A NOVEL HYBRID APPROACH OF FUZZY LOGIC AND AOSEDV FOR THE DETECTION OF SLEEP DEPRIVATION ATTACK IN MANET

Er.Sushil Lekhi[1], Divjot Kaur[2]
[1]Assistant Professor, [2]Research Scholar
[1,2]Department OfComputer Science and Engineering, Rayat Institute of Engineering and Information Technology, Railmajra, S.B.S. Nagar, (Punjab), India
[1]lekhi.engg@gmail.com, [2]divjot.kaur91@yahoo.in

***ABSTRACT*— In this research work, we focus on the detection and prevention methods of sleep deprivation attack. The victim of this attack is a battery powered computing device, such as a sensor node, which attempts to remain in a low power sleep mode for as long as possible without adversely affecting the nodes applications. Most of the existing works on sleep deprivation attack detection involve a lot of overhead, leading to poor throughput. Certain level of security can be obtained from the existing solutions. However, these solutions are not always necessarily suitable for wireless networks. In this paper, we have proposed a hybrid concept of AOSEDV and Fuzzy logic for the detection of sleep deprivation attack. The obtained results are compared with AODV protocol by considering the parameters of throughput, packet delivery ratio and path optimality.**

***KEYWORDS*— AODV, AOSEDV, Sleep Deprivation Attack, Fuzzy logic.**

I. INTRODUCTION

Mobile Ad-hoc networks (MANETs) have been widely researched during last few years, gathering lots of attention due to rapid increase in mobile devices. Today's world of dynamic changing technology of communication networks, MANETs play a vital role in wireless communication. MANETs are collection of wireless mobile nodes that acts as dynamic network without use of fix infrastructure and centralized control to authorise other entities in network. MANET comprises of mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the wireless network [1]. Unlike a wired network, nodes in an ad hoc network can free to move in random and arbitrary direction, so frequent changes in topology. These networks are self configuring network and nodes within MANETs provide a peer-level multi-hopping routing service because each node acts as a router [3]. Also, source to destination communication may require routing information via several intermediate nodes to route a packet to the destination node due to limited transmission range of a node. Each mobile node that communicates with other node via radio wave and can communicate directly to those nodes that is in transmission range of each other. Each participating node in MANETs is independent and makes routing decision like route request, route selection, route update and making new communication link with their neighbours as well as serving old established [2]. However, all network functions are based on the nodes mutual effort.The idea of the *sleep deprivation attack* was first proposed by Stajano [4]. The victim of this attack is a battery powered computing device, such as a sensor node, which attempts to remain in a low power sleep mode for as long as possible without adversely affecting the nodes' applications [5]. The attacker launches a sleep deprivation attack by interacting with the victim in a manner that appears to be legitimate; however, the purpose of the interactions is to keep the victim node out of its power conserving sleep mode. Thus, this attack can be used to dramatically reduce the lifetime of the victim. Further, this attack is difficult to detect given that it is carried out solely through the use of seemingly innocent interactions. In this paper, we have proposed a hybrid concept of AOSEDV and fuzzy logic to detect the sleep deprivation attack. AOSEDV is integrated form of AODV (Ad-hoc On-demand Distance Vector) and SEP (Stable Election Protocol). The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. Stable election protocol (SEP) is proposed to maintain the hierarchical routing in the MANET where two types of nodes have their own election probability. So in this proposed concept, AODV and SEP are combined as AOSEDV. But the overall decision of system is performed by the fuzzy logic.The rest of the paper is organized in the following manner: Section II describes the Basic concepts involved to hybrid proposed algorithm. Section III explains the proposed work, Section IV gives the result with evaluation parameters. And section V concludes the paper.

