GE-International Journal of Engineering Research
Vol. 5, Issue 1, January 2017 Impact Factor- 5.613
ISSN(O): 2321-1717, ISSN(P): 2394-420X
© Associated Asia Research Foundation (AARF) Publication
Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

ENERGY CONSUMPTION BASED EVALUATION OF AODV BY DETECTING SLEEP DEPRIVATION ATTACKOVER MANET

Er. Manpreet Kaur[1], Er. Sushil Lekhi[2]
[1]M.Tech Student, [2]Assistant Professor
Computer Science Engineering Department, Punjab Technical University
Rayat Institute of Engineering and Information Technology, Ropar, India.

ABSTRACT
A Mobile Ad hoc network (MANET) is configured by different mobile nodes. Its drawback is that it lacks in fix infrastructure like Wi-Fi devices or base stations. In MANET nodes communicate with each other without taking any help from centralized authority. The characteristics of MANET such as wireless medium, dynamic topology, etc. Various types of attacks are available on MANET but Sleep Deprivation Attack is also one of them. Our objective of this is to design a system that removes sleep deprivation attack based on danger theory. Energy constrained networks place the nodes into sleeping node in ordered to increase the network lifetime. Due to Sleep Deprivation Attack there is a big threat to lifetime of sensor network because it prevents the node from going into sleep node. To do this we designed algorithm classify and analyse the selfish node. After this we have to update or delete selfish node to increase the throughput.

Keywords— Sensor network, Denial, Sleep Deprivation Attack.

1. Introduction

MANET stands for "Mobile Ad-hoc Network" that can be configured by itself and can also change its location itsself also use wireless networks to connect with each other, they use medium such as cellular or satellite transmission. Ad-hoc on demand distance vector is a routing protocol for ad-hoc networks for large numbers of mobile nodes. Routes create in this protocol only when the routes requested by source nodes, giving the permission to the node to enter and leave the networks. In this protocol route will remain active upto the time when packets not reached the destination, at the time when source stop sending the packet it stops the route. It supports both unicast and multicast routing. Sleep Deprivation attack is distributed DOS attack, sleeping node connect with the MANET node as the network node, after this the malicious not start broadcasting the packet to the another nodes that it consumes energy and decrease the throughput. The malicious node in wireless network dramatically decrease the performance of the mobile nodes during their data transmission, if the malicious node increases in the networks it start consumption of energy to large extend due to the same network performance degrade with increase in the malicious node. In manet the data transmit between host and destination node according to the theory of the protocols design , these protocols are capable to find the path and route to send the packet to the destinations. Sometimes there may be the failure in the link between the communications nodes, due to the same reason the nodes choose another link to send the data , due to same there may the loss of energy occur. Above given figure no. 1 shows that communication between the nodes, are executed by using the gateway [1].

DIFFERENT KINDS OF ATTACKS ON WSN

The different kinds of attacks on sensor networks are [4]:

"**Black Hole attack**" back drop packet in which router suppose to the packet during transmission instead of discarding the packet when denial of service attack occur. In this attack the router become a

malicious router due to same behaviour its start dropping the packets to large extent, to overcome this problem we have to replace the malicious router with new one.

"Grey Whole Attack"In the AODV protocol every mobile node creates its own routing table in which it stores the path of the destination node, if the path exist in the routing table it send the packet through this path, if the path not exist then every mobile node send the RREQ REQUEST to all the neighbour nodes, if all the mobiles node does not have any path then every mobile node send s the RREQ request to their neighbour node, if this happen the intermediate node increment the routing table for reverse route to the sorce node. Then by doing this the AODV protocols intercepts the route to send the packet to destination and also it loss the packet through this interception route , so it is very difficult to identify the Grey hole attack.

"Warm Hole Attack"In wormhole attack, a malicious node takes packets from one location and place at another location. And create a tunnel between these two locations this tunnel is known as wormhole. It could be established between two clouding attacker through wireless and wired network. The attacker may create a tunnel even for packets node address to itself due to its broadcast nature. If proper mechanism are not used to protect wormhole attack then wireless and adhoc network are not able to find their routes

"Routing Table Attack "In routing table attack every node has its own routing table, the same helps to draw network topology for each node. When selfish node attack on this table then attacks nodes are not able to find any route. The reason for this attack by fabricating new control message and called fabricating attack.

