Indian Journal of Science and Technology, *Vol 9 (S1), DOI: 10.17485/ijst/2016/v9iS1/108432, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection and Prevention of Collaborative Attack and Energy Efficient Routing in Wireless and Ad hoc Network

S. Nithya[1] and C. Gomathy[2]

[1]Department of Electronics and Communication Engineering, SRM University, Ramapuram Campus, Bharathi Salai, Ramapuram, Chennai - 600 089, Tamil Nadu, India; nithisavidhina@gmail.com
[2]Department of Electronics and Communication Engineering, SRM University, Vadapalani Campus, No.1, Jawaharlal Nehru Road, (100 feet Road, Near Vadapalani Signal), Vadapalani, Chennai - 600 026, Tamil Nadu, India; hod.ece@vdp.srmuniv.ac.in

Abstract

Objectives: To implement Improved Cooperative Bait Detection Scheme which uses reverse tracing technique and to propose genetic algorithm to maximize the network lifetime. **Method**: The improved CBDS (Collaborative Bait Detection Scheme) and genetic algorithm are simulated in a randomly generated 16-node and 50-node topology using ns-2 network simulator and the performance is monitored. **Findings**: A comparison was made between existing CBDS, Improved CBDS and genetic algorithm. The overhead was high for genetic algorithm but the overall delay is found to be less and throughput was found to be high when compared to other techniques. The genetic algorithm provides efficient routing in spite of high overhead. **Conclusion:** The simulation result was compared with the existing technique and the efficiency was recorded in the chart.

Keywords: Collaborative Black Hole Attack, Data Packet, Genetic Algorithm, Gray Hole Attack, Improved Cooperative Bait Detection Scheme, Reverse Tracing Technique

1. Introduction

Wireless Networks are group of specialized transducers for monitoring and recording conditions at diverse locations. These systems are prone to security risks such as eaves dropping and require different technique compared to traditional security mechanism.

There are different routing attacks in network layer during wireless transmission of messages, in which black hole and gray hole are the predominant attacks in wireless and ad hoc network. In black hole attacks a node will falsely advertise that it has shortest path to destination from the source[1]. The black hole attacks[2] can also occur in groups known as cooperative black hole attack. In this (see Figure 1). The wicked node brings the entire packet by using false reply and discards the packet without forwarding them to destination.

In gray hole attack the node turn malicious only at a later time and then selectively discards or forward the data packets[3]. In this paper we implement improved cooperative bait detection method that uses reverse tracing technique for every hop to hop transmission. We also propose genetic algorithm to select energy efficient path in routing to save energy leading to increased operational life time of network.

The rest of the paper is organized as follows. In section 2, detection and prevention of cooperative black hole and gray hole attack using improved cooperative bait detection scheme is explained and in section 3, genetic algorithm was proposed to provide routing with maximum energy

*Author for correspondence

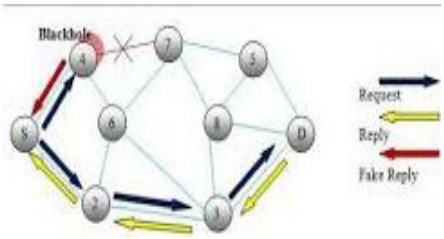

Figure 1. Cooperative Black Hole Attack.

and to improve the network performance. The performance analysis of simulation results were discussed in section 4. Finally conclusions was made in section 5.