II. BASIC CONCEPTS

In this paper, we have proposed concept of hybrid Fuzzy logic and AOSEDV algorithm. The basic concepts involved for this hybrid algorithm are as below:

A. Fuzzy Logic

The concept of fuzzy logic was introduced by Zadeh during his seminal work of 'Fuzzy Sets'. During this work, he defined the mathematical form of fuzzy set theory and furthers the extension of fuzzy logic concept [6]. This theory came into

existence by introducing various new concepts of reasoning and partial existence of a membership function. The partial existence of the membership function means to have the value of values partial True and partial False and that can function over the range of real numbers [0, 1]. For the generalization of classic logics, new operations wereproposed in the calculus of logic with the principle to achieve the generalized form of that logic. Fuzzy logic also gives an advanced inference that how knowledge based system can also be useful for the approximate human reasoning capabilities. Fuzzy logic theory strengthens the uncertainties of human cognitive processes like reasoning & thinking by providing the mathematical formulation of these concepts. The various facets of fuzzy logic are relational facet, logical facet, epistemic facet & set-theoretic facet. Beside the concept of uncertainty, the vague concepts are also possible to represent with fuzzy set theory by allowing partial memberships function. Modal logic & valued logic are two important logics among all the logics of fuzzy set theory that are linked with all the other logics [7]. Fuzzy set operators may be interpreted in terms of logic connectives in many-valued logic and the membership values in terms of truth values of certain propositions [16]. These logic connectives provide a base for the mathematical formulation of fuzzy set theory that is based on many-valued logic. There is the existence of many definitions for the logic connectives during the study of many-valued logic. In the similar manner, union, intersection & complement can also be defined in a number of ways [8]. Generally, t-norms and t-conorms are used to define the notion of intersection and union in fuzzy set theory so that distinct fuzzy systems can be designed. In most of the cases, to define the membership function of union, complement & intersection of fuzzy system, the whole system only depends upon the membership function of the system that involves solely in that particular fuzzy set system. The main focus of the fuzzy set system is on the fuzzy set operators of the truth-function [9][10].

B. Ad hoc On-demand Distance Vector (AODV)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol: the routes are created only when they are needed [11]. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is upto-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing-entry not recently used is expired. In case of a route is broken the neighbours can be notified [12]. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbours [13].

C. Stable Election Protocol

Stable Election Protocol uses the basic techniques of the LEACH protocol like cluster hierarchy, choosing optimal number of clusters, energy model used and optimal probability of a node to become the cluster head. In SEP, nodes are heterogeneous in nature means nodes have not same initial energy [14]. SEP have the fraction of advanced nodes (m) (nodes which have more energy than the normal nodes, where m is the percentage of advance nodes in total nodes) and the additional energy factor between advanced and normal nodes (Ị). In this, advanced nodes have to become cluster heads more often than the normal nodes. This new heterogeneous setting (with normal and advanced nodes) has no effect on the spatial density of the network. But, the total energy of the system changes [15].

III. PROPOSED ALGORITHM

This work proposes to develop a hybrid intrusion detection system for MANET, based on Fuzzy logic. In this Hybrid concept, we have considered the routing protocols of AAODV with SEP and Fuzzy logic. The AODV (Ad-Hoc On-Demand Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). An advantage of this approach is that the routing overhead is greatly reduced. Stable election protocol (SEP) is proposed to maintain the hierarchical routing in the MANET where two types of nodes have their own election probability. So in this proposed concept, AODV and SEP are combined as AOSEDV. But the overall decision of system is performed by the fuzzy logic. This proposed algorithm is structured as below:

Input: Virtual training dataset of packets.

Output: Sleep Deprivation Attack Detection Model.

ALGORITHM

Step 1: Consider the virtual packets for the detection of sleep deprivation attack.

Step 2: Fix the source and destination where the packets have to be sent through the routing protocols of AOSEDV.

Step 3: Classify the packets of different destination with different paths.

Step 4: For this do make the classification of the packets. All the decision are to be made by the process of fuzzification in fuzzy logic.

Step 5: To search the multiple copies of same example in D, if found then keeps only one unique example in D.

Step 6: For each continuous attributes in D find the each adjacent pair of continuous attribute values that are not classified into the same class value for that continuous attribute.

Step 7: Fuzzy estimation is done based on the value of matrices RS, (R1, R2, R3, ….Rn). Based on the threshold value T and T1, the matrices values are calculated.