"DoS Attack"The DoS attack is to flood packets to finish the services provided by intermediate nodes. Due to same network no longer available those attack can be launched against any layer of the network protocol stacks.

"Sleep Deprivation Attack": Sleep deprivation Attack introduced by starjno. This attack is victim of battery powered computing device such as node which try to remain in a sleep mode. The attacker deploys this attack by interacting with a node to keep in out of power by conserving sleep mode, and used to reduce the lifetime of the victim. Further this attack difficult to detect.

"SYN flooding": In this attack, a misbehaving node sends SYN packets in large amount to a victim node due to the same spoofing the return addresses of the SYN packets occur.

Distributed DoS: Distributed DoS attack try to prevent legitimate users from accessing the services offered by the network.

ENERGY CONSUMPTIONS IN WSN

Sleep Deprivation attack is distributed DOS attack, sleeping node connect with the MANET node as the network node., but its purpose is to consume the energy by going into sleeping mode.in a sleep deprivation attack, an malicious node send an huge amount of packets to another nodes to consume computation and memory resources

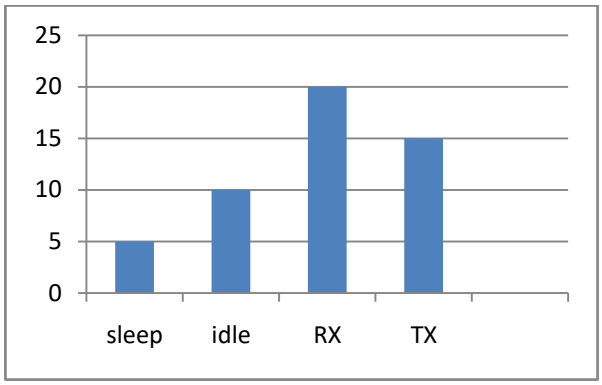


Fig.2 Energy Consumption

Fig. 2 the above figure shows that the energy consume is less when in the manet in AODV protocols not sending any packet to the destination it indicates it's better to keep node in sleeping node when the source not send any packet to the destination. But when the source is sending packets to the destination at that time if the node is sleeping then it consumes more energy.

THE APPLICATION OF SLEEP DEPRIVATION ATTACK OVER AODV ROUTING PROTOCOL

AODV is used as a large scale routing protocol. AODV may be affected by different attacks. This section is explaining Sleep Deprivation Attacks over MANET.As shown in figure 1 the source node sends the request (RREQ) with the help of MANET node and set the timer to wait for the reply. Every intermediate node checks the RREQ packets that are a fresh route to the destination. If yes then it sends the RREP packet to source node else the RREQ packet waits until it reach the destination. As shown in figure 2.

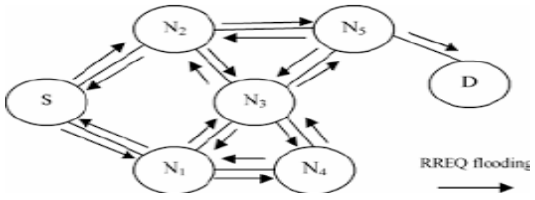


Figure 1: Propagation of RREQ packet

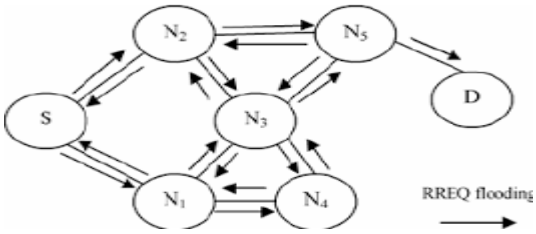


Figure 2: Path of RREP packet

The figure 3 shows how Sleep Deprivation Attack disturbs the route discovery process in AODV. By broadcasting RREQ packet it consume resources of energy, bandwidth and memory. The figure 4 shows how attacker keeps on sending RREQ packets when MANET links already had been congested with malicious node. That interrupts the services of the network.

