Journal of Computer Science & Computational Mathematics, Volume 7, Issue 1, March 2017
DOI: 10.20967/jcscm.2017.01.002

Fuzzy Selfish Detection Ad hoc On-demand Distance Vector routing protocol (FSDAODV)

Mohammad Masoud Javidi*, Mahboobeh Vanday Baseri

Department of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran
*Corresponding author email: javidi@uk.ac.ir

***Abstract*:** A Mobile Ad hoc Network (MANET) is a decentralized infrastructure-less network where wireless nodes move arbitrarily. Every node has limited energy that is provided by battery. Some operations like taking part in finding rout, forwarding packets and receiving packets consume energy. So there are some nodes that are not willing to cooperate and want to save their energy called selfish. These nodes affect network performance and security. Recently security is one of the major challenges in network. So in this paper for detecting selfish nodes we proposed a new routing protocol.

***Keywords*:** Mobile Ad Hoc Network (MANETs), selfish nodes, security, Fuzzy Selfish Detection Ad hoc On-demand Distance Vector routing protocol (FSDAODV).

1. Introduction

Mobile ad hoc network called MANET consists of mobile nodes that are capable of communicating with each other without centralized control [1]. The node communicates directly with nodes in its transmission range. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers [2]. In MANET every node has limited energy with battery. Some nodes try to detach from network, because they want to refrain from cooperating in order to reserve their energy. These nodes can be classified into two groups: malicious nodes and selfish nodes. Malicious nodes can modify received packets or drop them. These nodes can cause denial of service (DOS) attacks. Selfish nodes have some traits like:

- They do not take part in routing process
- They do not send hello messages or delay the process
- They drop data packets [3].

In section 2, we explain routing protocol specially AODV and also different types of attack have been reviewed. In section 3, we review the related works. Section 4 is about proposed protocol and section 5 expresses simulation and results evaluation. In section 6 we present conclusion and finally section 7 is about future work.

2. Background

In MANET routing protocol can be classified into three groups [4]:

- Proactive routing protocol
- Reactive routing protocol
- Hybrid routing protocol

In proactive routing protocol each node maintains routing information to every other node in the network. The routing information is usually kept in a number of different tables. These tables are periodically updated.

Reactive (on-demand) routing protocol was designed to reduce the overhead in proactive routing protocol by maintaining information for active routes only. This means that routes are determined and maintained for nodes that require sending data to a particular destination.

Hybrid protocols are both reactive and proactive. These protocols are designed to increase Scalability and reduce the route discovery overheads.

2.1 AODV: Ad-hoc On-demand Distance Vector

It is one of the most popular MANET routing protocols [5] named as re-active or on-demand protocols. Upon arrival of data if no route exists, source broad cast a route request to the destination. Each intermediate node hop automatically builds a reverse route to the source and also rebroadcast the route request .The destination replies to the first route request and sends a route reply in the direction it was received. AODV finds the shortest path between the source and the destination. AODV cannot detect selfish nodes, so in this paper we improve this protocol for detecting these nodes.

2.2 Security in MANET

Security in MANETs is an essential requirement. Compared to wire networking, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, lack of trust relationships between mobile nodes, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices. They are also very easily eavesdropped because of shared wireless medium [6].

Attacks in MANETs can be divided in to two groups: active attacks and passive attacks. Passive attacks do not disrupt the network operations but active attacks alter the data transmitted within the network and prevent message flow between the nodes. Active attacks can be external or internal. Figure 1 shows classification of attacks in MANETs [7].

In this paper we focused on non-participation attacks and proposed new protocol for detecting them.

3. Relative work

Paul et al. [8] produced a new text inference mechanism based on informing other nodes about misbehaving nodes in routing protocol.

