Investigating the effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks

Bikram Ballav
M Tech Student, Computer Science & Engineering Dept
ITER, SoA University Bhubaneswar, Odisha, India

Binod k Pattanayak
Associate Professor, Computer Science & Engineering
Dept ITER, SoA University Bhubaneswar, Odisha, India

Summary
Mobile Sensor Network(MSN) is a collection of mobilizer attached sensor nodes which can move randomly or task specifically. Routing is a basic step for data exchange in MSN. The routing protocols designed for ad hoc networks are suitable to MSN because they support mobility but due to resource constraint nature of MSN these protocols are not used directly. Hence we need new protocols. Zone based Energy Efficient Routing Protocol (ZEEP) is one of the new protocol in this direction which is the modified form of famous Ad Hoc On Demand Distance Vector Routing Protocol (AODV). The broadcasting nature of the sensors presents a number of security threats to this kind of network. Black Hole Attack is one such deadly attack, which grasps all data packets of the network. Since data packets do not reach the destination, data will loss. Which badly affects the performance of the whole network. In this paper, we investigate this issue and proposed a new protocol known as Black Hole affected ZEEP or BZEEP. We compare the performance of Black Hole affected AODV or BAODV and BZEEP by using multiple graphs and our results show that the effect of Black Hole Attack is less in case of BZEEP. For simulation purpose Network Simulator version 2.35 has been used.To support our views we used two quality of service parameters like Packet Delivery Ratio and Throughput. And analyzed them using graphs about how they have improved with BZEEP.

Key words:
Mobile sensor network, Energy efficient routing, BAODV, BZEEP

1. Introduction

Increasing use of mobile devices brings new dimension in wireless communication area. The concept of mobile wireless sensor network in the context of ubiquitous computing has emerged in recent years. Currently, most of the connections among these wireless devices are achieved via fixed Infra- structure based networks. While infrastructure based networks provide a great way for mobile devices to provide network services, it takes time and potentially high cost to set up the necessary infrastructure. There are many situations where user required networking connections are not available in particular geographic areas, and providing the needed connectivity and network services in these situations becomes a real challenge[1].For all these reasons, combined with advanced processing speed and memory capacity, new alternative ways to deliver mobile connectivity have been emerged.

Here comes the story of Wireless Sensor Network or WSN. WSN is a collection of sensor nodes that measure local environmental conditions like temperature, sound, pressure etc and forward such information to a base station for processing [1].

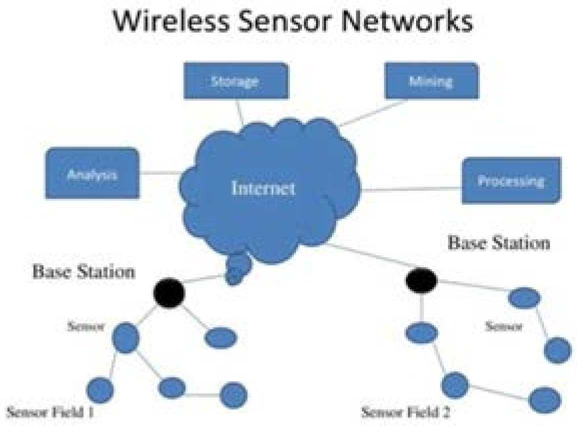


Figure 1: The structure of Wireless sensor Network

Figure 1 describes the structure of a wireless sensor network.The application scenarios for WSN includes environmental monitoring, military surveillance, digitally equipped homes, health monitoring, manufacturing monitoring, vehicle tracking and detection etc [2-4].
A Mobile wireless sensor network (MSN) can be defined as a wireless sensor network (WSN) in which the sensor nodes can move within the network. Mobility is achieved by equipping mobilizers or springs or wheels to nodes. These nodes can be attached to transporters like animals, vehicle, robots etc. Sometimes these nodes have to move due to the environment where they are placed.

Manuscript received July 5, 2015
Manuscript revised July 20, 2015

Recent research has proved that MSN outperformed the static WSN[5]. Here some advantages of MSN-

Mobility can reduce energy consumption during communication that actually increases the lifetime of the network.

By reducing number of hops, the probability of error decreases and data fidelity can be achieved by MSN.

