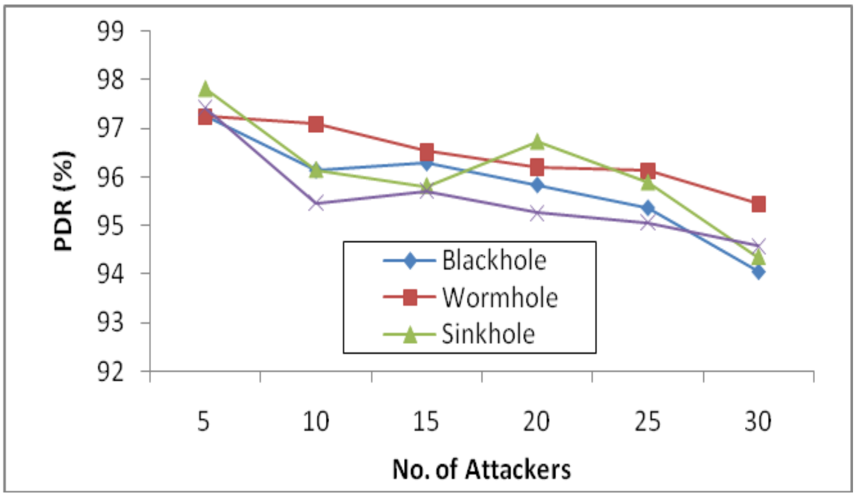

Fig. 4 Packet Delivery Ratio (PDR) Vs No. of Attackers

Figure 4 shows the simulation result of PDR with respect to the number of attackers. In this network when there s no attacker nodes, then the PDR achieves up to 98%. When the number of attackers in the network increases, the PDR will decrease. Here four different attackers with different properties are simulated.

Table 4. Packet Delivery Ratio (PDR) Vs Simulation Time

Routing Protocols	Simulation Time				
	50s	100s	150s	200s	250s
OSRP	97.42	96.21	96.08	96.01	95.94
AODV	96.29	92.46	95.83	93.24	94.61
FAODV	96.56	94.22	94.78	96.47	95.83
FSRS-AODV	95.44	94.3	94.53	93.57	92.36
FRLP-FSRS-AODV	94.62	93.54	94.87	91.67	89.38

Figure 5 shows the simulation result of PDR with respect to the simulation time. Initially the PDR of the proposed method achieves up to 97%. When compared to other routing protocols, on an average OSRP achieves around 96.3%. Table 4 shows the variations in the PDR at different time intervals, also the comparison of other protocols with OSRP.

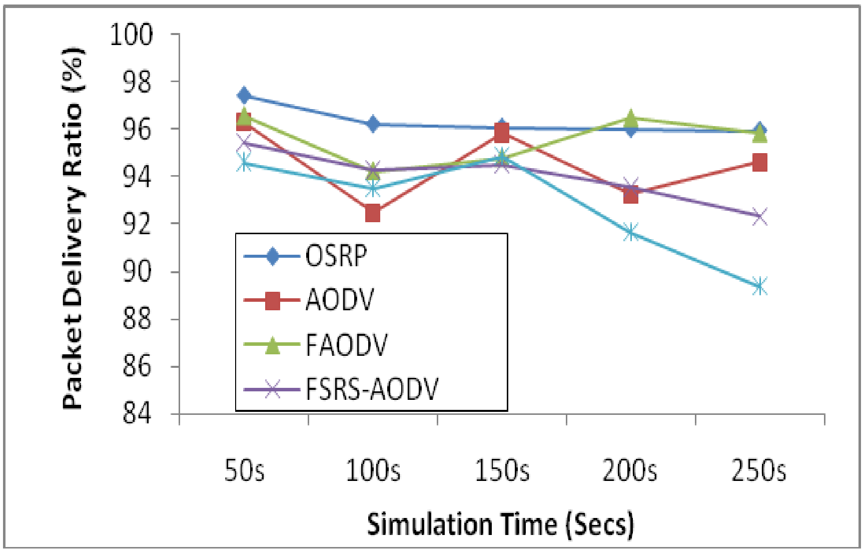

Fig. 5 Packet Delivery Ratio (PDR) Vs Simulation Time

Figure 6 shows the simulation result of the average End-to-End Delay of packets in-between the source and the destination with the varying number of attacker nodes. The average delay increases as the number of attacker's increases. The highest delay obtained in this proposed method is 0. 239ms. In the presence of black hole attacker nodes the delay varies from 0.235 to 0.2826ms and for worm hole it varies from 0.2201 to 0.1643, for sink hole attack, the delay is in between 0.2394 to 0.2574 and for the gray hole it ranges from 0.2341 to 0.2686. The delay with varying number of attackers is given in table 5.