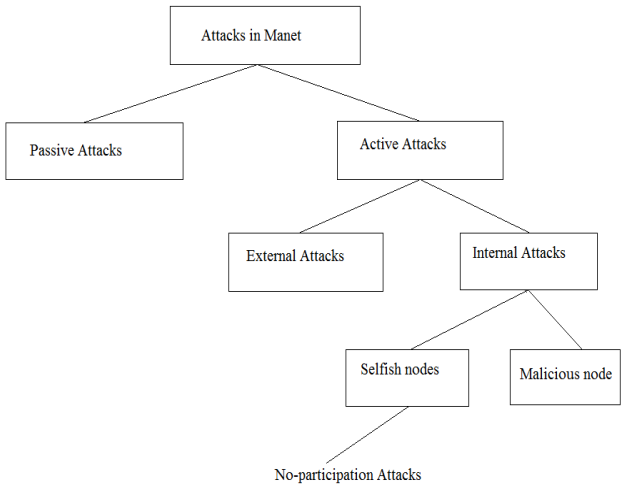

Figure 1. Classification of attacks in MANETs

Buchegger and Le Boudec [9] proposed CONFIDANT, an extension to the source routing protocol. CONFIDANT uses monitoring system for observation that includes a reputation system, trust manager and path manager. This protocol can detect and isolate anomaly nodes in the network. Watchdog mechanism is one of the basic security mechanisms that it was introduced in 2003. It is able to detect both malicious attacks and selfish behaviors. In this technique the misbehaving node is detected by listening on next hop transmissions. When a node sends a packet, watchdog checks whether the next node in route sends packet or not. If that node refrains to send packet, it is recognized as misbehaving node [10].

Hasswa et al. [11] introduced a simple method to detect misbehaving nodes. They classified nodes into fresh, member, unstable, suspect and malicious based on comparison between recent and previous nodes actions.

Abdalla et al. [12] concentrated on Optimized Link State Routing protocol (OLSR). Their proposed mechanism for detecting and removing misbehaving nodes was based on end-to-end communication between source and destination. One group of nodes cooperate with each other to determine these nodes. By creating a list of attackers and broadcasting this to all nodes, nodes can determine and remove misbehaving nodes from routing process.

Vijayan et al. [13] proposed energy-based trust solution for detecting selfish nodes that in this paper we named it EBTS (Energy Based Trust Solution). They used fuzzy logic in evaluating trust for misbehavior detection of selfish nodes in MANET. In their proposed scheme there are four steps as supervisor, aggregator, trust calculator and disseminator. They used the solution to calculate the trust for every node in MANET and to identify the selfish nodes taking energy utilization factor as a main factor in calculating trust.

Iacit et al. [14] presented multi hop acknowledgment scheme named N-Ack that was an extension of 2-Ack for detecting selfish nodes.

Hussain et al. [15] introduced new protocol for detecting selfish nodes called Selfish Node Detection Protocol (SNDP). They used clustering method in their proposed protocol. Three main stages exist in their protocol:

- monitoring nodes and collecting data
- detecting selfish node
- response

4. Fuzzy Selfish Detection Ad hoc on-demand Distance Vector routing protocol (FSDAODV)

In this paper we introduce a new routing protocol for detecting selfish nodes that is an improvement of AODV routing protocol. The following flowchart has been proposed:

