ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks

Shailendra Pratap Nirala

Pursuing Master of Technology, Department of Computer Science and Engineering, GITM Lucknow, India

ABSTRACT A wireless Sensor Network (WSN) consists of a set of distributed sensors with sensing, computation, and wireless communication capabilities to monitor physical or environmental conditions. Wireless nodes have limited energy capabilities with limited computation and memory capacity on a dynamically changing environment. A Mobile Sensor Network (MSN) is a collection of mobilizer attached sensor nodes. These nodes can move randomly or task specifically. The relation between WSN and MSN is that when WSN nodes are moving they are known as MSN. 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 which change the topology frequently. But these protocols are not suitable due to resource constraint nature of MSN nodes.

Hence we need new ones. Zone based Energy Efficient Routing Protocol (ZEEP) is one of the new protocol in this direction which is the modified form of one of the most famous Ad-hoc routing protocol Ad Hoc On Demand Distance Vector Routing Protocol (AODV). One of these attacks is the Black Hole Attack, which grasps all data packets of the network.

In this thesis, I simulated this Black Hole Attack in AODV and ZEEP protocols using Network Simulator and have tried to find that the effect of Black Hole Attack is less affected in case of ZEEP protocol. To support my views I used two quality of service parameters like Packet Delivery Ratio and Through- put. And show that they have improved with Black Hole affected ZEEP (BZEEP) than Black hole affected AODV (BAODV).

KEYWORDS - Black Hole Attack , WSN , MSN, BAODV, BZEEP.

I. INTRODUCTION

In this new era of communication, the advent of mobile computing has revolutionized our information society. We are moving from the Personal Computer age to the Ubiquitous Computing age in which a user utilizes, at the same time, several electronic platforms through which he can access all the required information whenever and wherever needed. Among the numerous applications and services run by mobile devices, net- work connections and corresponding data services are the most demanding ones [1]. Currently, most of the connections among the wireless devices are achieved via fixed Infra-structure based service provider, or private networks. There are, many situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge [2].

II. WIRELESS SENSOR NETWORK (WSN)

A **Wireless Sensor Network (WSN)** is a collection of relatively inexpensive computational nodes that measure local environmental conditions like temperature, sound, pressure etc. and forward such information to a base station for appropriate processing [2]. WSN is somehow similar to ad hoc mobile network in the sense that both are resource constrained, like the battery power, computation capacity, communication range and memory. WSNs nodes (WNs) can

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

sense the environment, can communicate with neighboring nodes, and can, in many cases, perform basic computations on the data being collected.

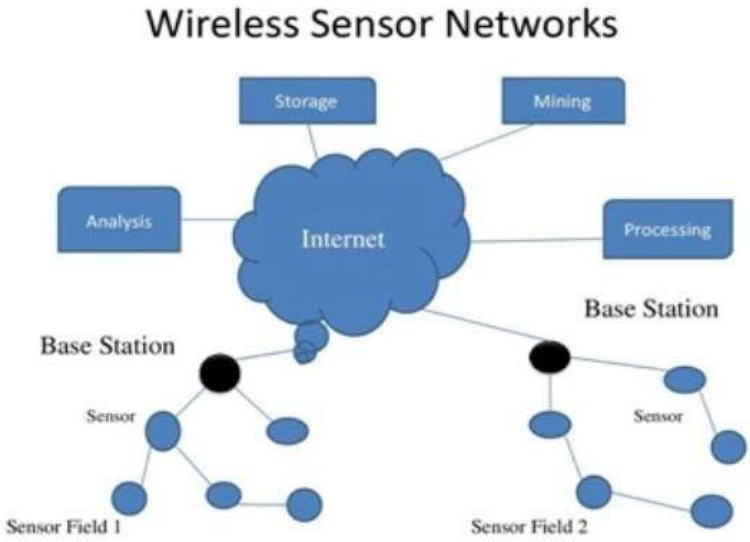


Figure 1.1: Wireless Sensor Networks: A Structure

III. DESIGN CONSTRAINTS

These challenges can be attributed to multiple factors, including severe energy constraints, limited computing and communication capabilities, the dynamically changing environment within which sensors are deployed, and unique data traffic models and application-level quality of service requirements.