Figure 7 illustrates the plot between the delay and the simulation time. The proposed routing protocol OSRP has produced a minimal delay when compared to other routing protocols at different time intervals. In the table 6, delay at various time intervals for protocols is shown.

Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. Table 7 shows the value of simulation result for normalized routing overload with respect to varying number of attackers.

Table 5. Delay (ms) Vs No. of Attackers

Attacks	No. of Attackers					
	5	10	15	20	25	30
Blackhole	0.235	0.2451	0.254	0.2681	0.2799	0.2826
Wormhole	0.2201	0.2194	0.2071	0.1982	0.1884	0.1643
Sinkhole	0.2394	0.2354	0.2413	0.2498	0.2522	0.2574
Grayhole	0.2341	0.2463	0.2484	0.2514	0.2503	0.2686

Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. Table 7 shows the value of simulation result for normalized routing overload with respect to varying number of attackers.

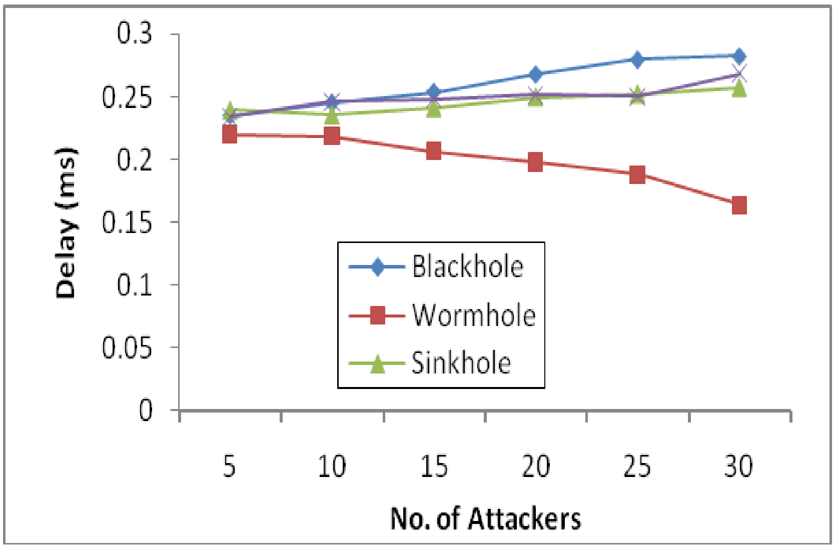

Fig. 6 Delay (ms) Vs No. of Attackers

Table 6. Delay (ms) Vs Simulation Time

Routing Protocol	Simulation Time				
	50s	100s	150s	200s	250s
OSRP	0.232241	0.234747	0.238772	0.244198	0.240643
AODV	0.1842	0.2974	0.2754	0.2865	0.2913
FAODV	0.1752	0.2651	0.2766	0.2702	0.2893
FSRS-AODV	0.2102	0.2453	0.2947	0.3468	0.3982
FRLP-FSRS-AODV	0.1542	0.2341	0.2458	0.2968	0.3621

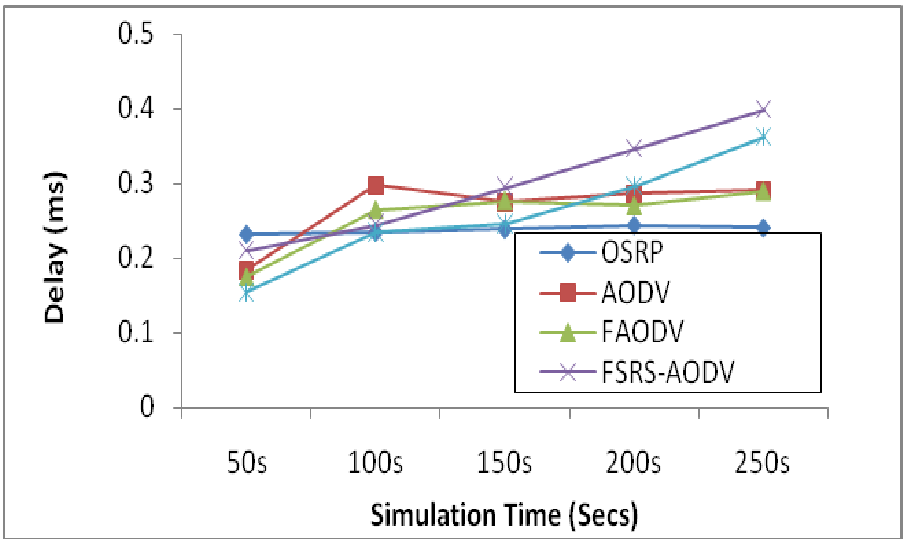

Fig. 7 Delay (ms) Vs Simulation Time

Table 7. Normalized Routing Overload Vs No. of Attackers

Attacks	No. of Attackers					
	5	10	15	20	25	30
Blackhole	0.521	0.5342	0.5864	0.6342	0.6872	0.7126
Wormhole	0.3871	0.2652	0.6365	0.5442	0.6553	0.4563
Sinkhole	0.9782	0.8975	0.8745	0.9723	0.5476	0.9785
Grayhole	0.4212	0.5554	0.5546	0.54265	0.7414	0.6568