MSN can achieve better targeting Mobile sensor networks are believed to have more channel capacity as compared to static wsn

Also mobility helps in better quality of communication between sensor nodes

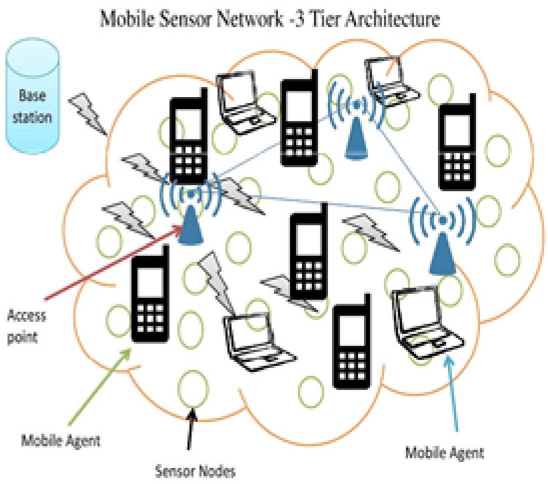


Figure 2: The architecture of a three tier MSN

Figure 2 describes the three tier architecture of a mobile sensor network. Sensor nodes are deployed randomly in the network, they can communicate with each other and mobile agents. At any time those mobile agents can move anywhere and they are responsible for collecting sensed data and forwarding them towards fixed network consisting of access points. Access points communicate with base stations to forward the data.

Not only advantage there also many disadvantages, the introduction of mobility in WSN is a very challenging task due to path breakage and node failure. Also frequent location changes can lead to drain of energy which increases number of collisions. Since, mobile wireless sensor networks are a relatively new concept; its specific, unique application areas are yet to be clearly defined. Most of its application scenarios are the same as that of traditional wireless sensor networks, with the only difference of mobility of mobile sink, preferably in the form of mobile phones.

Routing plays an important role to identify paths and transfer data towards base station in energy constraint sensor network. Energy is consumed more during path finding and data transmission operations.Initially routes are defined by the nodes then nodes become able to send or receive the data by using those routing paths[6].It is possible that if sensed data is available to some segments of network,but network is not able to transfer it to the destination due to the energy deplete of sensor nodes for some segments. To solve these energy efficiency issues several energy efficient routing protocols have been developed recently. In wireless networks routing protocols normally specified into following types:

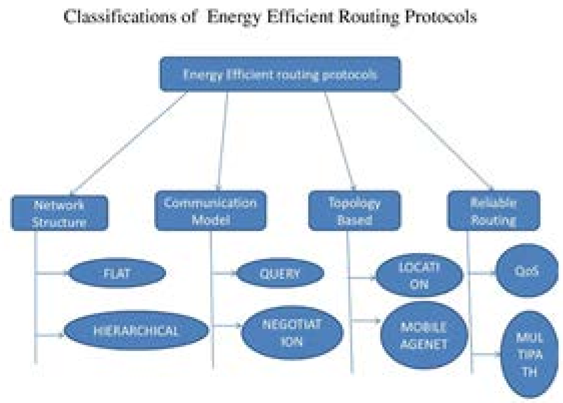


Figure 3: Classification of energy efficient routing protocol

This routing protocols works in broadcasting manner, like if source node wants to send data to destination node then it broadcasts route request to it's neighbor nodes. This approach makes them vulnerable to several kinds of attacks, black-hole is one such attack where data packets are dropped by intermediate malicious node.

2. PROBLEM STATEMENT

In this paper we discuss about energy efficient routing protocol, why it is zone based, effects of black-hole attack on one such newly developed protocol ZEEP and analyze the results how black-hole effects on ZEEP based on some parameters.

This paper is organized in five sections. In the next section,we will present and discuss the working principles of ZEEP. Fourth section will elaborate black-hole attack and how it causes problem for ZEEP, here we describe our proposed protocol BZEEP. Fifth section analyzes the performance of existing and proposed protocol with two Quality of Service(QOS)parameters using different graphs. Sixth section describes the conclusion and future work followed by references.

3. RELATED WORK

ZONE BASED ENERGY EFFICIENT ROUTING PROTOCOL:
In Energy efficient routing protocols sensor nodes save their energy level by using different techniques to increase node and network lifetime. Energy efficiency is a critical issue in MSN. The existing energy-efficient routing protocols often use residual energy, transmission power, or link distance as metrics to select an optimal path. There are many energy efficient routing protocols exist, in this paper we will discuss one such protocol ZEEP. Introduction of zone increase energy efficiency as only zone head have the authority to send and receive data from other zone heads and base station. For this facility other member nodes may not active all the time, it saves nodes energy and increase network lifetime. Obviously the node with highest energy selected as a zone head.