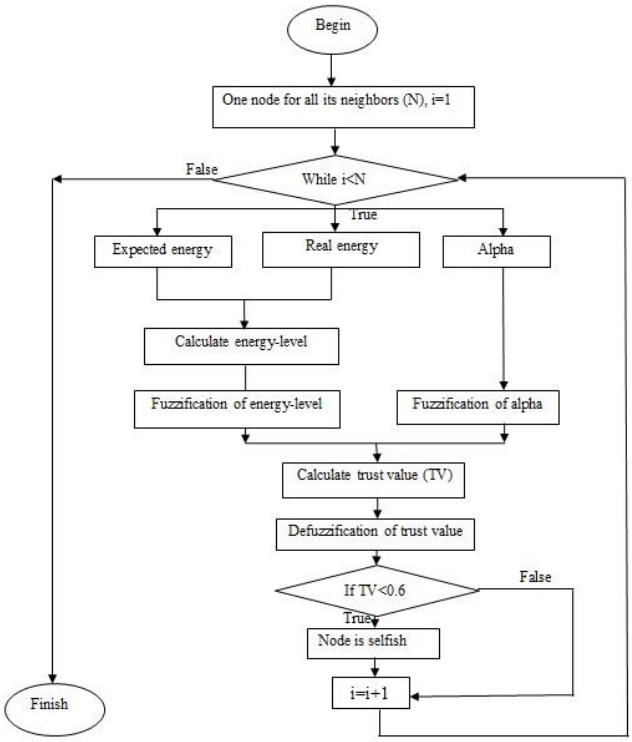

Figure 2. Flowchart of proposed protocol

In the proposed protocol every node acts as a judge node and calculates energy-level and alpha for all of its neighbors and then makes judgment about them. Energy value is carried in the hello packet header. N is the number of the judge node's neighbor. Some main parameters have been explained as follows.

Real energy

We determined four parameters for energy according to [16]:

- The initial Energy (initenery)
- The transmission power (txpower)
- Reception power (rxower)
- Remainder energy (Renergy)=initenergy

For a node initial energy will be reduced if it transmits or receives packets. Energy consumed during the transmission process (txenergy) and reception process (rxenergy) for one packet is calculated based on the following formula:
For sending packet:

$$txenergy = txpower\left(packetsize/bandwidth\right) \quad (1)$$

$$Renergy = Renergy - txenergy \quad (2)$$

For receiving packet:

$$\text{rxenergy} = \text{rxpower} \times (^{\text{packetsize}}/_{\text{bandwidth}}) \quad (3)$$

$$Renergy = Renergy - rxenergy \quad (4)$$

Alpha

We define alpha for every node by calculating node's direct neighbors as bellow:

$$alpha = (outC + outD)/(inpC + inpD) \quad (5)$$

InpC, inpD, outC, outD are the number of input control packet, number of input data packet, number of output control packet and number of output data packet, respectively. If alpha is 1 a node behaves in a good way but if it is less than 1 it shows that the node does not send all receiving packets and maybe it is selfish.

Expected energy(E-expect)

After an interval time (T) every node calculates the expected energy for each of its direct neighbor as bellow:

$$n = (inpC + inpD)_T \quad (6)$$

$$E_1 = rxenergy \times (n) \quad (7)$$

$$E_2 = txenergy \times (n) \quad (8)$$

$$E - expect = initenergy - (E_1 + E_2) \quad (9)$$

According to equations 2,4,7,8 and 9 energy is depleted by linear model.

Energy-level

So proportion of remainder energy on expected energy is defined as energy-level for every node.

$$Energy - level = {}^{energy}/_{E - expect} \quad (10)$$

Fuzzy logic

Fuzzy set is a generalization of conventional set theory that was introduced by Zadeh in 1965 as a mathematical way to represent vagueness in everyday life [17]. Fuzzy Logic deals with the analysis of information by using fuzzy sets, each of which may represent a linguistic term like "Warm", "High" etc. Fuzzy sets are described by a range of real values over which the set is mapped, called domain, and the membership function. A membership function assigns a truth value between 0 and 1 to each point in the fuzzy set domain. A Fuzzy system basically consists of three parts: fuzzifier, inference engine, and defuzzifier. The fuzzifier maps each crisp input value to the corresponding fuzzy sets and thus assigns it a truth value or degree of membership for each fuzzy set while the defuzzifier extracts a crisp value from a fuzzy set as a representation value [18].

Fuzzification of alpha and energy-level

So we define membership function for alpha and energy-level as bellow [19, 20]:

