Volume 2, Issue 2, February 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Routing by Elimination of Black Holes in Ad Hoc Networks

Vishal Sharma,Takshi Gupta
Student,B.Tech.
Department of Computer Science & Engineering,
Amritsar College of Engineering & Technology,
Punjab Technical University, Jalandhar, India

Abstract-- **Mobile Ad Hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Ad Hoc Networks have the attributes such as wireless connection, continuously changing topology, distributed operation and easy of deployment. Each node operates not only as an end system, but also as a router to forward packets. Routing in Ad Hoc Networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is continue changes in network topology because of high degree of node mobility. A number of protocols have been developed to accomplish this task. Ad hoc networks are extensively used in military and civilian applications. In the paper, we address the problem of multiple black holes that may arise in the network structure, and further we propose the technique to remove the problem of multiple black holes with efficient routing for Ad Hoc Networks.**

Keywords-- **Ad hoc networks, AODV, black hole, SBHERP, packet loss, and packet received.**

I. INTRODUCTION

A wireless ad hoc network is based on the nodes that are mobile and have capabilities of communicating each other with packet radios over a shared wireless medium. The limited radio propagation causes the route to be multi hop [1] [2] [7] [8]. The applications of such networks can be search and rescue, automated battlefields, disaster recovery, crowd control and sensor networks. The routing protocol must have the ability to manage the frequent topology changes caused by the mobility of nodes and these need to be efficient as compared on basis of efficiency in terms of bandwidth and power as well as on basis of load transmission [11]. With the advent of On-demand routing, the tables are not maintained and the topological views are also rescued and the routing totally becomes dynamic [11]. Existing on demand routing protocols such as DSR (Dynamic Source Routing), AODV (Ad-hoc on demand distance vector routing) are the shortest path based routing protocols, also these don't consider the packet size and the antenna range of the nodes as a performance metric due to which there is a problem of long delays and congestions in the routing path and the whole set up of the nodal structure enters in to the dead state [10]. Also, on demand protocols that use the shortest paths as performance metric suffer from performance degradation as the network traffic increases [10]. In the paper [6], the energy of the nodes is the major area of concerned for the research to be carried on in this field. The one of the method suggested was CPACL protocol. It stands for cost based power aware routing protocol. In this paper the energy factor of the nodes is taken to be major concern. In this paper, a routing algorithm has been suggested that selects the path form the source to the destination on basis of the path that consumes the least energy [10]. The path selected for this transmission is the best selected path for the particular types of nodes. This means that if a path is defined from node 1 to node 2 by CPACL algorithm, it is the best suited path in all conditions [7] [10]. This protocol is the reactive routing protocol. It maintains the established routes as long as they are needed by the sources. AODV- CPACL uses sequence numbers to ensure the freshness of routes. The route discovery process is initiated whenever; a traffic source needs a route to a destination. Route discovery typically involves a network wide flood of route request packets targeting the destination and waiting for a route reply. It has also been shown that the per node throughput capacity of ad hoc networks with nodes n decreases with n as Θ (1/n log n) $^{1/2}$ [3]. The issue regarding this has been shown as the general capacity cost function of channel capacity for arbitrary input alphabets was studied on single link [4]. In the related work the bits per joule capacity of the network is assumed [3]. The tradeoff between energy and the bandwidth has been analyzed under various assumptions on the channel condition and the interference under a linear equidistant relaying network model without considering the energy consumption at the receiver end [5][6][7]. Also the receiver consumption can be improved by using the cross layer design including the effects of the power amplifier used at the transmitter end [8]. The transport efficiency of an ad hoc network was defined considering the transmitter energy and the receiver's processing energy [9] [10]. Thus the energy consumption for the packet transmission and the large number of hops is considered [6]. For the networks that have energy as their limiting resource, the network lifetime related to the energy is one of the significant performance metrics [6]. To solve the dead state problem, we have earlier got our paper published that resolved this issue of nodes getting into the dead state. This protocol was termed as DSPO.

Further, the problem regarding security issues that may arise in the process of routing is that of black hole. This problem has been discussed and the solution to optimize the problem has been proposed in the paper. Also, the technique is applicable to multiple black hole containing network structure.