In ZEEP we have to calculate first mobility factor to select zone head.The goal of this protocol is to reduce the number of control packets when searching for a route. Figure 4 shows how it works.It has two phases.

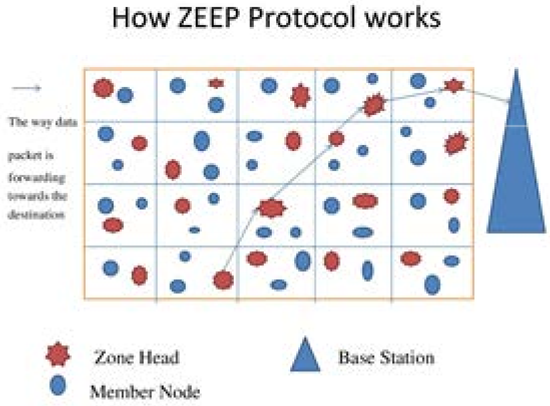
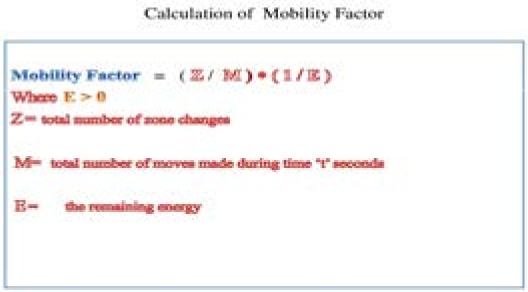


Figure 4: Working principle of ZEEP

Phase 1: Zone Head Selection based on Mobility Factor - The mobility factor is the node's remaining energy and the number of zone changes it makes at a particular instant. Figure 5 describes how it is calculated. A smaller value indicates less mobility and therefore a good contestant for the zone head selection. If a node with more remaining energy and lesser mobility factor is seen in comparison to the current zone head, then this node becomes the new zone head. The process of zone head selection is repeated periodically.

Phase2: Packet Forwarding- Each node in the network, including zone head and base station possesses a unique identifier and is named as Node ID. Each node will keep track of its mobility factor; number of zone changes it made, the zone size, and a zone table[7]. This table maps the zone ids and the corresponding locations to which they are attached and a zone head. A maximum of 10 entries is present in a zone table.When a source node is ready to send the data it initially checks whether it is a zone head or not. If it is not a zone head it sends a control packet to corresponding zone head.That zone head send control packet to it's nearest zone head towards destination.



Calculation of Mobility Factor

Mobility Factor = (Z / M) * (1 / E)
Where E > 0
Z= total number of zone changes

M= total number of moves made during time 't' seconds

E= the remaining energy

Figure 5: Mobility factor calculation for zone head selection

Once this control packet is received by the base station it sends acknowledgement back to the source by considering the distance factor. Once the acknowledgement is received by the source, the source starts sending the data. The base station acknowledges for each and every packet. If the source node does not receive any acknowledgement for the data packet it stops sending the data and sends the control packet periodically until the control packet is delivered. This helps in maintaining consistent path towards the base station[7].Next section describe the black hole attack and our proposed protocol.

4. PROPOSED PROTOCOL

A. How Black hole attacks ?

In this section we first describe how black hole attack works for normal on demand based protocol next we show our proposed protocol BZEEP working principle.

Black hole is one kind of security attack where a malicious node sends fake routing information, claiming that it has an optimum route towards destination and causes other good nodes to route data packets through the malicious one. This is a famous ad-hoc routing attack where nodes are dropped.

Figure 6 shows an example of a black-hole attack, here node1,which is a source node wants to send data packets to destination node 4,and initiates the route discovery process by broadcasting RREQ packets. We assume node 3 to be a malicious node with no fresh enough route to destination node4.However,node3 claims that it has the route to node 4 whenever it receives

RREQ packets from1,by increasing its Destination sequence number and decreasing number of hop counts towards 4 and sends the response to source node1.