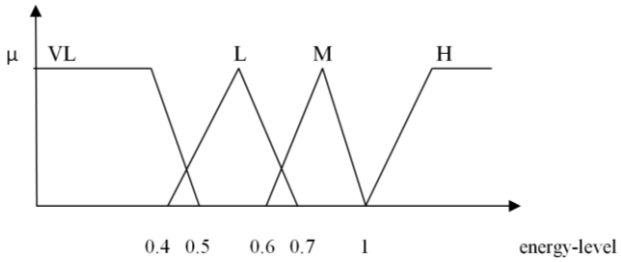

Figure 3. Membership function for energy-level

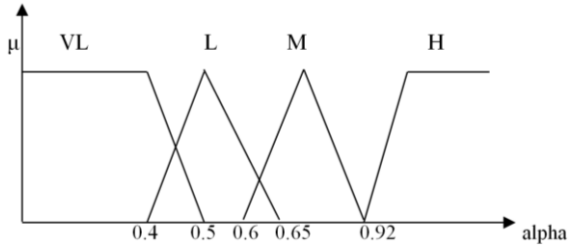

Figure 4. Membership function for alpha

Figure 5 shows membership function for four linguistic values : Very Low (0,0,0.3,0.4), Low (0.3,0.45,0.45,0.6), Medium (0.47,0.63,0.63,0.8) and High (0.7,0.8,1,1).

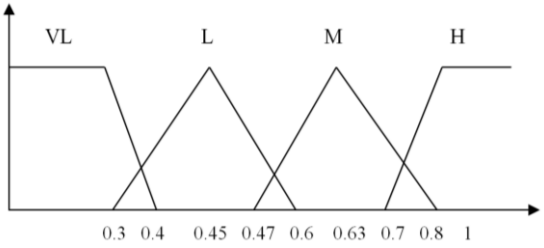

Figure 5. Membership function for four linguistic values

In the proposed protocol (FSDAODV) we define trust value (TV) for every node that depends on two parameters: energy-level and alpha. Energy-level has a reverse relation with trust value while alpha has a direct relation. Now suppose that energy-level and alpha are fuzzy inputs as bellow:

$e - l = (e_1, e_2, e_3, e_4) \qquad \alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

We obtain reverse of energy-level according to [19]:

$$e - l = (1 - e_4, 1 - e_3, 1 - e_2, 1 - e_1) = (E_1, E_2, E_3, E_4) \quad (11)$$

Finally TV is calculated [20, 21]:

$$tv = (t_1, t_2, t_3, t_4) \quad (12)$$

$$t_1 = \min(\alpha_1, E_1) \quad (13)$$

$$t_2 = \frac{\sum(\alpha_2, E_2)}{2} \quad (14)$$

$$t_3 = \frac{\sum(\alpha_3, E_3)}{2} \quad (15)$$

$$t_4 = \max(\alpha_4, E_4) \quad (16)$$

We defined four fuzzy rules:

1-If (energy-level is very low) and (alpha is very low) then (trust value is very low)

2- If (energy-level is low) and (alpha is low) then (trust value is very low)
3- If (energy-level is medium) and (alpha is medium) then (trust value is very low)
4- If (energy-level is high) and (alpha is high) then (trust value is very low)

Defuzzification of alpha and energy-level

In this stage we use average method for defuzzification of trust value:

$$Tv_B = {(t_1 + t_2 + t_3 + t_4)}/{4} \quad (17)$$

This TV is an opinion of node A about B, but A asks other direct neighbors' opinion (o_i) about B and finally calculates trust value [22]:

$$Tv_{BA} = w_1 \times Tv_B + w_2 \times Tv_{BOi} \quad (18)$$

$$Tv_{BOi} = \left({Tv_{O_1}}/{sum}\right) + \left({Tv_{O_2}}/{sum}\right) + \cdots + ({Tv_{O_n}}/{sum}) \quad (19)$$

$$sum = Tv_{O_1} + Tv_{O_2} + \cdots + Tv_{O_n} \quad (20)$$

Tv_{BA}: Final trust value that B calculates for A

Tv_B: Trust value that is just B's opinion

Tv_{BOi}: Trust value of B that is opinion of other direct neighbors (o_i)

w_1, w_2 are weighted for Tv_B and Tv_{BOi} that are 0.8 and 0.2.

In the protocol we define a threshold for trust value that equals to 0.6. If Tv_{BA} is less than the threshold, it is selfish, otherwise it behaves in a good way.