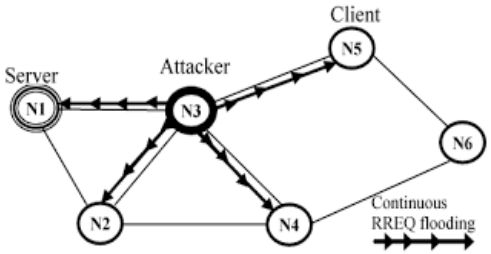


Figure3: RREQ broadcasted by sleep deprivation attacker

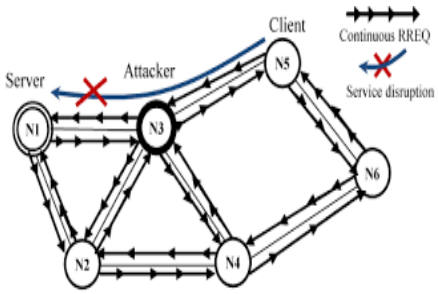


Figure4: RREQ packets flooding by sleep deprivation attacker

DANGER THEORY BASED AISs

This paper tells about the danger theory algorithm the danger theory algorithm tells that how to behave with the nodes when they are become the selfish nodes,Sleep Deprivation attack is distributed DOS attack, sleeping node connect with the MANET node as the network node., but its purpose is to consume the energy by going into sleeping mode.in a sleep deprivation attack, an malicious node send an huge amount of packets to another nodes to consume computation and memory resources. To overcome this problem in our danger theory algorithm we have to update the node which is sleeping node try to convert the specification of the node into the active nodes, if we are not able to get the node into the active node we have to change the route of the path in the end if everything fails we have to delete the node, when we deleteted the selfish node then the new path will be created to send the packet to the destination by using this the energy consumption will be less and it also decrease the packet delivery ratio and increase the through put.[10].

DETECTION OF SELFISH NODE

The credit risk [13] can be de-scribed by the following equation expected value of risk, if it is greater less than the expected risk then the node will mark as non selfish node else the node is selfish node, then node waits for replica allocation to be done. And if node is non selfish then for each connected node it replicates the replica of the node its share memory space and shared data item, else it does not replicate the shared data item and the shared memory space. And in algorithm 2, it updates the selfish node during route discovery, if any new node comes in the network then first it will treat as a non selfish node and in route discovery if it serves the query then according to algorithm the shared data item added into the network and also shared memory size added into the network. If new node does not serves the query then increase the expected risk value of the node and remove the shared data item and memory size.

- **Algorithm 1**: **Detection of malicious node**

During every relocation time
/* N_j used to detect malicious node */
Detect () {
For (every connected nodeN_p)
{

$$nCR_i^k < \delta$$
$$N_p$$

IF ( )N_p marked as non-malicious node
ELSE market this as malicious node ;}
Look for next relocation period;
For ($for\ each\ connect\ node\ \ N_P$) {
IF (N_j has allocate replica to N_p) {
ND_i^k = replica allocated;
SS_i^k = size of the replica;

}

ELSE {
ND_i^k = 01;
SS_i^k =Data Item size;
}}}

- **Algorithm 2: UPDATING THE SELFISH NODE**

During query processing time

/* at time when N_j issues a query */

Modify () {

WHILE (at predefined time w) {

IF (special node serves the query)

ReduceP_i^k;

IF (the special node N_j evaluates the query)

{

In mathematical form it can be written to detect selfish node at relocation period, node Ni detects maliciousnodes}}

ND_i^j = +1;

SS_i^j = + (data item size);

Credit Risk = $\frac{\text{Expected Risk}}{\text{Expected Value}}$

Algo 2 judge the value at query processing time according to algo2.According to 1 first node will check the credit risk value by}}

If (a selected node N_p does not evaluate the query) {

P_i^k

ND_i^k

SS_i^k

Increase;

ND_i^k = -1;

SS_i^k = - (Data item size);

$$nCR_i^k = \frac{P_i^k}{\alpha * \widehat{S_I} + (1-\alpha) * \widehat{n_i}}$$

Deletion Algorithm:

The proposed MDCA pseudo code

Used to store "Input Packet ID" in Queue

WHILE

Queue packet! =NULL then receive packet ID, Now Checking of"Packet ID" in memory

IF (packet ID exists)