1. **Network Scale and Time-Varying Characteristics:** There is a need for self-organize sensor nodes to adjust their behavior constantly in response to their current level of activity. Furthermore, sensor nodes may be required to adjust their behavior in response to the erratic and unpredictable behavior of wireless connections caused by high noise levels and radio-frequency interference, to prevent severe performance degradation of the application supported.
2. **Resource Constraints:** Sensor nodes are designed with minimal complexity for large-scale deployment at a reduced cost. Energy is a key concern in WSN, which must achieve a long lifetime while operating on limited battery reserves. Multi-hop packet transmission over wireless networks is a major source of power consumption. The requirements of these applications are such that a predetermined level of sensing and communication performance constraints must be maintained simultaneously. Therefore, a question arises as to how to design scalable routing algorithms that can operate efficiently for a wide range of performance constraints and design requirements. The development of these protocols is fundamental to the future of WSN [7].
3. **Sensor applications Data Models:** The data model describes the flow of information between the sensor nodes and the data sink. These models are highly dependent on the nature of the application in terms of how data are requested and used [4].

The need to support a variety of data models increases the complexity of the routing design problem. Optimizing the routing protocol for an applications specific data requirements while supporting a variety of data models and delivering

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

the highest performance in scalability, reliability, responsiveness, and power efficiency becomes a huge design and engineering problem.

IV. APPLICATIONS OF WSN

With WSNs one can monitor and control factories, offices, homes, vehicles, cities, the ambiance, and the environment etc. For example, one can detect structural faults (e.g., fatigue-induced cracks) in ships, aircraft, and buildings. Also applications like Volcanic eruption, earthquake detection, and tsunami alerting that generally require Wireless Nodes deployed in remote, even difficult-to-reach locations [2].

V. MOBILE WIRELESS SENSOR NETWORK (MSN)

A wireless sensor network (WSN) in which the sensor nodes are mobile. MSN is a smaller, emerging field of research in contrast to their well-established predecessor. MSN is much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. However, many of their applications are similar, such as environment monitoring or surveillance.

VI. APPLICATIONS OF MSN

The advantage of allowing the sensors to be mobile increases the number of applications beyond those for which static WSNs are used. Sensors can be attached to people for health monitoring, which may include heart rate, blood pressure etc. Animals can have sensors attached to them in order to track their movements for migration patterns, feeding habits or other research purposes. Sensors may also be attached to unmanned aerial vehicles (UAVs) for surveillance or environment mapping [4].

VII. OBJECTIVE

The goal of this thesis is two-fold.

i. It aims towards implementing and analyzing the effect of routing attack for energy efficient routing protocols.

(ii)The results of simulation has shown that Black hole affected Zone based energy efficient routing protocol (BZEEP) has a better performance compared to the black hole affected famous on demand based routing protocol Ad hoc on demand distance vector routing protocol (BAODV) in terms of energy consumption and packet delivery ratio of the network.

VIII. ENERGY EFFICIENT ROUTING PROTOCOL

Energy efficient routing protocols are kind of routing techniques where 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.

IX. WHY ENERGY EFFICIENT ROUTING PROTOCOL IS REQUIRED ?

The distributed nature and dynamic topology of Mobile Sensor Networks (MSN) introduces very special requirements in routing protocols. The most important feature of a routing protocol, in order to be efficient for MSN, is the energy consumption and the extension of the networks life time[9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