5. Simulation and results evaluation

We used MATLAB simulator and then compared our work with AODV routing protocol, EBTS and SNDP. In our simulation, nodes move according to Random WayPoint (RWP) mobility model. For simulation, we have fixed some parameters according to table 1 and table 2.
For comparing FSDAODV with AODV, SNDP and EBTS we used some criterions that are defined as bellow [15, 23, 24]:

- **Packet delivery ratio** (PDR): This is the percentage of the total number of packets received by the intended receivers to the total number of packets originated by all nodes.
- **Throughput** (Th): It is the number of packets/bytes received by source per unit time.
- **Packet dropped ratio**: This is the percentage of the total number of packets dropped to the total number of packets originated by all nodes.
- **Effect on Network Performance** (ENP): PDR and Th are two significant parameters for analyzing the effect of selfish nodes on network efficiency, so according to [15]:

$$ENP = a_1 \times \Delta Th + a_2 \times \Delta PDR \quad (21)$$

a_1, a_2 are 0.6 and 0.4 respectively.

Table 1. Parameters for calculating trust value

Parameter	Value
Initial energy	20 J
Bandwith	1.375*10^6 bit/s
Txpower	280 w
Rxpower	180 w
W1	0.8
W2	0.2
Threshold	0.6

Table 2. Parameters for simulation

Parameter	Value
Area size	200*200
Node speed	2 m/s
Packet size	512 byte
Number of nodes	30
Number of selfish nodes	0-15

ΔTh Shows the percentage of change in throughput value while ΔPDR Shows the percentage of change in packet delivery ratio.
Figure 6 shows PDR in the presence of different selfish nodes. It shows that FSDAODV operates better than others when number of selfish nodes is more than 10.

In figure 7 we have packets dropped as a function of selfish nodes. It represents that when the number of selfish node is more than 10, FSDAODV has less packets dropped in comparing to others.

Figure 8 shows percentage of throughput for various numbers of selfish nodes. It can be observed that when the number of selfish nodes increases, throughput will decrease while after 13 selfish nodes, FSDAODV throughput is better.

Figure 9 is about the effect on network performance. When number of selfish nodes increases the negative effect on network performance will increase too. So if ENP for

protocol is less, it acts better. In comparison with AODV and SNDP it is obvious that FSDAODV is better.

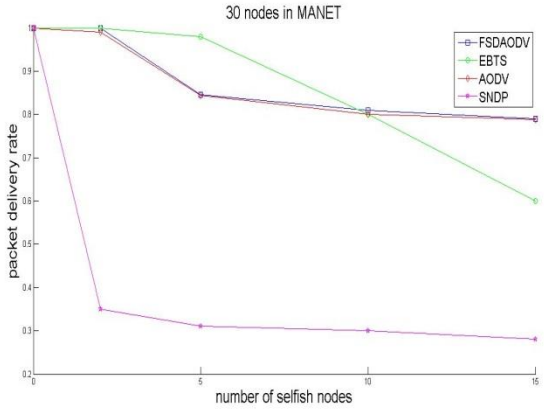

Figure 6. PDR as a function of number of selfish nodes

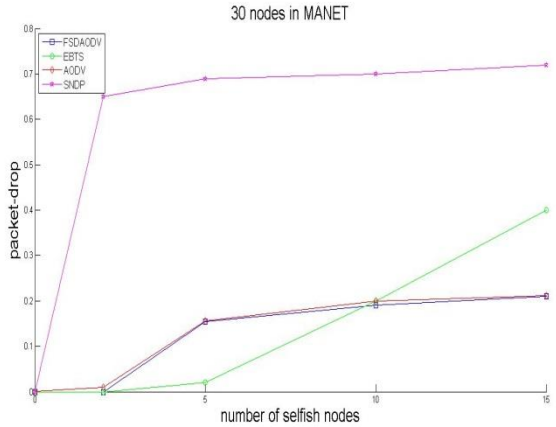

Figure 7. Packet dropped as a function of number of selfish nodes.