A variety of secure routing protocol was proposed by the researcher to defend against malicious node. Most of these solutions were focused in finding the single wicked node, which are time consuming and not energy efficient. In[4] a scheme based on backbone network to detect and remove black hole nodes from the network was discussed. In[5-7] proactive detection scheme is used to constantly monitor nearby node, which may increase the overhead of detection and wastage of resource. In[8] the mechanism which modifies AODV protocol by data routing information table and cross checking to find whether next hope node is reliable or not. In[9] the author proposed BDSR scheme to select virtual destination address for bait RREQ as one hop neighbor from source. CBDS[10] (cooperative bait Detection Scheme) is an extension of BDSR scheme to identify black hole nodes by sending bait RREQ and DSR route discovery was proposed. But the selection of virtual destination address to bait malicious node is not specified. In DBA-DSR scheme[11], the author use fake RREQ packets to identify malicious node in the network before actual routing takes place. It also uses acknowledgement mechanism by the source and intermediate node, if fake RREQ-RREP fails to identify black hole nodes. The drawback is increase in routing overhead. In[12] disadvantage of DBA-DSR scheme is removed, which provides a improved way to find black hole node using acknowledgement packets sent by previous node. In[13] source routing and caching property of DSR to prevent black hole in network is processed, which reduces packet drop. In the integration of proactive and reactive detection scheme are used to detect malicious node that launch gray hole or collaborative black hole attacks. It uses DSR route discovery where the packet delivery ratio is compared with the threshold only at the destination to detect the packet drop. The disadvantage of this scheme is failure in detection of packet drop at the intermediate node.

An improved cooperative bait detection scheme was proposed, where the packet delivery ratio is compared with the threshold for every hop to hop transmission. Further, to increase the quality of service and to save energy genetic algorithm was proposed to select an energy efficient path in routing.

2. Improved Cooperative Bait Detection Scheme

This method utilizes Dynamic Source Routing Protocol (DSR), which mainly depends on source routing[14]. It consists of two major phases: route discovery and route maintenance. When a mobile node has to send a packet from the source to destination, it checks the route cache for the availability of route. If route is available, it will use the route to forward the data packet[15], else it initiates route discovery by sending RREQ (Route Request packet). To limit the number of RREQ, mobile forwards RREQ only if mobile address doesn't appear in the table. When the route request reaches the destination, RREP (Route Reply) is generated.

Algorithm 1: Improved CBDS Algorithm

1) Initialize the Hello timer
2) If Hello timer expires
    a. Send hello message
3) If node has data
    a. If coop checking not yet over
        i. Get the random neighbor from table
        ii. Send the req to the neighbor node
    b. Else
        i. Send the req to destination
4) If packet received
    a. If the packet is hello packet
        i. If sender is not malicious
1. If node is unknown node
    a. Add details in table
2. Else
    a. Update the expire time
        ii. Else
1. Ignore the packet
    b. If packet is Req packet
        i. Do basic packet filtering and updating operation
        ii. If current node is destination && sender is neighbor
1. Set packet as Freq

2. Ignore the packet
        iii. If current node is malicious node
1. Send reply
        iv. If node is destination
1. Send reply
        c. If packet is reply packet
        i. If current node is destination of reply packet && source is neighbor
1. Set packet final node is malicious
2. Ignore the packet
        ii. Else
1. Do normal filtering and updating operation

We present a improved cooperative bait detection algorithm based on Dynamic Source Routing, as shown in Algorithm 1. From the original algorithm[16] we modify it to detect the malicious node in every hop by hop transmission. In this the origin node selects the one hop neighbor node address as destination address of bait RREQ. If only the selected node replies then there is no malicious node in the route. If more than one node sends RREP, then the malicious node exists in the route, therefore reverse tracing technique should be initiated to find the malicious node. Suppose if the selected node doesn't give any reply RREP, then that node can be listed directly in the black hole list.

To detect the gray hole attack, the threshold value was set to detect whether the packet has reached the destination within the threshold and checked for every hop to hop transmission. If the ratio falls below the threshold, then the neighbor will be identified as malicious node.

3. Genetic Algorithm

The intermediate node plays a vital role in routing the packet from source to destination. So the battery power of the node has to be used efficiently to avoid drain out of energy of a node or network. We propose an energy efficient routing protocol which performs route discovery technique by considering the residual energy level of node and hop count as shown in Algorithm 2.

This algorithm collects the data about their neighbor nodes based on the residual energy and selects a reliable route. Initially when the source node sends route request, nodes will check the energy of one hop neighbor node with the database. If the old energy is less than current energy then the node is identified as fake node. If the old energy is equal to current energy, it will check the energy cost and selects the node with high energy cost. This goes on until the end node receives RREQ with the information of residual energy in both hop by hop and end-to-end communication. After validating these factors, destination will send RREP through high energy path.