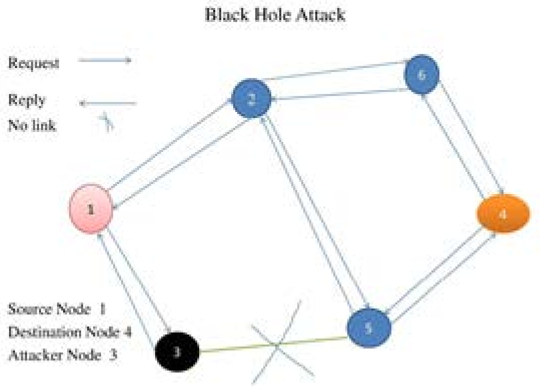


Figure 6: Black hole working principle

The destination node and any other normal intermediate nodes that have the fresh route to the destination may also give a reply.If the route reply from a normal node reaches the source node of the RREQ first, there is no problem. But the reply from malicious node3 could reach the source node first, as node3 is nearer to the source node1.Moreover,node3 does not need to check its routing table when sending a false message[8]. This makes node1 to think that route discovery process is complete, ignore all other reply messages and begin to send data packets to node3.As a result of that all packets through node3 are consumed or lost.Node3 forms a black-hole in the network. And we call this problem is a Black-hole problem[9].In this way the malicious node3 can easily misroute a lot of network traffic to itself, and could cause an attack to the network with very little efforts on its part.

B. How BZEEP works?

In Normal ZEEP or NZEEP first we calculate the Mobility Factor (MF) for each node to select the zone head or ZH. Then only corresponding zone head or ZH transfer the data towards the base station by first sending the control packet to it's nearest ZH then sending the data packet after creating the route.

Mobility factor is calculated from remaining energy and observing the total number of moves and from those moves number of move causes zone changes.For each node we need to calculate the MF then for each zone compare the MF of each node with other ones.The node which have Less MF will be the zone head (ZH).After selecting ZH we can send the packet to base station by first create the route through control packet then sending data packet along the path.

Now in case of Black-Hole Attack in ZEEP the malicious node show it's remaining energy high above than other nodes in it's zone.For that it's MF is low than compared to remaining nodes in the zone.When a malicious node enter the zone it enter as a normal node then show it's MF and compare with ZH it's obvious that this node have less MF than current ZH.This makes malicious node current ZH.After becoimg the ZH it can able to communicate with source node. Now if this malicious ZH is in the route of data packets send by source node towards base station. It capture those packets and drop them.

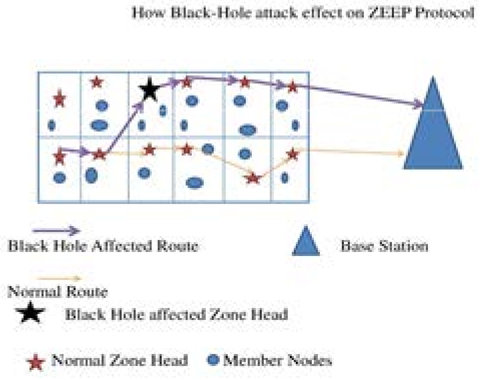

How Black-Hole attack effect on ZEEP Protocol
Black Hole Affected Route
Base Station
Normal Route
Black Hole affected Zone Head
Normal Zone Head
Member Nodes

Figure 7: Black hole affected path Vs Normal path in ZEEP

Figure 7 shows you the black-hole affected path and normal route to send the data packets.That blackhole affected path does not exist in reality.Malicious ZH show this path to source zone head so that it can send it's data packets along this malicious node.

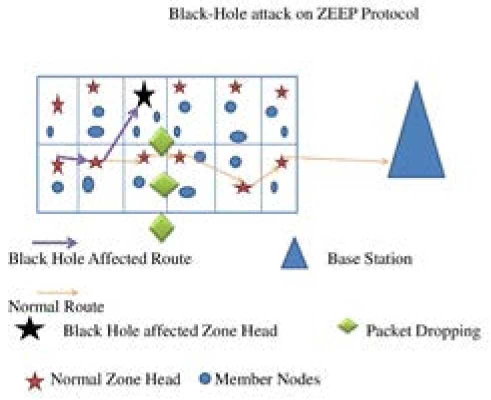

Black-Hole attack on ZEEP Protocol
Black Hole Affected Route
Base Station
Normal Route
Black Hole affected Zone Head
Packet Dropping
Normal Zone Head
Member Nodes

Figure 8: Drop of packets due to black hole attack on ZEEP

Now in figure 8 you can see how the packets are dropping when packets are passing through malicious ZH.This phenomenon affect the effectiveness of the whole network.