Underline the List

ELSE

Discard the list and delete the packet detail from the routing table

Then

Start sending beep message

Else If

Packed ID exist in beeped message list

Then

Discard packet

Delete information of route

Else

Extract Packet foreign substance and transfer

Packet foreign substance to foreign substance Store

Extract signal and transfer

Signal to Signal Buffer and Call DCA

IF

Foreign Substance is begin

Then

Receive the packet and start the Danger Theory

algorithm

ELSE

Discard the packet and delete the routing information

And broadcast the beep message and

store the packet ID in beep message list

END IF

END IF

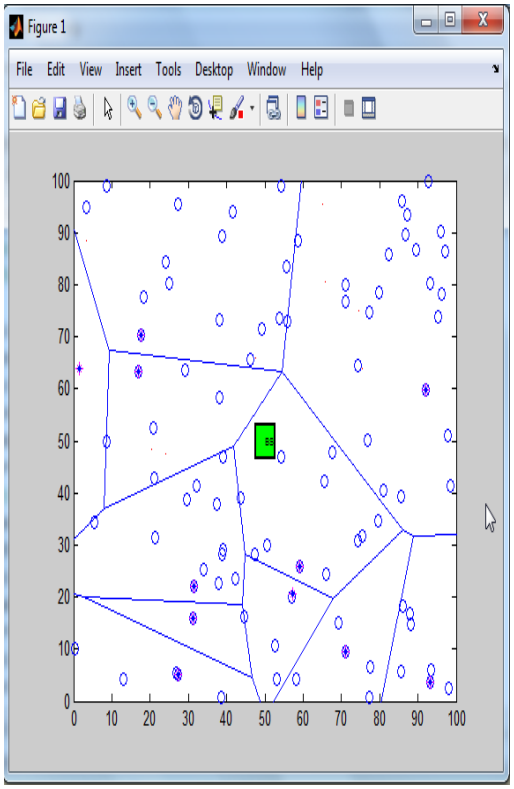
END WHILE

RESULT & DISCUSSION

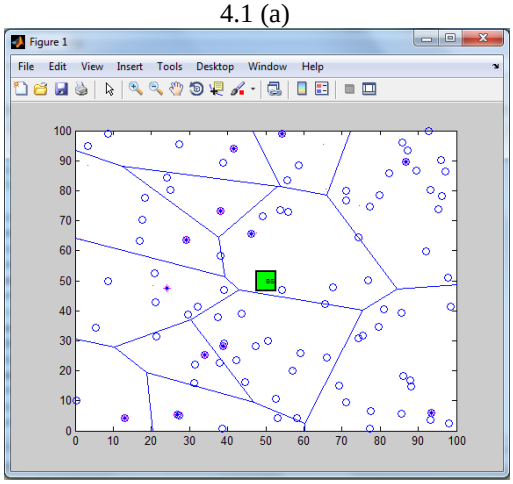
This section examines the performance of the proposed algorithm. It also provides a performance comparison between proposed algorithms with the existing one.

A. Experimental Setup

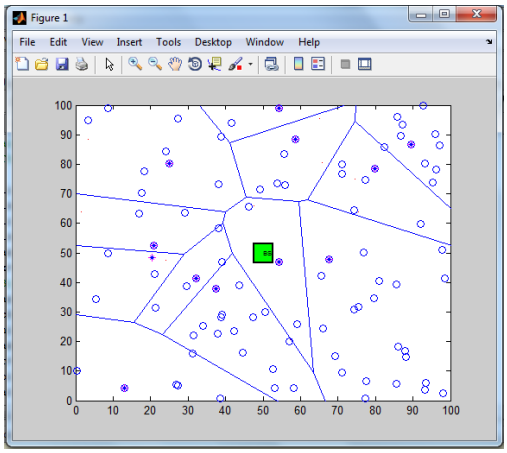
The experimental setup is done to detect the attack of the hacker, if found any then with the help of AOSEDV algorithm IP address is changed and finally path changed. These results are setup with the value of Base Station (BS) in the centre of the routing protocol and packets has to be send. The system 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.