Algorithm 2: Genetic Algorithm

1. Set initial energy level for each node
2. Initialize Hello timer
3. If Hello timer triggered
    a. Generate the hello message
        i. Attach current energy
    b. Broadcast the pkt
4. If node has data
    a. If route is found
        i. Send data to next node
    b. Else
        i. Generate the req
1. Attach energy level with pkt
        ii. Broadcast req
5. If node received packet
    a. If packet is hello packet
        i. Checks database
1. If old energy is less than current energy
    a. Set as misbehavior node
    b. If packet is Req
        i. If received node is destination
1. Check in routing table
    a. If old min energy is less than new
        i. Accept and send reply
    b. If old min energy is equal to new
        i. Checks the energy cost
1. If old cost is more than new
    a. Accept and send reply
2. ignore the packet
        ii. if node is intermediate node
1. if pkt is duplicate or prev node is malicious
    a. ignore pkt
2. Else
    a. Check in routing table
        i. Add the energy cost
        ii. If pkt min energy is more than own
1. Add own energy as min energy
        iii. Forward the pkt
    c. If pkt is Reply
        i. If prev node is malicious
1. Ignore the packet
        ii. Else

1. If node is not destination
    a. Forward the pkt

4. Performance Analysis

We evaluated the improved CBDS and genetic algorithm in a randomly generated 16-node and 50-node topology using ns-2 network simulator[17]. We compared the proposed scheme with CBDS[18].

- **Throughput:** It is defines as total size of data packets received by the destination node from the source every second
- **Average End-to-End-Delay:** It is defined as average time taken for the packet to be transmitted from the source to destination.
- **Message Overhead:** It is the size of Type Length Value (TLV) blocks in total messages, which are used to carry trust values.

The simulation parameters are listed in Table 1

The simulation is done with different number of nodes with Constant Bit Rate traffic (CBR). The maximum velocity of each node is set from 0 to 20 m/s. The pause time is 1s.

First, we study the performance of detecting black hole and gray hole with respect to throughput, end-to-end delay and message overhead. The throughput for CBDS and ICBDS are shown in Figure 2 with respect to packet size and time to deliver the packet in seconds. The simulation is done for 16 nodes with the maximum speed set to 20m/s.

Second, we observe the routing overhead using improved CBDS algorithm. The results are shown in Figure 3. In which the overhead is slightly higher for CBDS compared to ICBDS.

Table 1. Simulation Parameters

Parameter	Value
Application traffic	10CBR
Transmission rate	0.05MB
Radio Range	40m
Pause Time	1s
Maximum Speed	20 m /s
Simulation Time	250s
Number of Nodes	16,50
Area	480*480,600*600
Malicious Node	19%
Threshold	For every hop count

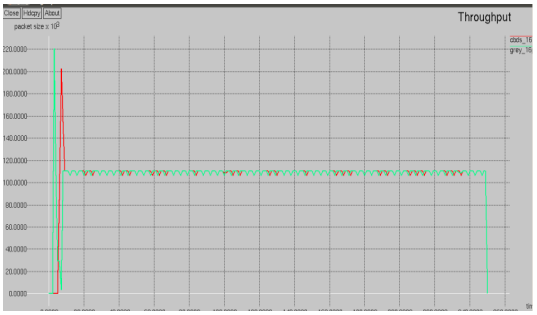

Figure 2. Throughput of CBDS and Improved CBDS.

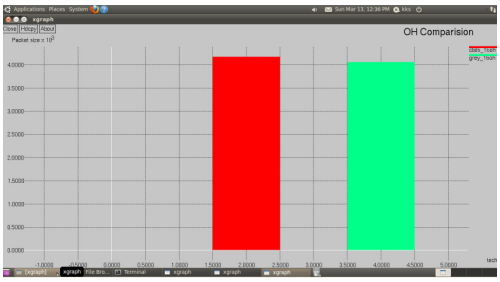

Figure 3. Overhead Comparison of CBDS and Improved CBDS.