Step 8: Consider the matrix RS, the value of matrix is calculated by using the node number and corresponding

member function value and denoted by RS[node number][member function value]. The member function value is calculated by using trapezoidal membership method.
Membership value = (x-a)/ (b-a)
Where x=threshold value, a = number of packets forwarded, b = number of packets dropped.

Step 9: The IPS gets input from the fuzzy technique and it categorizes the range of attack.

Step 10: If a malicious node is node is detected, then IPS mechanism is activated by setting the node against malicious node. The IPS mechanism changes the path of data packet once the malicious node is detected; this is done by AODV which modifies the path in order to provide secure data communication

Step 11: The IPS mechanism and this can be done by attacking the malicious node using the node index and increase the network jam for the packet flow of particular node and uses the alternate path.

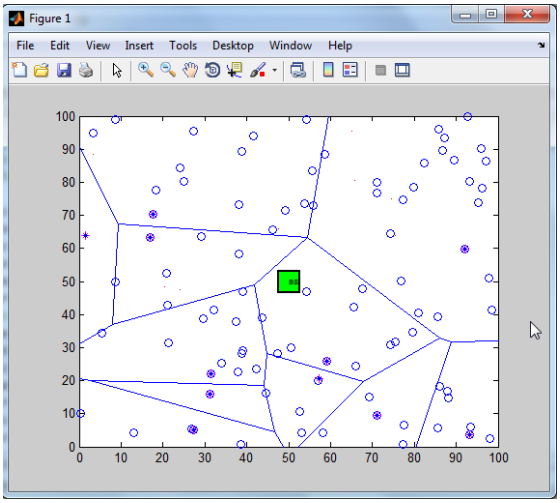
Step 12: The IPS is located between the sender and receiver. If any node type matches the gray hole or black hole attack then AODV block the particular node and choose alternate path.

IV. Result & Discussion

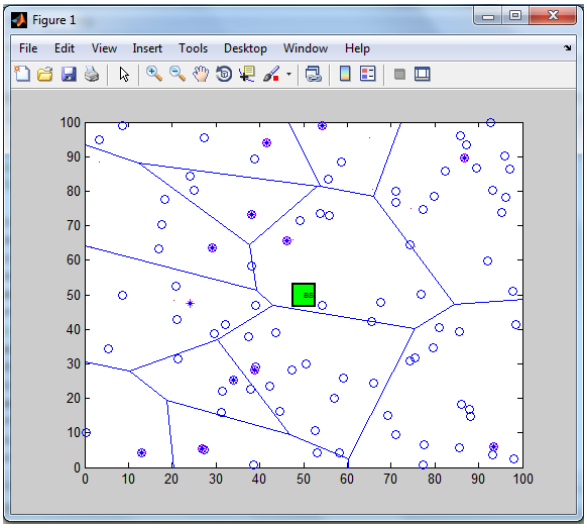
This section examines the performance of the proposed algorithm. It also provides a performance comparison between proposed algorithms with the existing one.

A. Experimental Setup

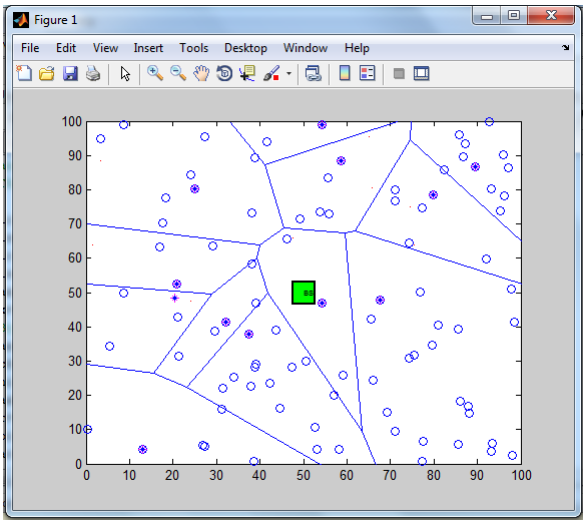
The experimental setup is done to detect the attack of the hacker, if found any then with the help of AOSEDV algorithm IP address is changed and finally path changed. These results are setup with the value of Base Station (BS) in the centre of the routing protocol and packets has to be send. The system is set for the number of iterations. With the change of iterations the simulation can be shown as figure 4.1 (a) to 4.1 (d), some of the random path for the intrusion detection system from the iteration set of 70.