II. SYSTEM MODEL

The network model we considered comprises of k number of hops, hops here are the nodes, and the nodes here considered are to be single channel node. This means for k number of nodes there is k number of channels. Thus, if two nodes are communicating at a time, then we have k-1 number of relaying nodes in the network model. The distance between the source and the destination is denoted by d. the distance between the relaying nodes can be decided on basis of the dynamic routing considered or it can be given on mathematical computations, this means that the distance between the relaying nodes will be less than the actual distance between the source and destination. Thus, if we consider a constant, let this constant be α then, from the theoretical analysis [6], we obtain that this value is multiplied with the total distance to obtain the actual distance between the relaying nodes then this value should be positive and less than one. Thus, the distance between the relaying nodes will be:

$$\mathrm{de} = \sum_{n=0}^{k} \alpha \mathrm{d}$$

The mobility introduces another simple concept. If the mobility of the structure nodes is more, the attenuation has greater effect but if the nodes are considered to be at rest then, the attenuation comes out to be so small that it can be neglected. Also the simplifier power amplifier is considered with the following expressions:

$$f_o(P_{in}) = \rho P_{in},\ 0 < P_{in} < P_1$$

$$P_{SAT},\ P_1 < P_{in} \leq P_{max}$$

$$f_c(P_{in}) = f_o(P_{in}) + P_h \text{ ....[6]}$$

Where ρ and P_h are constants. Also it is considered that $P_{max} = P_1$. The values for the constant are ρ=50(17) dB, P_1=1.5 mW, P_{SAT}=75 mW, and P_h=35 mW. Thus, the modified formula for the attenuation loss in a network model will be:

$$\mathbf{P_r = \beta\, P_{out} / d^{\eta},\quad where\ d > 0.}$$

Here, is the attenuation loss in the AD HOC NETWORKSs, β is the antenna constant, d is the end to end distance between source and destination, ε is the path loss constant such that 2 < ε < 4 and δ is the mobility factor. The mobility can be computed by analyzing the movement in terms of number of bits transferred per second per meter of the network model. Here, *Pout* = *fo* (*Pin*), which is based on the working power amplifier present in each of the node.

III. SECURE BLACK HOLE ELIMINATION ROUTING PROTOCOL (SBHERP)

A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets [10]. Second, the node consumes the intercepted packets. The black hole in general is the node that causes security problems by accepting the data which is not actually meant for it. This problem can be shown from the following snap shots of the simulator.

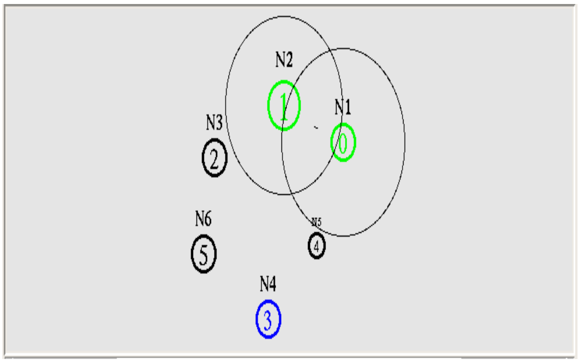


Fig. 1 Normal Transmission

The above figure shows the normal state transmission in Ad Hoc Networks. The figure shows the correct transmission between the Node 1 and Node 0. The black hole is that if any of the other nodes procures for data without any confirmation of without actual selection between path of transmission between source and destination. The detection of the black hole is detected from the table maintained after the start of transmission that contains the metric number and sequence number for the node. Thus, the detection can be easily carried out by matching the sequence number obtained from acknowledgement from the node receiving the data with the sequence numbers contained in the routing table. If the sequenced number is not matched with any of the data, then the node is not authenticated. The black hole can be shown as follows:

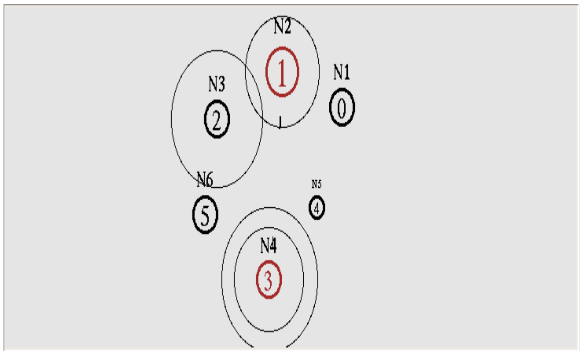


Fig.2 Black Hole

The figure shows that node 3 is receiving data but its information is not included in the table maintained for routing, so it is confirmed to be the black node that is accepting the data without any confirmation. Thus, in general the algorithm (SBHERP) for finding the black hole can be defined as follows:

```
 Set centralized_node== node (0)
While ( Search_routing_table(n) ==True)
{
Set node_location=table_reading
Generate Postion_Signal
If (Node_location==unauthorized)
{
Black_hole Detected
Change Transmission Mode
}
Else
{
Continue_transmission
}
```