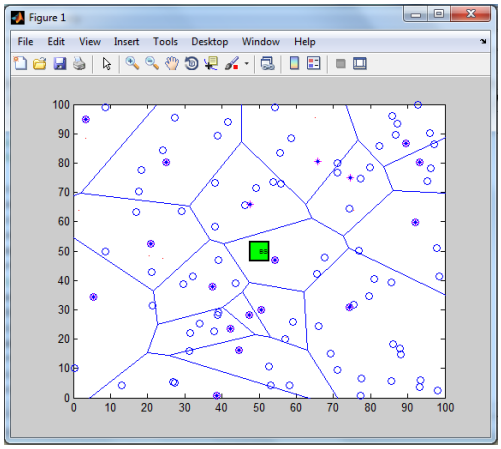
4.1 (a)



4.1 (b)



4.1 (c)



4.1 (d)

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

Simulation scenario that I have used to calculate Residual Energy (E) as given in equation 5.1, Packet Delivery Ratio (PDR) given in equation 5.2 and Average throughput given in equation 5.3 of protocols such as AODV (Before deleting selfish node) and AODV (After deleting selfish node). Node value is varied from 50 to 300 in scenario. Scenario is presented in Table 5.1 below.

S. No.	Parameter	Value
1	No of Nodes	50-300
2	Traffic Load(kbps)	5
3	Simulation time	400 seconds
4	Data Pattern	Node-UDP
5	Routing Protocols	AODV
6	MAC type	MAC/802.11
7	Simulator	NS-2.35
8	Speed	0.5 m/s to 1.5 m/s
9	Antenna Type	Omni Directional

The results of the simulation are as follows in Table 5.2

Table 5.2: Energy Consumption Result

NODES	AODV(Before)	AODV(After)
50	89.51	85.07
100	85.72	88.55
150	93.17	89.87
200	88.11	91.49
250	83.47	87.13
300	80.92	78.39

Figure 5.1 Energy Consumption vs. Nodes used for AODV based upon results given in the Table 5.2

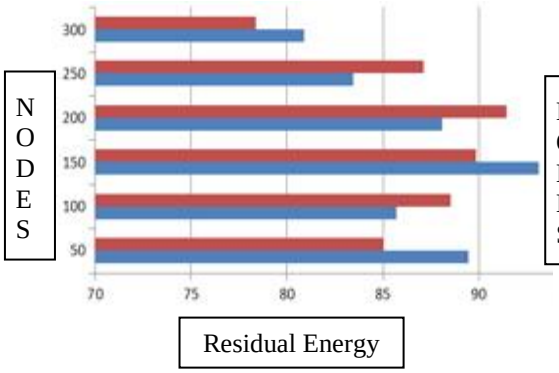


Figure 5.1: Energy Consumed verus Nodes

In the above **Figure 5.1**, Energy Consumed for AODV Protocol before and after detecting selfish node. It is clearly observed from figure that in case of lower number of nodes AODV (After deleting selfish Node) is more energy efficient than AODV(Before deletion of selfish node) and consumes less energy at 300 number of node value.

5.3.2Packet Delivery Ratio vs. Number of Nodes

Table 5.3: The Result for PDR (Packet Delivery Ratio)

NODES	AODV(AFTER)	AODV(BEFORE)
50	162.33	158.1
100	112.67	108.31
150	93.17	90.37
200	80.66	74.84
250	69.43	64.38
300	63.32	54.43

NODES

NODES	AODV(BEFORE)	AODV(AFTER)
50	0.9954	0.9695
100	0.984	0.9448
150	0.9834	0.9582
200	0.9631	0.9073
250	0.9343	0.8688
300	0.9123	0.7951

Figure 5.2showsthe graph for Packet Delivery Ratio for AODV before deletion of selfish nodes and AODV after deletion of selfish node, based on the simulation results given in Table 5.3.

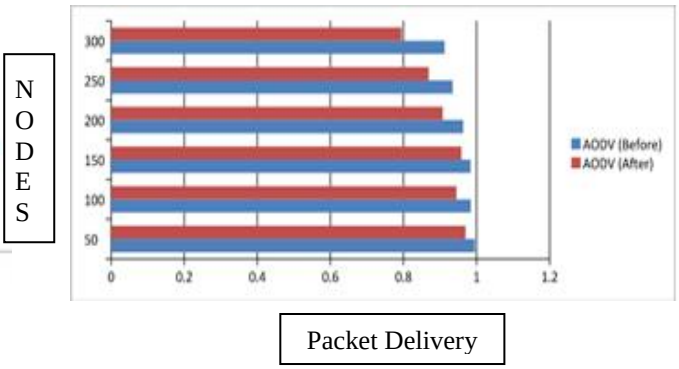


Figure 5.2: Packet Delivery Ratio versus Number of Nodes

It is clearly observed that PDR value of AODV (after deletion of selfish node) is similar for lower number of nodes. But AODV (after deletion of selfish node) performs well for higher number of nodes.