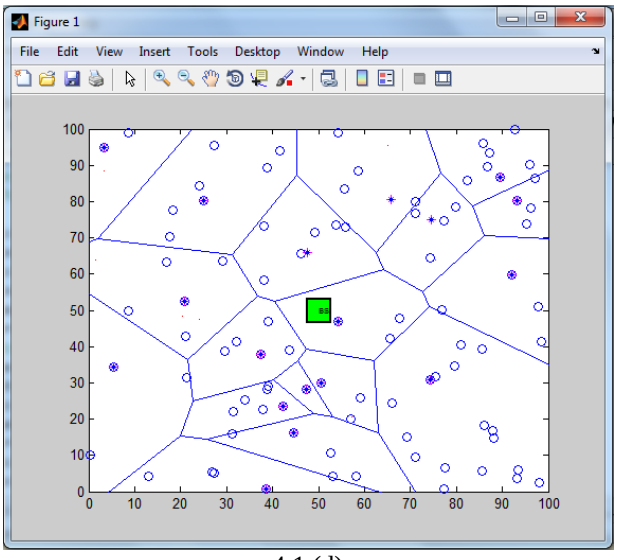
4.1 (a)



4.1 (b)



4.1 (c)



4.1 (d)

Figure 4.1(a)-(d): Sleep Deprivation Attack detection system

To check the traffic of the network, a fuzzy based network control system is generated having some fuzzy rules which are

shared before figure 4.5. GUI is created as shown in figure 4.2 below:

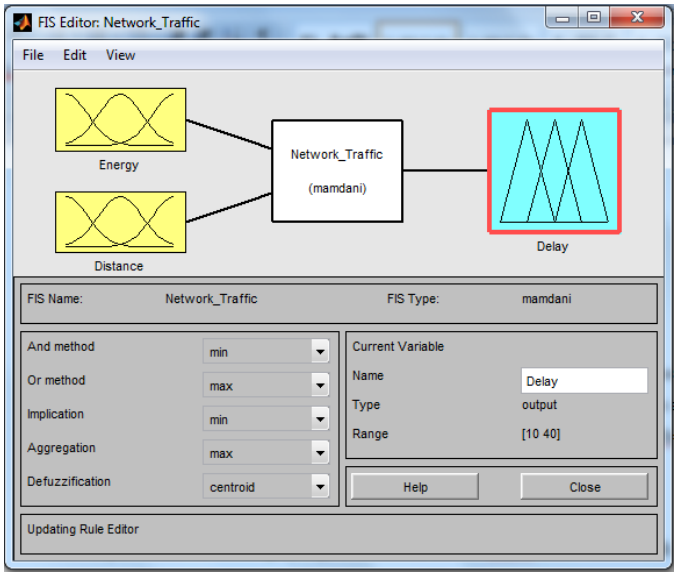


Figure 4.2: GUI of the Network_Traffic

This traffic ruler has paths, rules and 4 decision values as per the system generated. The energy spectrum, Distance spectrum and Delay variables shows different graph plotation as shown in figure 4.3, 4.4, 4.5.

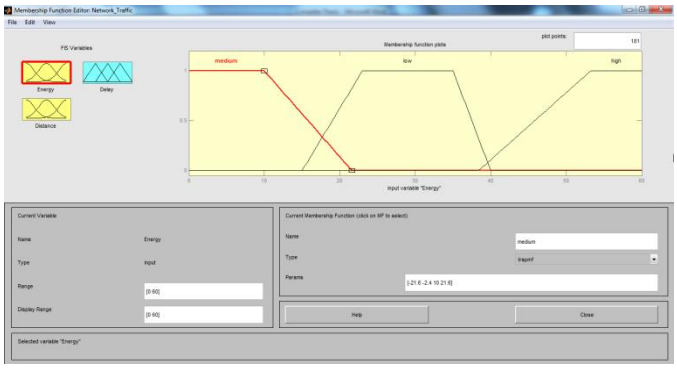


Figure 4.3: Energy Spectrum Graph.