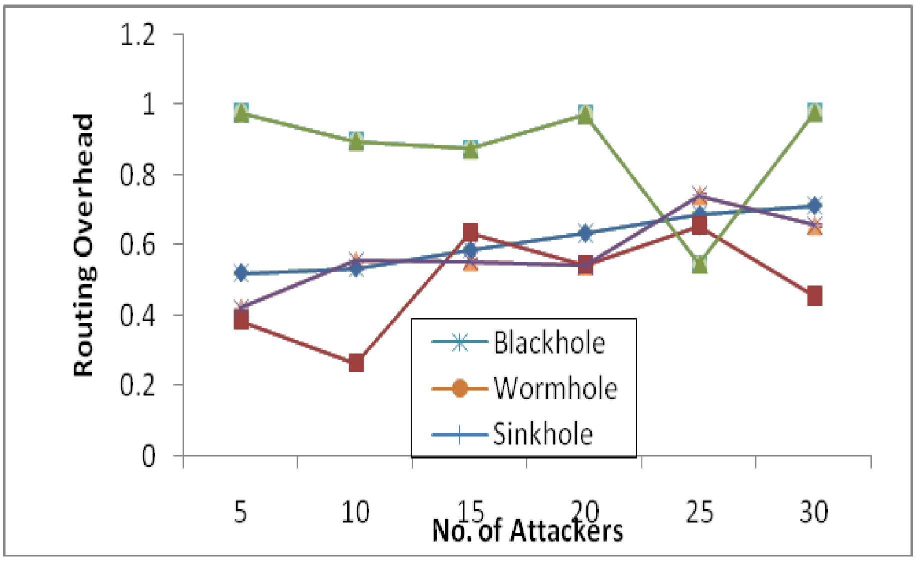

Fig. 8 Normalized Routing Overload Vs No. of Attackers

Figure 8 illustrates the normalized routing overload for different kind of attackers. When the number of attackers in the network increases the routing overhead may also increase. In case of existence of attacker in the estimated path, a new path should be established, hence the routing packets count increase. Table 8 shows the simulation result of normalized routing overload at different time intervals of various protocols. The proposed protocol produces minimized routing overload.

Table 8. Normalized Routing Overload Vs Simulation Time

Routing Protocol	Simulation Time				
	50s	100s	150s	200s	250s
OSRP	0.3689	0.6374	0.7237	0.6449	0.7828
AODV	0.82	0.86	0.94	0.83	0.87
FAODV	0.62	0.813	0.901	0.821	0.8
FSRS-AODV	0.619	0.8354	0.8731	0.793	0.786
FRLP-FSRS-AODV	0.5842	0.7946	0.7638	0.7295	0.774

Figure 9 shows the simulation result of normalized routing overload of the proposed protocol with respect to time. The normalized routing overload achieved by the OSRP is around 0.63. This is considered to be low when compared to that of the other existing protocols.