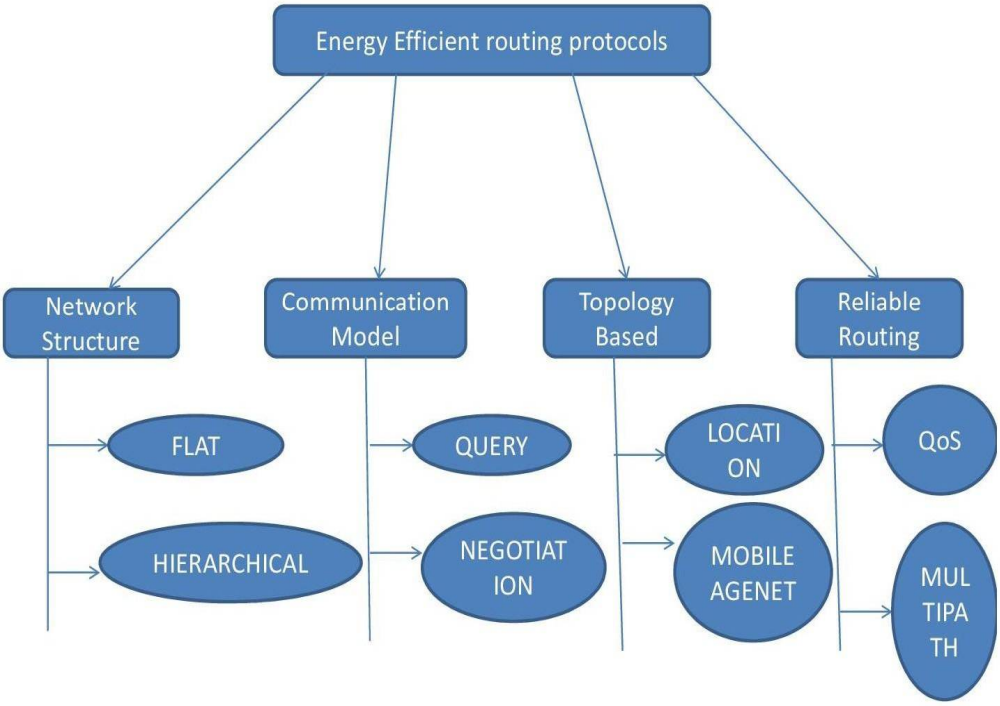
Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

- The devices used in MSN are resource constrained, they have a low processing speed, a low storage capacity and a limited communication bandwidth.
- Moreover, the network has to operate for long periods of time, but the nodes are battery powered, so the available energy resources limit their overall operation. To minimize energy consumption, most of the device components, including the radio, should be switched off most of the time.

The main design goal of MSN is not only to transmit data from a source to a destination, but also to increase the lifetime of the network [9]. This can be achieved by employing energy efficient routing protocols.

Classifications of Energy Efficient Routing Protocols



Depending on the applications used, different architectures and designs have been applied in MSN. The performance of a routing protocol depends on the architecture and design of the network, and this is a very important feature of MSN. However, the operation of the protocol can affect the energy spent for the transmission of the data. Most of the energy consumption, in MSN, is spent on three main activities:

sensing, data processing and communication.

All these factors are important and should be considered when developing protocols for MSN. The communication of the sensor nodes is the major component of the energy consumption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

X. CLASSIFICATIONS OF ENERGY EFFICIENT ROUTING PROTOCOLS

TYPES OF ZONE BASED ENERGY EFFICIENT ROUTING PROTOCOLS

Zone Routing Protocol (ZBR)

Zone Based Routing (ZBR) : The zone based routing scheme that is modified from Adhoc On demand Distance Vector Routing protocol [11].The goal of this protocol is to develop a routing protocol that offer reliability, improved error control mechanism, better link repair with low overhead in MSN [5].

PROTOCOL OPERATION:

In ZBR, after observing an event the member nodes transmit data to their respective zone head, which is always one hop neighbor of all member nodes. Zone head performs the aggregation depending on the type of application and transmit the aggregated or individual data to the base station. Route discovery, maintenance and consistent availability of route for reliable data delivery are the core responsibility of the zone head.

The protocol is divided into three phases which are individually addressed in the following sections.

Mobility Factor and Zone Head Selection: Depending on the remaining energy and the ratio of number of times a node change it's zone with respect to total number of moves it perform during t seconds is used to calculate the Mobility factor for ZBR protocol. Each node keeps track of its mobility and records the number of movements it has made and the energy spent in these movements.