Due to this attack the data packets cannot reach the destination and packet delivery ratio along with throughput affected very much.Mobility cause path breaks but black hole attck grasp all packets in the network causes energy waste and dying of whole network.Through ZEEP provide better packet overhead and causes longer route maintenance due to dynamic forwarding ,it can affect badly due to black-hole attack. Harm the throughput of whole network and eventually result in delay in delivery or packet loss or dying of network.

5. EXPERIMENTAL DATA ANALYSIS AND RESULTS

A. Implementing AODV and ZEEP Protocol in NS2.35 To

Simulate Black Hole Behavior:

First, BZEEP was implemented using Network Simulator version 2.35 (NS2.35) and the results are compared with NZEEP, NAODV and BAODV[10].To test the implementation we used two simulation parameters namely throughput and packet delivery ratio. The evaluation parameters are common to all protocols under comparison.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation Time	100s
Field Size	500m x 500m
Zone Size	100m x 100m
MAC layer	IEEE 802.11
Data packet Length	40bytes
Data Interval	0.25 s
Radio Range	250m
Node Velocity	20 m/s
Initial node Energy	100J

1) Packet Delivery Ratio: Packet Delivery Ratio is the measured end-to-end successful transmission probability. This ratio is calculated by the number of data packets received by the sink divided by number of data packets produced by the source.

2) Throughput: It is defined as total number of packets received by the destination. It is a measure of effectiveness of a routing protocol.There are two representations of throughput one is the amount of data transferred over the period of time expressed in kilobits per second (Kbps).The other is the packet delivery percentage obtained from a ratio of the number of data packets sent and the number of data packets received.

3) Energy Consumption: Total energy consumption of the network is evaluated on the basis of total amount of control packets and data packets generated and successfully delivered. Energy consumed also depends on the amount of energy spent during zone creation, clustering, and leader selection in the algorithm. The CBR flow is not continuous and varies with

The graphs in Figure 9 and 10 shows that BZEEP also gives a high packet delivery ratio and throughput over BAODV and NZEEP. In every case the PDR and throughput value for BZEEP is always above than other protocols and the decrease in PDR value is due to the increase in network traffic with time.