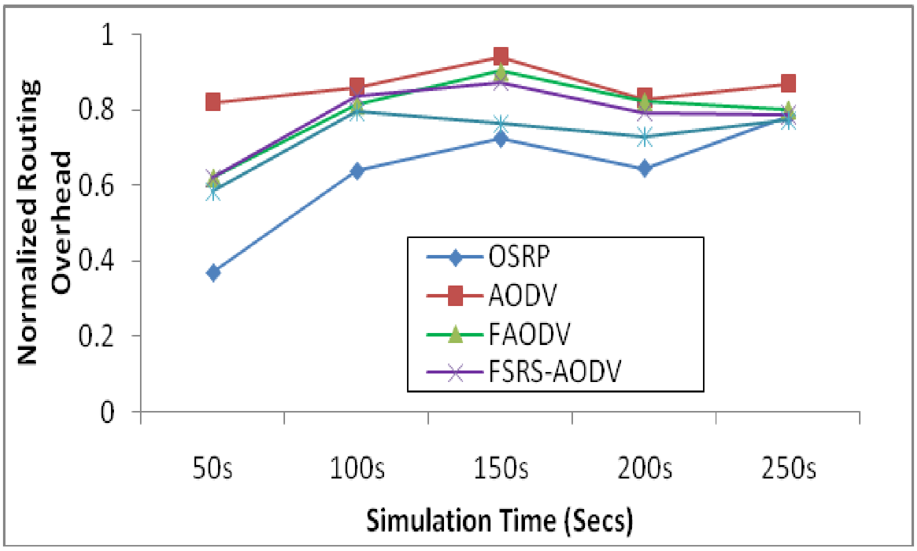

Fig. 9 Normalized Routing Overload Vs Simulation Time

5. Conclusion

Most of the existing systems are designed in a way to effectively identify and handle either routing or security related attacks. A multipath reactive routing protocol OSRP is proposed to discover the optimal and secure multiple paths in the multicasting environment. The routing path and the path selection are carried out by means of using the Adaptive Fuzzy Petri Net generator. And the security level of the path and the efficiency of the path are estimated using the fuzzy logic. As well, the proposed protocol is achieved a higher PDR, minimal E2ED and it also reduces the routing overhead.

References

[1] Xue-Guo Xu, Hua Shi, Dong-Hui Xu, and Hu-Chen Liu, "Picture Fuzzy Petri Nets for Knowledge Representation and Acquisition in Considering Conflicting Opinions," Journal Applied Sciences, Vol. 9, Issue 5, pp. 1-19, March 2019.

[2] Jiming Li, Xiaolin Zhu, and Xuezhen Cheng, "Sensor Fault Diagnosis Based on Fuzzy Neural Petri Net," Journal of Complexity, Volume 2018.

[3] Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar, "A Fuzzy Based Approach to

Detect Black hole Attack," International Journal of Soft Computing and Engineering, Vol.2, No.3, pp.388-391, July 2012.

[4] Michele Nogueira, Helber Silva, Aldri Santos, Guy Pujolle, "A Security Management Architecture for Supporting Routing Services on WANETs," IEEE Transactions on Network and Service Management, Vol.9 No.2, pp.156-168, June 2012.

[5] Dezun Dong, MoLi, Yunhao Liu, Xiang-Yang Li and Xiangke Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks," IEEE Transactions on Networking, Vol.9 No.6, pp.1787-1796, December 2011.

[6] Arash Dana, Golnoosh Ghalavand, Azadeh Ghalavand and Fardad Farokhi, "A reliable routing algorithm for Mobile Adhoc Networks based on fuzzy logic," International Journal of Computer Science Issues, Vol. 8, No 3, pp.128-133, May 2011.

[7] Taqwa Odey Fahad and Abdulahim A.Ali, "Improvement of AODV Routing on MANET using Fuzzy Systems," Arab Journal of Electrical and Electronic Engineering, Vol.7, No.2, pp.102-106, 2011.

[8] Kulbhushan and Jagpreet Singh, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET," IJCA Special Issue on Network Security and Cryptography, Vol.1, pp.28-35, 2011.

[9] Taqwa Odey Fahad and Abdulahim A.Ali, " Fuzzy Controller based Stable Route with lifetime Prediction in MANET's," International Journal of Computer Networks, Vol.3, No.1, pp.37-42, 2011.

[10] A.Gowri, R.Valli and K.Muthuramalingam, "A Review: Optimal Path Selection in Ad hoc Networks using Fuzzy Logic," International Journal on Applications of Graph Theory in wireless ad hoc networks and sensor networks, Vol.2, No.4, pp.1-6, December 2010.

[11] Ming-Yang Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," Elsevier Computer and Security, Vol.29 No.1, pp.208-224, January 2010.

[12] Tzu-Chiang Chiang, Cheng-Feng Tai, Ting-Wei Hou, "A knowledge-based inference multicast protocol using adaptive fuzzy Petri nets," Elsevier Expert Systems with Applications, Vol.39 No.1, pp.8115-8123, October 2009.

[13] Bey-Ling Su, Ming-Shi Wang, Yueh-Ming Huang, "Fuzzy logic weighted multi-criteria of dynamic route lifetime for reliable multicast routing in ad hoc networks," Elsevier Expert Systems with Applications, Vol.35 No.1, pp.476-484, 2008.

[14] Pitipatana Sakarindr, Nirwan Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Transaction on Wireless Communication, Vol. 14, No. 5, pp.8-20, October 2007.

[15] Essam Natsheh, Sabira Khantun and Adznan B.Jantan, "Adaptive Fuzzy Route Lifetime for wireless Ad-Hoc Networks," International Arab Journal of Information Technology, Vol.3, No.4, pp.283-290, October 2006.

[16] Jing Nie, JiangchuaWen, Ji Luo, Xin He and Zheng Zhou, "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks," Elsevier Fuzzy Sets and Systems, Vol.157, pp.1704 – 1712, 2006.

[17] I-Shyan Hwang, Chang-Chieh Liu, and Chiung-Ying Wang, "Link Stability-Based Clustering and Routing in Ad-Hoc Wireless Networks Using Fuzzy Set Theory," International Journal of Wireless Information Networks, Vol. 9, No. 3, pp. 201-212, July 2002.