Here, a move is considered as the change in location of node without a pause, irrespective of the distance, destination and direction. A node may change its zone as a result of a movement and joins a new zone as a member.

The zone head selection procedure starts with each node broadcasting its Mobility factor(M.F). This broadcast is intended for the members of the same zone and is discarded by others. Initially each node keeps its own M.F as the zone head M.F. Once a broadcast is received, the node compares the zone head M.F with the one received. If the received value is lower than the value already kept, the zone head M.F. and zone head identifier are appropriately updated.

At the end of the broadcast phase, each node has the knowledge of the node with least mobility factor and hence the node is considered as a zone head.

The lowest values of M.F ensures that the node will serve as zone head for longer duration and if participating in the route towards the base station the route will be stable for maximum period of time[5].

Route Maintenance: This section describes the format of enhanced route re- quest, route reply and the process of route creation and preservation for ZBR protocol.

XI. ZONE BASED ENERGY EFFICIENT ROUTING PROTOCOL (ZEEP)

In case of ZEEP also Mobility Factor is calculated to select the zone head. The goal of this protocol is to reduce the number of control packets than ZBR. It has two phases.

Phase1. Zone Head Selection based on Mobility Factor– As introduced in ZBR, ZEEP also, as it is based on, accounts for keeping track of a node's mobility factor. The mobility factor is the node's remaining energy and the number of zone changes it makes at a particular instant. A smaller value indicates less mobility and therefore a good contestant for the zone head selection.

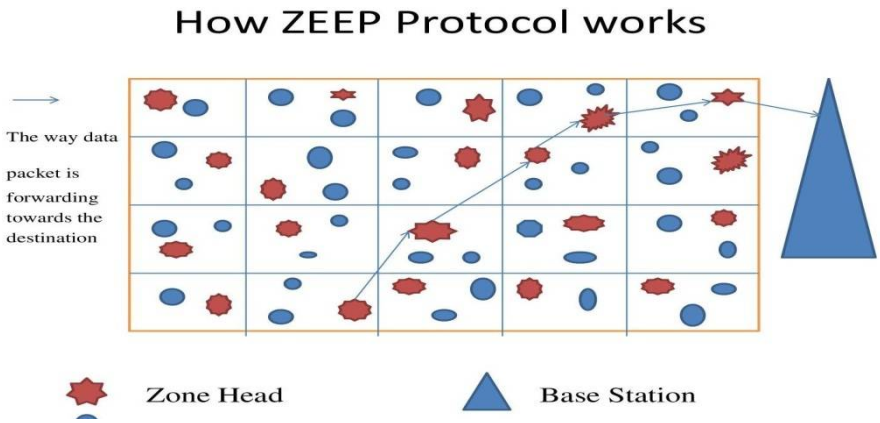
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

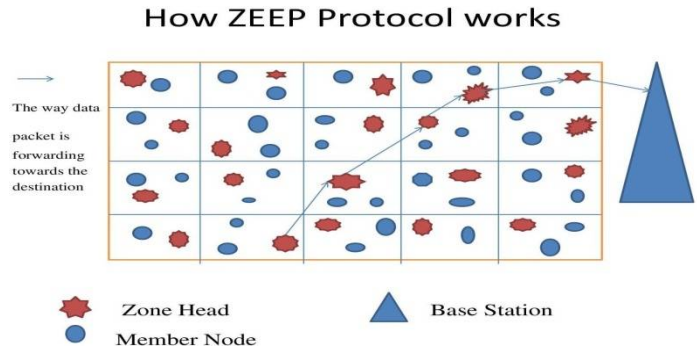
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019



Phase 2. 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[10]. This table maps the zone ids and the corresponding locations to which they are attached and a zone head.



XII. SECURITY ISSUES IN WIRELESS NETWORK

These security attacks can be roughly classified by the following criteria:

- passive or active
- internal or external
- different protocol layer
- stealthy or non-stealthy
- cryptography or non cryptography related

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

XIII. BLACK HOLE ATTACK

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.