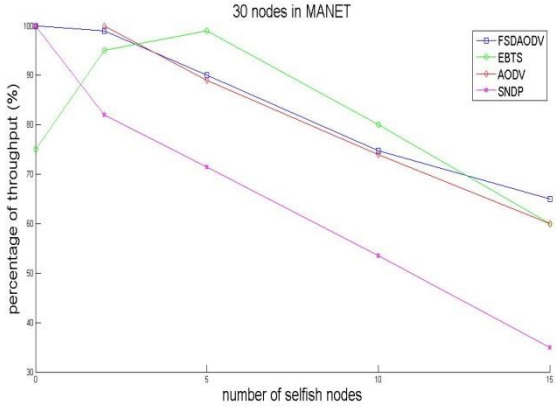

Figure 8. Throughput as a function of number of selfish nodes

Figure 10 represents consumption energy in FSDAODV protocol with deferent number of selfish nodes. It shows that when number of selfish nodes increases, consumption energy will decrease.

6. Conclusion

Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In MANET each node has limited energy, so some nodes do nott send packets. In this paper we proposed new routing protocol (FSDAODV) for detecting selfish nodes in MANETs. Energy and number of input and output packets were two most important parameters in our protocol. We used fuzzy logic in our protocol and also we compared FSDAODV with AODV, SNDP and EBTS.

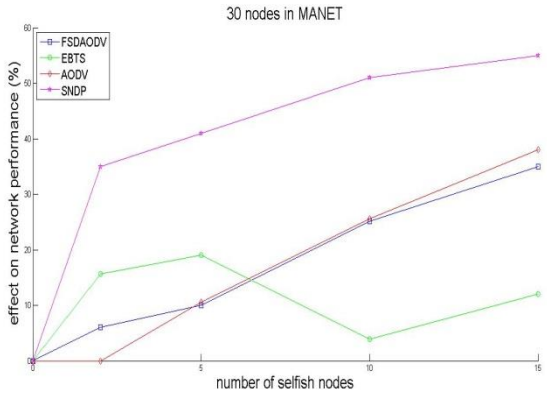

Figure 9. Effect on network performance as a function of number of selfish nodes

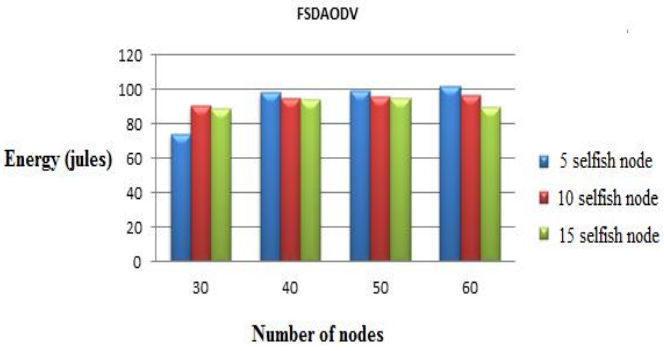

Figure 10. Energy as a function of different number of nodes with various selfish nodes

7. Future work

In this paper we just detected selfish nodes. In future we are aiming to remove selfish nodes from network. Also in fuzzy stage, we can use PSO algorithm for improving membership functions that it gives better result.

References

[1] D. Das, K. Majumder and A. Dasgupta, "Selfish Node Detection and Low Cost Data Transmission in MANET Using Game Theory", *Proceedings of Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)*, Bangalore, India, vol. 54, pp. 92-101, 2015.

[2] A. Rajaram and S. Palaniswami, "A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks", *International Journal of Computer Science Issues*, vol. 7, no. 5, pp. 37-45, July 2010.

[3] Sh. Gupta, C. K. Nagpal and Ch. Singla, "Impact of Selfish Node Concentration in MANETs", *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 3, no. 2, pp. 29-37, 2011.

[4] Shikha Jain, "Security Threats in MANETS: a Review", *International Journal on Information Theory (IJIT)*, vol. 3, no. 2, pp. 37-50, April 2014.

[5] M. Pushpalatha, R. Venkataraman and T. Ramarao, "Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks", *World Academy of Science, Engineering and Technology*, vol. 43, no. 21, pp. 37-40, 2009.

[6] H. L. Nguyen and U. T. Nguyen, "A Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", *Journal of Ad Hoc Networks*, vol. 6, pp. 32-46, 2008.

[7] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 1, no. 5, 2012.