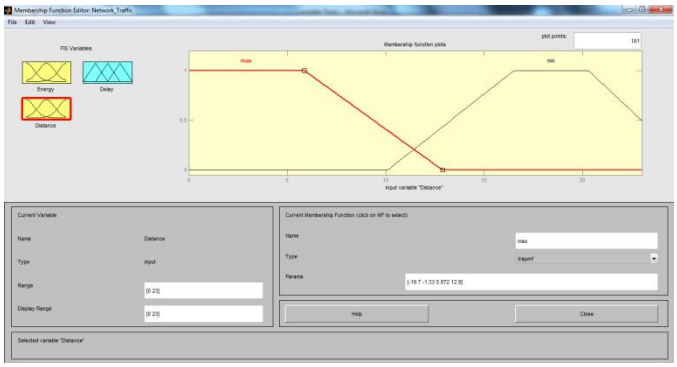


Figure 4.4: Distance Spectrum Graph

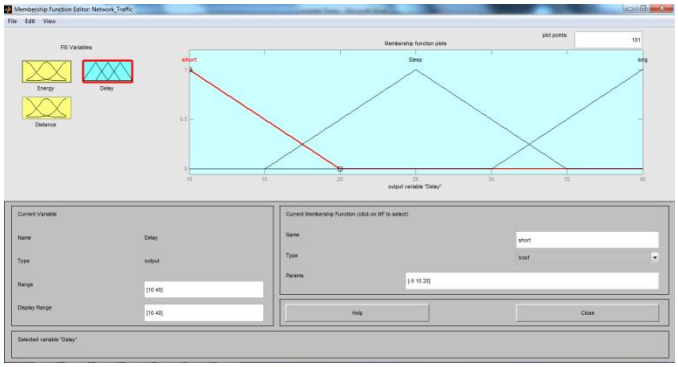


Figure 4.5: Delay Variables Graph

The four different rules of the traffic detection are shown by figure 4.6. These rules are:

If (Energy is **high**) and (Distance is **min**) then (Delay is **sleep**)
Else If (Energy is **high**) and (Distance is **max**) then (Delay is **long**)
Else If (Energy is **low**) and (Distance is **min**) then (Delay is **short**)
Else If (Energy is **low**) and (Distance is **max**) then (Delay is **sleep**)

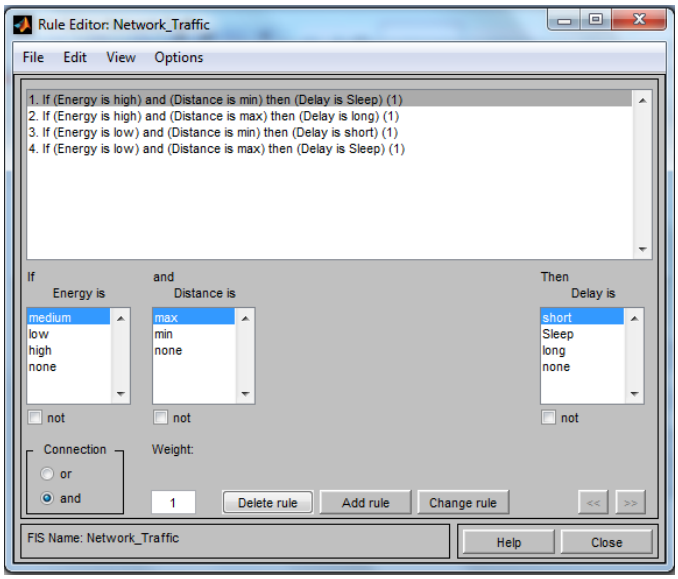


Figure 4.6: Network Traffic Detection Rules

B. Evaluation Parameter

To define the accuracy of proposed algorithm, we are defining parameters of Throughput, Packet Delivery Ratio and Path Optimality. These terms are defined for the comparison with simple AODV routing Protocol.