XIV. HOW IT WORKS FOR AD HOC NETWORK ?

In this attack a malicious node uses the ad-hoc routing protocol (here we use AODV) to advertise itself as having the shortest path to the node whose packets it wants to intercept. As AODV is a broadcast based protocol, here if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack[21].

XV. HOW BLACK HOLE ATTACK EFFECT ON ZONE BASED ENERGY EFFICIENT ROUTING PROTOCOL OR ZEEP ?

We first calculate the mobility factor from remaining energy and observing the total number of moves and from those moves number of move causes zone changes.

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' second

E = the remaining energy

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 protocol** 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.

Due to this attack the data packets cannot reach the destination and packet de- livery ratio along with throughput affected very much. Mobility cause path breaks but black hole attack grasp all packets in the network causes energy waste and dying of whole network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Though 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.

XVI. SIMULATION OF BLACK HOLE ATTACK AND EFFECTS

To test the implementation we used two simulations. In the first scenario we did not use any Black Hole AODV Node 5 (the malicious node that exhibits the Black Hole Attack will be called Black Hole Node). This AODV is named as NAODV or Normal AODV.

In the second scenario we added a Black Hole AODV Node to the simulation. This AODV is known as BAODV as Black hole affected AODV. Then we compared the results of the simulations using NAM. After that we do the same with ZEEP protocol like BZEEP and NZEEP.

XVII. EVALUATION OF RESULTS

The traffic sources are CBR (continuous bit rate). The source-destination pairs are spread randomly over the network. The mobility model uses random waypoint model in a rectangular filed of 900m x 900m with 50 nodes. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for different number of nodes and pause times are generated.

Energy Conversation: 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 Constant Bit Rate or CBR flow is not continuous and varies with respect to time. The results are considered for both the protocols in the same scenario. As observed from the seventh graphs, it is clearly seen that the total energy consumption of the network, whether the nodes are stationary or mobile in ZEEP, is considerably less when compared to AODV.

XIX. CONCLUSION AND FUTURE WORK

From the above graphs for simulation results has shown that ZEEP has a better performance compared to AODV protocol in terms of energy consumption of the network. Black hole affected ZEEP(BZEEP) provide better packet delivery ratio and throughput than black hole affected AODV(BAODV).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 system can be an important domain of research. In this thesis 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 attack in case of energy efficient routing protocols.

BIBLIOGRAPHY

1. C. S. Raghavendra, K. M. Sivalingam, T. Znati Eds., Wireless Sensor Net- works, Kluwer Academic, New York, 2004.
2. K Sohraby, D Minoli, T Znati, Wireless Sensor Networks , Technology, Protocols, and Applications.
3. B. Krishnamachari, ”A Wireless Sensor Networks Bibliography,” Autonomous Networks Research Group, University of Southern CaliforniaLos Angeles, http://ceng.usc.edu/ anrg/SensorNetBib.html 0103.
4. Getsy S Sara and D. Sridharan, Routing in mobile wireless sensor network: a survey, Springer, Aug. 2013.
5. Faisal Bashir Hussain, Usama Ahmed, ”Energy Efficient Routing Protocol for Zone Based Mobile Sensor Networks ”, IEEE 2011, pp.1081-1086.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

6. Q. Cao, T. Abdelzaher, T. He, and R. Kravets, "Cluster-Based Forwarding for Reliable End-to-End Delivery in Wireless Sensor Networks", IEEE Infocom07, May 2007.
7. Younis, O , Fahmy, S, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks". IEEE Trans. Mob. Comput. 2004, 3, 366379.
8. C. Perkins, E. Belding-Royer, S. R. Das,: "Ad hoc On-Demand Distance Vector (AODV) routing ". rfc356J.txt (2003).
9. Ray Hunt, Network Security: The Principles of Threats, Attacks and In- trusions, part1 and part 2 ," APRICOT, 2004.
10. P. Yau and C. J. Mitchell, Security Vulnerabilities in Adhoc Network.
11. S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating Routing Misbehavior in Ad Hoc Networks, Proc. 6th Annual Intl. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.
12.