[8] K. Pual, D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR Based Ad-hoc Networks", *Proceedings of the Global Telecommunication*, vol. 1, pp. 178-182, 2002.

[9] E. Chiejina, H. Xiao and B. Christianson, "A Dynamic Reputation Management System for Mobile Ad Hoc Networks", *Computers*, vol. 4, no. 2, pp. 87-112, 2015.

[10] Manoj V, Mohammed Aaqib, Raghavendiran N and Vijayan R, "A Novel Security Framework Using Trust And Fuzzy Logic In MANET", *International Journal of Distributed and parallel Systems (IJDPS)*, vol. 3, no.1, pp. 285-299, 2012.

[11] A. Hasswa, M. Zulkemine and H. Hassanein, "An Intrusion Detection and Response System for Mobile Ad hoc Networks", *Proceedings of the IEEE International Conference On Wireless and Mobile Computing*, vol. 3, pp. 336-343, 2005.

[12] A. M. Abdalla, I. A. saroit, A. kotb and A. H. afsari, "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", *Journal of procedia Computer Science*, vol. 3, pp. 115-121, 2011.

[13] Vijian R, Mareeswari V and Ramakrishna K, "Energy Based Trust Solution for Detecting Selfish Nodes in MANET Using Fuzzy Logic", *International Journal of Research and Reviews in Computer Science(IJRRCS)*, vol. 2, no. 3, pp. 647-652, 2011.

[14] S. Usha and S. Radha, "Multi hop Acknowledgement Scheme Based Selfish Node Detection in Mobile Ad hoc Networks", *Proceedings of the Information and Electronics Engineering*, vol. 3, no. 4, pp. 723-730, 2011.

[15] M. A. Hussain, A. Nadeem, O. Khan, S. Iqbal and A. Salam, "Evaluating Network Layer Selfish Behavior and a Method to Detect and Mitigate its Effect in MANETs", *Proceedings of the 15th International Multitopic Conference (INMIC)*, pp. 283 – 289, 2012.

[16] A. Gabri Malek, Ch. LI, Zh. Yang, N. Hasan.A.H and X. Zhang, "Improved the Energy of Ad Hoc On-Demand Distance Vector Routing Protocol", *ELSEVIER, Procedia of IERI*, vol. 2, pp. 355 – 361, 2012.

[17] J. Bezdek, "Fuzzy Models-What are They and Why", *IEEE transactions on fuzzy systems*, vol. 1, no. 1, pp. 1-6, 1993.

[18] T. Haider and M. Yusuf, "A Fuzzy Approach to Energy Optimized Routing for Wireless Sensor Networks", *The International Arab Journal of Information Technology*, vol. 6, no. 2, pp. 179-185, April 2009.

[19] B. L. Su, M. Sh. Wang, Y. M. Huang, "Fuzzy Logic Weighted Multi-Criteria of Dynamic Route Lifetime for Reliable Multicast Routing in Ad Hoc Networks", *Expert Systems with Applications*, vol. 35, no. 1-2, pp. 476–484, 2008.

[20] A. Yücel and A. F. Güneri, "A Weighted Additive Fuzzy Programming Approach for Multi-Criteria Supplier Selection", vol. 38, pp. 6281-6286, 2011.

[21] Chen-Tung Chen, Ching-Torng Lin and Sue-Fn Huang , "A Fuzzy Approach for Supplier Evaluation and Selection in Supply Chain Management", *International journal of production economics*, vol. 102, no. 2, pp. 289-301, 2006.

[22] Imran Raza, S.A. Hussain, "Identification of Malicious Nodes in an AODV Pure Ad Hoc Network Through Guard Nodes", *Computer Communications*, vol. 31, pp. 1796–1802, 2008.

[23]Y. Wang and M. Singhal, "On Improving the Efficiency of Truthful Routing in MANETs with Selfish Nodes", *Pervasive and Mobile Computing*, vol. 3, pp. 537–559, 2007.

[24] Z. D. Katheeth and K.K. Raman, "Performance Evaluation with Throughput and Packet Delivery Ratio for Mobile Ad-hoc Networks", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 5, pp. 6416-6419, May 2014.