IV. BLACK HOLE CORRECTION

The detection of the black hole is followed by the correction of this defect. The correction includes prevention of the data which is being transmitted on the path between the black hole node and the source of transmission. The packets transmitted this way are made to drop so as no unauthorized access is available to transmitted data. The dropping of the packets can be seen from following packets:

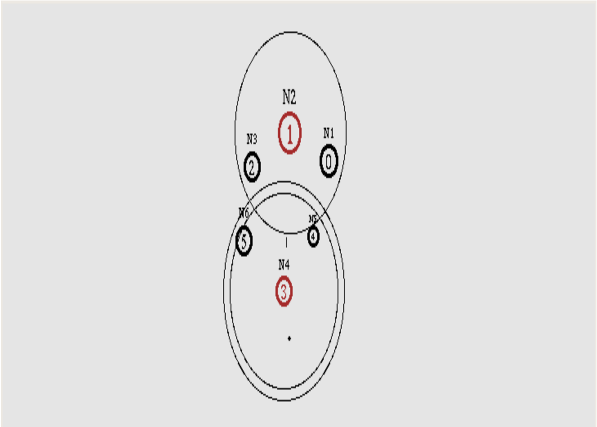


Fig. 3 packet drops from wrong path

The figure 3 shows the dropping of the packet when transmitted along the wrong path. Thus in the way, it is easy to correct the black hole by actual dropping of packets.

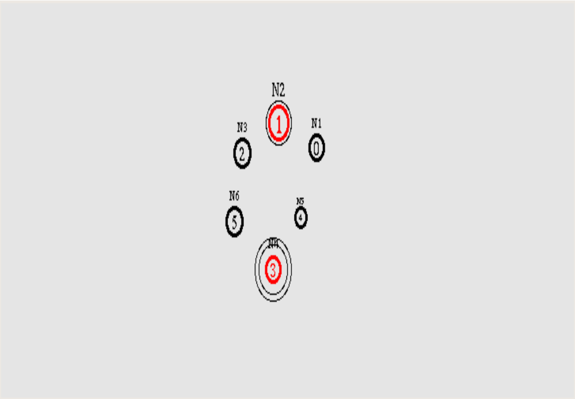


Fig. 4 node penalized

The figure 4 shows that node causing threat is been eliminated form path of transmission. Thus the black hole can be corrected and the correct transmission can be further carried on as shown below in the figure 5.

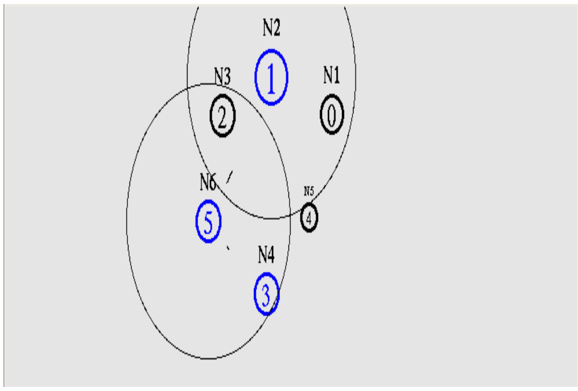


Fig. 5 Correct Transmission after Black hole solution

A. *Performance Metrics*

We simulated the typical Ad Hoc Networks for hop and calculated the results for bandwidth, energy, throughput of the network structure taking mobility and the antenna range as the basis of the technique. We have taken values as constant to compute our results. The simulation has been performed for the area ranging over 1000x1000. Also, the values for the noise power spectral density are 0.00384, heat loss from power amplifier to be 35 mW, packet size to be 512 bytes, transmitter energy is taken to be 0.38 µJ and that of receiver processing energy is 0.25 µJ. We concentrated on the following performance metrics:

- **Black Hole:** Any unwanted transmission in the network structure that lead to eroded transmission from source to destination by handling of bytes by unauthorized node.
- **Packet Lost:** The packet lost and received ratio is checked in the process of black hole detection and correction. This includes actual number of packet reaching the destination node.
- **Energy Efficiency:** Energy efficiency is the efficiency computed over the total energy consumption of the network including the useful energy and the wasted in form of losses during the transmission process. This is calculated as the modified energy for the network structure.
- **Bandwidth efficiency:** Bandwidth efficiency is the effective rate of transmission that can be considered at the common rate as well as at the common power. The effective rate i.e. the bandwidth is computed over the minimum achievable rate and the number of channel used for the purpose of transmission between the source and the destination. The value considered for minimum achievable rate over which bandwidth efficiency is calculated is 0.25.
- **Throughput:** throughput is the number of bits transferred during the transmission process. It is calculated I bits transferred per unit time. For our analysis the time considered is the simulation time.
- **Mobility:** Mobility is the new parameter that is highlighted in this paper. The readings have been taken by considering the scenario to be mobile and animations has also been recorded for the mobile nodes.

B. *Equation for performance calculation during Black Hole Eradication*

$(E_{tot,\ bit})_{CR}$= Efficiency at transmitter + Efficiency at the receiver

$$= \text{ʍ}R^{-1}_{min}\ [E_{tx}\ {}_{i=1}\Sigma^{k}\,(d_i/\ d_{max})^{\eta} + k\ (E_p + P_h\,Ts_{)}]$$

$$= R^{-1}_{eff}\ [B_{k,\ CR}.\ \ E_{tx}\ /\ k + E_p + P_h\,Ts]$$

$$B_{k,\ CR} =\ \ {}_{i=1}\Sigma^{k}\,(d_i/\ d_{max})^{\eta \leq}\ \ k$$

$$(E_{tot,\ bit})_{CR}\ d_e^{-\eta}/\ N_o = \text{ʍ}\ R^{-1}_{eff}\ [B_{k,\ CR}.\ \gamma/\ k + \gamma_c]$$

$$\gamma = E_{tx}\ d_e^{-\eta}/\ N_o$$

$$\gamma_c = (E_p + P_h\,Ts)\ d_e^{-\eta}/\ N_o$$

$$\mathbf{E_{eff} = R_{eff}\ /\ b\_fac\ (B_{k,\ CR}.\ \gamma/\ k + \gamma_c)}$$

Where Eeff is the modified energy efficiency defined in terms of bits transferred per joule, γ is the signal to noise ratio, N_o is the noise power spectral density, γ_c is the energy constant, Ph is the heat loss from power amplifier, d is the end to end distance, ʍ is the mobility, b_fac is the black hole factor that depends upon the probability of occurrence of black hole and the ʍ (mobility) during transmission.

V. SIMULATION RESULTS AND ANALYSIS

The simulations of the above technique are carried out using NS-2 simulation and the graphical result of the analysis is shown below:

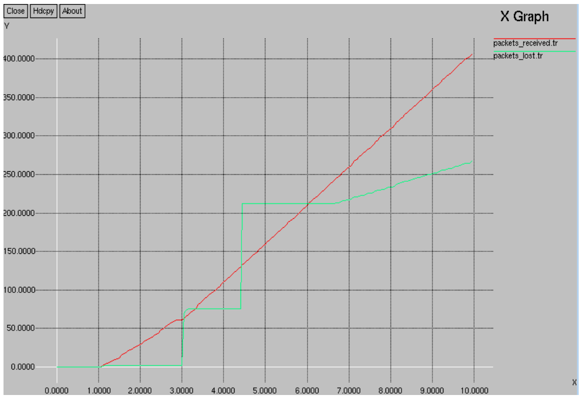
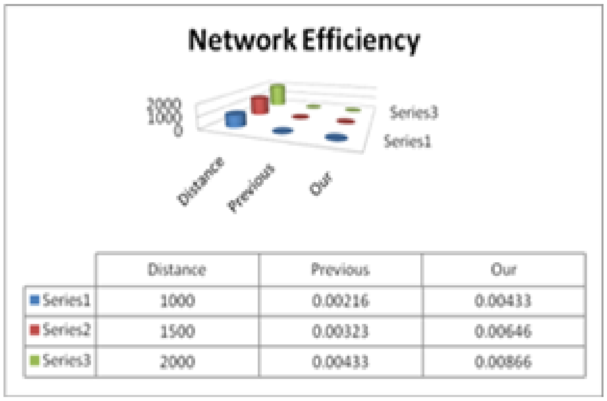


Fig. 6 Packet Received Vs Packet Lost

The above graph shows the relation between the numbers of packet lost and received along with the number of nodes taken for different scenario of transmission.