5.3.3 Average Throughput vs. Number of Nodes

Results are given below in Table 5.4

Table 5.4: Results for Throughput

In Table 5.4 we have observed that with increase in number of nodes the value of Average Throughput decreases because of higher congestion and higher computation requirements.

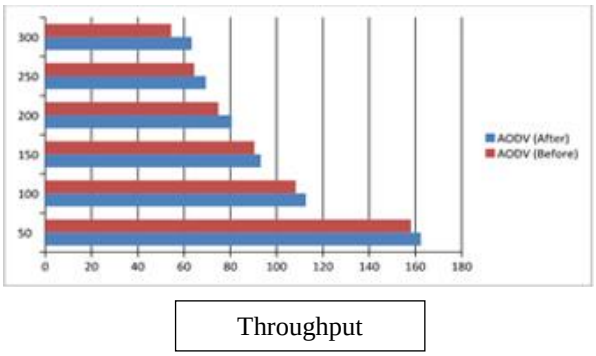
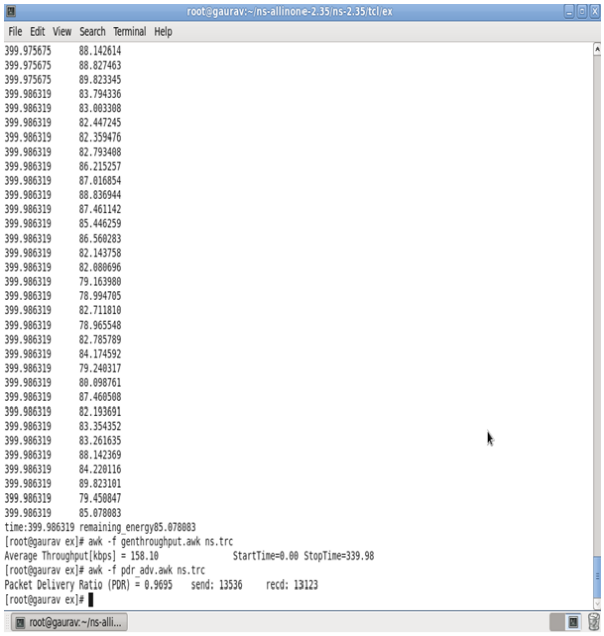


Figure 5.3: Graph representing Average Throughput versus Number of Nodes

As shown in **Figure 5.3** the graph of protocols is almost overlapping for lower number of nodes for example number of nodes below 150. AODV (after deletion of selfish node) is performing better than AODV (before detecting selfish node) with higher number of average throughput because of efficient

routing paradigm which leads to comparatively higher packet transfer. Here are some of the screenshots of research work.

Screenshot: Showing the Result of AODV protocol using 50 nodes network& 400 simulation time



CONCLUSION AND FUTURE SCOPE

The most import issue in the wireless sensor network designing is the Security and energy efficiency, because wireless sensor networks are affected due to different types of network attacks and intrusion. The purpose of the thesis is to detect the malicious node and identify the attacker. We term this problem the malicious node problem. “Danger Theory based on AIS” algorithm to detect the Energy Consumption based Evaluation of AODV to increase the throughput over MANET. This thesis entitled, Sleep Deprivation Attack, the hacker keep sending the route request packet in order to include every node continuously and due to same try to observe energy bandwidth and memory. The attacker starts overflowing the network with a route request. Due to the same attack the link has been congested with the malicious packet due to the same service of server isolated by the attacker. To avoid this be used “Danger Theory based on AIS.” So, my thesis is used for better energy consumption after detecting malicious node for the performance parameter like energy, PDR (Packet Delivery Ratio) and throughput is improved. After detecting malicious node.

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).