- **Throughput:** Throughput is the measure of how fast we can actually send through network. The number of packets delivered to the receiver provides the throughput of the network.
- **Packet Delivery Ratio:** The ratio between the number of packets received by the TCP sink at the final destination and the number of packets originated by the "application layer" sources. It is a measure of efficiency of the protocol

- **Path Optimality:** The difference between the number of hops a packet took to reach its destination and the length of the shortest path that physically existed through the network when the packet was originated.

C. Comparison with AODV

To check the accuracy of our proposed algorithm, we have considered the concepts packet transfer from the routing protocol of AODV. The comparison results are shown by figure 4.7, 4.8, 4.9.

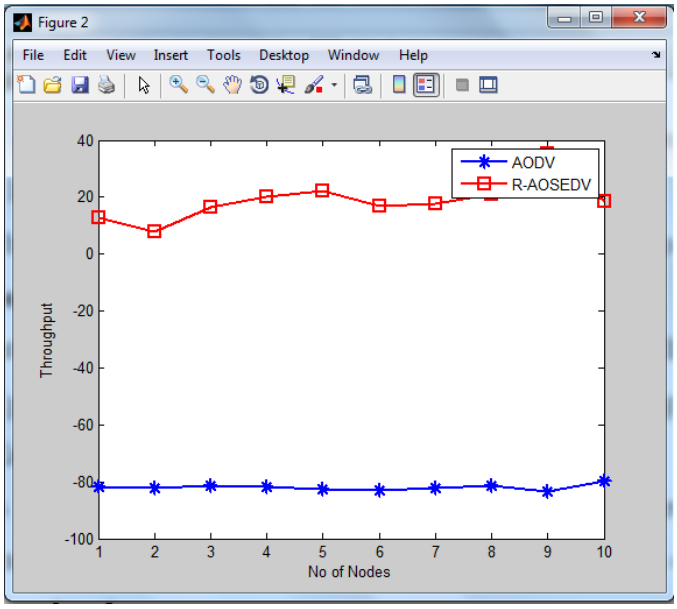


Figure 4.7: Throughput of AODV and Proposed Concept

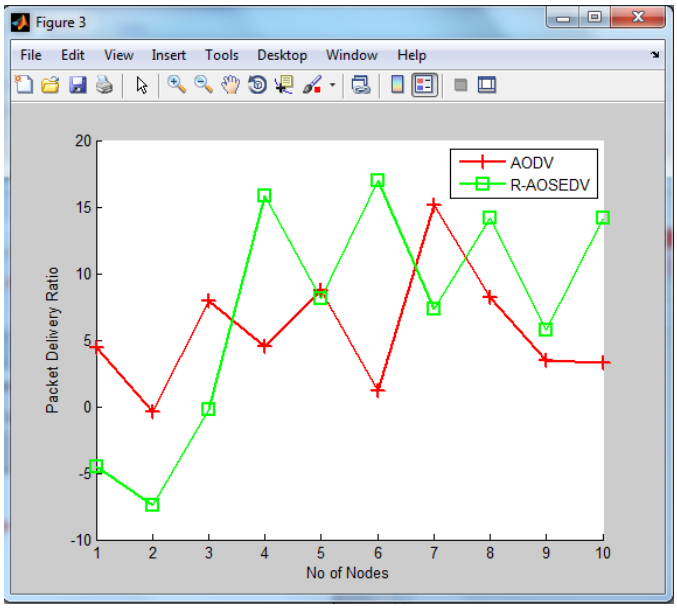


Figure 4.8: Packet Delivery Ratio of AODV and Proposed Concept

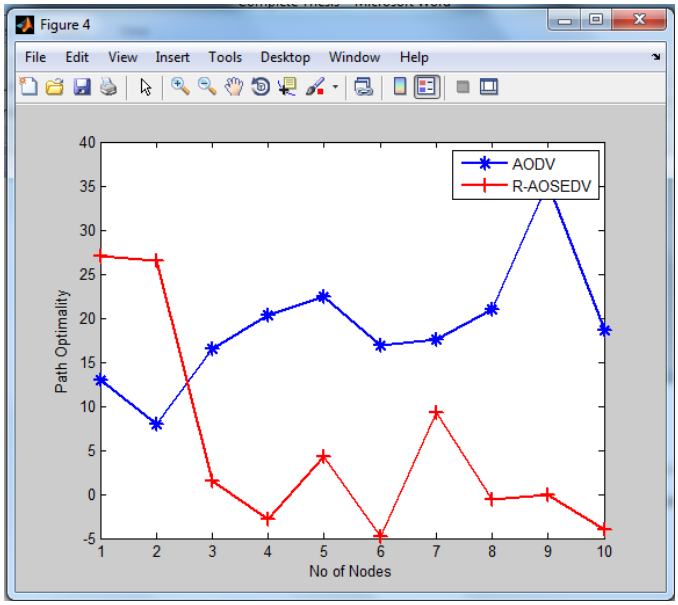


Figure 4.9: Path optimality of AODV and Proposed Concept

From the comparison results of figure 4.7, 4.8 & figure 4.9, we can say that our proposed Hybrid Fuzzy based AOSEDV concept performs better as compare to simple routing protocol of AODV.

V. Conclusion

The aim of this research work was to detect the sleep deprivation attack that interrupts the transfer of routing packets by reducing the resources of the system. The proposed algorithms in this research work has successfully completed the all these objectives by giving verification results in the form of evaluation parameters of Throughput, Packet Delivery Ratio and Path Optimality. We also have shown the proposed algorithm gives better results from AODV routing protocol by showing the graphical representation as shown in figure 4.7, 4.8 and 4.9. The proposed method not only identifies the attack, it also identifies the range and extension of attack. This proposed system provides the noble solution and identify the attack is clearer by using the fuzzy logic technique. The system also contains IPS mechanism technique which gets input from fuzzy technique and provides the secure data communication over the network.