	Distance	Previous	Our
🟦 Series1	1000	0.00216	0.00433
🟥 Series2	1500	0.00323	0.00646
🟩 Series3	2000	0.00433	0.00866

Fig. 7 Network Efficiency

The above graph shows the comparison of network efficiency of AODV before black hole determination and the AODV with black hole determination technique.

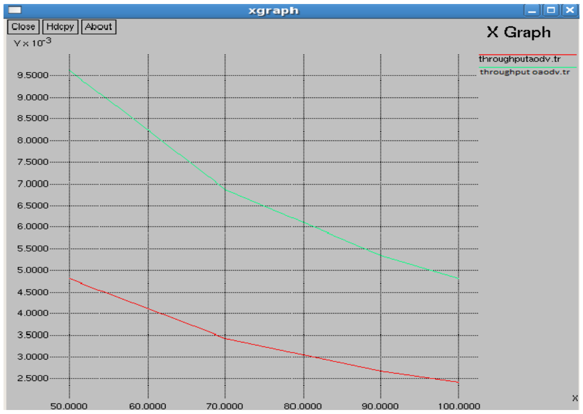


Fig. 8 Throughput

The above graph shows the comparison of throughput of AODV before black hole determination and the AODV with black hole determination technique.

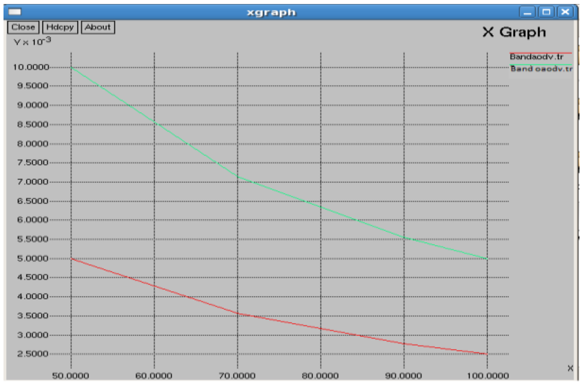


Fig. 9 Bandwidth Comparison

The above graph shows the comparison of bandwidth Efficiency of AODV before black hole determination and the AODV with black hole determination technique.

VI. CONCLUSION

In the paper, we proposed the secure black hole elimination routing protocol (SBHERP) for Ad Hoc Networks. The system developed by us is able to detect multiple black holes at the single instance of time and also has the capacity to correct the network structure by eradicating all the harmful and threat causing nodes. In future, work can be carried out to optimize the delays that may arise due to halt in transmission process on occurrence of black hole.

REFERNCES

[1]Dr. R.K. Singh, Tanu Preet Singh, Vishal Sharma:"Dead State Recovery Based Power Optimization Routing Protocol for Ad Hoc

Networks", HPAGC-2011, CCIS 169, pp.424-429,2011. © Springer-Verlag Berlin Heidelberg-2011.

[2]Sunil Taneja and Ashwani Kush:" A Survey of Routing Protocols in Mobile Ad Hoc abstract". International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[3]M.Saravana karthikeyan, M.Murali, Dr.S.Sujatha:"Identifying performance metrics to maximize Manet's throughput"; 2010 International Conference on Advances in Computer Engineering.

[4]Manika Vinay Rali, Min Song, Sachin Shetty:"Virtual wired transmission scheme using directional antennas to improve energy efficiency in Wireless Mobile Ad Hoc Network"; 978-1-4244-2677-5, IEEE 2008.

[5] http://www. csi.uoregon.edu.

[6]Sehoon Kim, Jinkyu Lee and Ikjun Yeom," Modeling and Performance Analysis of Address Allocation Schemes for Wireless sensor networks", IEEE transactions on vehicular technology, vol. 57, NO. 1, JANUARY 2008.

[7] Rekha Patil, Dr. A. Damodaram:"cost basedd power aware cross layer routing protocol for Manet"; 2008 IJCSNS.

[8]Changchun Bae and Wayne E. Stark:"A Tradeoff between Energy and Bandwidth Efficiency in Wireless Networks"; 2007 IEEE.

[9]V. Rodoplu and T. H. Meng: "Bits-per-Joule capacity of energy-limited wireless networks," IEEE Transaction Wireless Communications, vol.6(3), pp.857-865, March 2007.

[10]B. Rankov and A. Wittneben: "Spectral efficient protocols for half-duplex fading relay channels," IEEE Journal on Selected Areas in Communications, vol. 25, pp.379-389: Feb. 2007.

[11] Network simulator-2 www.isi.edu/nanam/ns/.