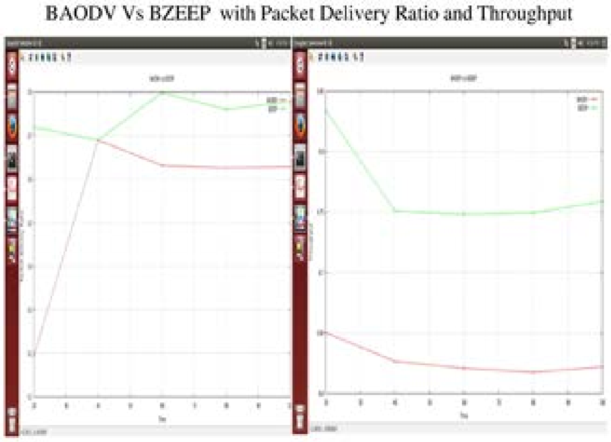


Figure 9: Performance comparison of BAODV and BZEEP

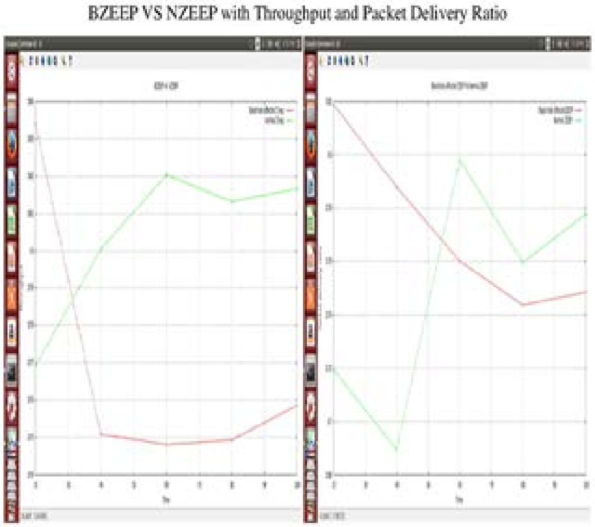


Figure 10: Comparison of performance between BZEEP and NZEEP

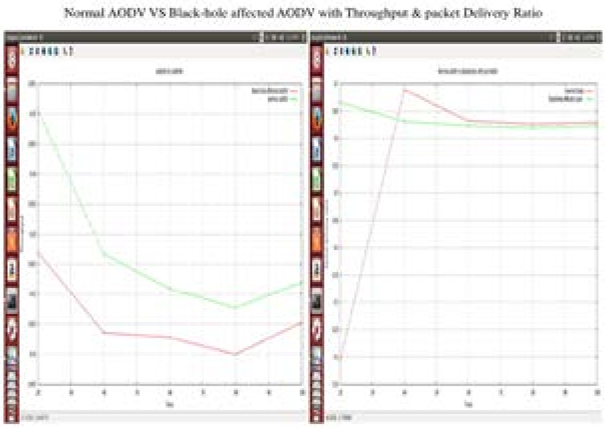


Figure 11: Analysis of performance between NAODV and BAODV

Figure 11 shows the performance of black-hole affected AODV. In every case PDR and throughput value is less than normal AODV protocol.

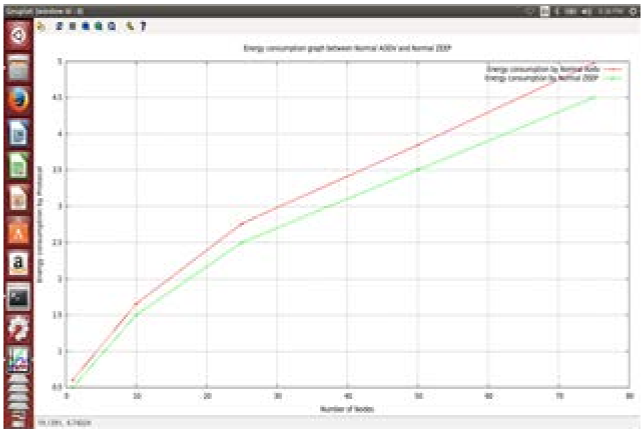


Figure 12: Performance analysis based on Energy for 80 nodes

NAODV and NZEEP, AODV took more energy even when number of nodes are increasing, these results are considered for both the protocols in the same scenario.

6. CONCLUSION AND FUTURE WORK

In this paper, extensive simulation results has shown that BZEEP provide better performance compared to BAODV in terms of packet delivery ratio and throughput. Graphs also shows NZEEP has a better performance compared to NAODV in terms of energy consumption of the network. That means the effect of black hole attack is more severe in case of AODV protocol than energy efficient routing protocols.

For future consideration the security of the MSN can be an important are of research. In this paper we have not consider solution to Black hole affected ZEEP protocol. In future we should come with some ideas about how to solve this kind of attacks in case of energy efficient routing protocols for mobile sensor networks.

References

[1] K Sohraby,D Minoli,T Znati, Wireless Sensor Networks , Technology, Protocols, and Applications.

[2] Wei Wang, Vikram Srinivasan, Kee-Chaing Chua, “Using Mobile Relays to Prolong the Lifetime of Wireless Sensor Networks”, MobiCom ’05.

[3] Liu, B., Brass, P., Dousse, O., Nain, P., Towsley, D. “Mobility Improve Coverage of Sensor Networks,” Proceedings of ACM MobiHoc 2005.

[4] A. K. Sadek, W. Su, and K. J. R. Liu, Multinode cooperative communications in wireless networks, IEEE Trans. Signal Processing, vol. 55, no. 1,pp. 341-355, 2007.

[5] Munir, S.A. and Biao Ren and Weiwei Jiao and Bin Wang and DongliangXie and Man Ma (2007),"Mobile Wireless Sensor Network: Architecture and Enabling Technologies for Ubiquitous Computing" Advanced Information Networking and Applications Workshops, AINAW '07. 21st Intl Conference on, pages 113-120.

[6] Mohammad Rahimi, Hardak Shah, Gaurav S. Sukhatme, John Heideman, Deborah Estrin “Studying the feasibility of Energy Harvesting in a Mobile Sensor Network”, In. Proc. of the 2003 IEEE International Conference on Robotics & Automotion, Taipei, Taiwan.

[7] J R Srivastava, TSB Sudarshan ,ZEEP: Zone based Energy Efficient Routing Protocol for Mobile Sensor Networks , IEEE International Informatics (ICACCl) ,2013.

[8] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75.

[9] Semih Dokurer , Y. M. Erten , Can Erkin Acar., Performance analysis of ad-hoc networks under black hole attacks IEEE Southeast conference, 2007.