References

[1]. Giordano, S. (2002). Mobile ad hoc networks. Handbook of wireless networks and mobile computing, 325-346.

[2]. Perkins, C. E. (2008). Ad hoc networking. Addison-Wesley Professional.

[3]. Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.

[4]. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., & Brooks, R. (2006). The sleep deprivation attack in sensor networks: Analysis and methods of defense. International Journal of Distributed Sensor Networks, 2(3), 267-287.

[5]. Bhattasali, T., Chaki, R., &Sanyal, S. (2012). Sleep deprivation attack detection in wireless sensor network. arXiv preprint arXiv:1203.0231.

[6]. Ross, T. J. (2009). Fuzzy logic with engineering applications. John Wiley & Sons.

[7]. Yen, J., &Langari, R. (1998). Fuzzy logic: intelligence, control, and information. Prentice-Hall, Inc..

[8]. Zadeh, L. A. (1996). Fuzzy logic= computing with words. Fuzzy Systems, IEEE Transactions on, 4(2), 103-111.

[9]. Zadeh, L. A. (1983). The role of fuzzy logic in the management of uncertainty in expert systems. Fuzzy sets and systems, 11(1), 197-198.

[10]. Turunen, E., &Turunen, E. (1999). Mathematics behind fuzzy logic. Heidelberg: Physica-Verlag.

[11]. Yager, R. R., &Zadeh, L. A. (Eds.). (2012). An introduction to fuzzy logic applications in intelligent systems (Vol. 165). Springer Science & Business Media.

[12]. Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[13]. Zapata, M. G. (2002). Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3), 106-107.

[14]. Chakeres, I. D., & Belding-Royer, E. M. (2004, March). AODV routing protocol implementation design. In Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on (pp. 698-703). IEEE.

[15]. Kashaf, A., Javaid, N., Khan, Z. A., & Khan, I. (2012, December). TSEP: Threshold-sensitive stable election protocol for WSNs. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 164-168). IEEE.

[16]. Mostafa, B., Saad, C., &Abderrahmane, H. (2013). Fuzzy logic approach to improving Stable Election Protocol for clustered heterogeneous wireless sensor networks. Journal of Theoretical and Applied Information Technology, 53(3).