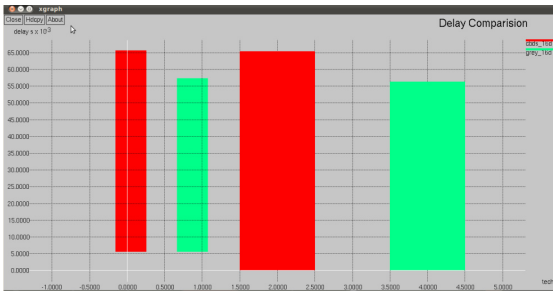

Figure 4. Delay Comparison of CBDS and Improved.

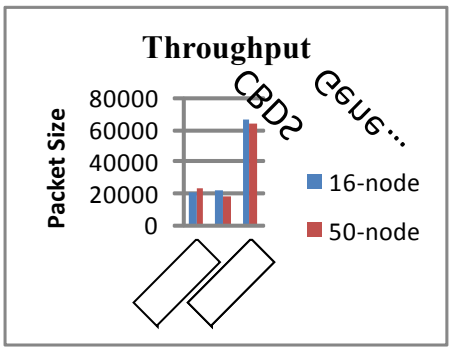

Figure 5. Throughput for different algorithm CBDS.

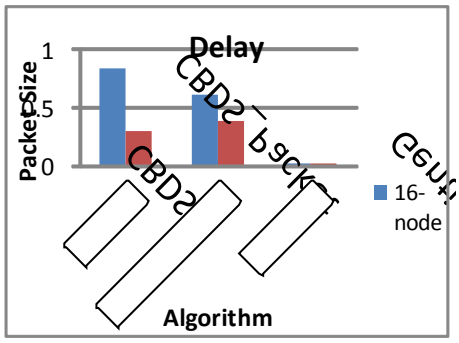

Figure 6. Delay comparison for different algorithm.

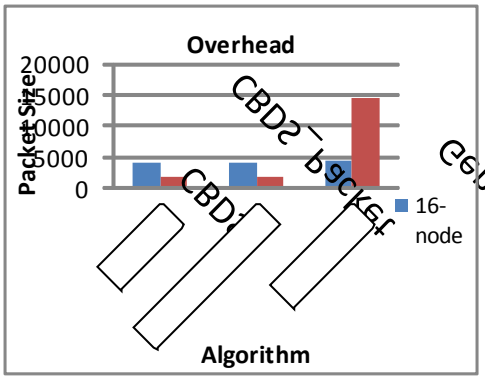

Figure 7. Overhead for different algorithm.

Third, the end-to-end delay comparison was made with respect to delay and time in seconds. The results were shown in Figure 4.

Fourth, we compare the throughput of CBDS, CBDS_ packet and genetic algorithm for 16 and 50 nodes with respect to packet size. The results are captured in Figure 5; which give higher throughput compared to other algorithm.

Fifth, we study the delay in transmitting the Packets with respect to packet size using CBDS, CBDS_ packet and genetic algorithm. From the Figure 6, we can observe that packet transmission is faster in genetic algorithm compared to CBDS.

Sixth, we discuss the routing overhead of the CBDS, CBDS_packet and genetic algorithm for different size of nodes. The results are shown in Figure 7; it can be viewed that genetic algorithm can still provide a efficient routing even when the overhead is greater than CBDS.

5. Conclusion

An improved CBDS algorithm to detect the cooperative black hole and gray hole attack in every hop to hop transmission was proposed. We also proposed genetic algorithm, which maximizes the network lifetime by minimizing the power consumption. Improved CBDS technique provides more latency and reduced packet delivery fraction compared to genetic algorithm. Genetic Algorithm provides better performance using Max-Min Route selection method. In future we extend our proposed scheme to overcome the attacks in other layer.

To refer a research article:

1. Kimio T, Natarajan G, Hideki A, Taichi K, Nanao K. **Higher involvement of subtelomere regions for chromosome rearrangements in leukemia and lymphoma and in irradiated leukemic cell line.** *Indian Journal of Science and Technology*. 2012 April, 5 (1), pp. 1801-1811.

To refer a Book/ Report:

2. Cunningham CH. A laboratory guide in virology. 6th edn. Burgess Publication Company: Minnesota, 1973.

To refer a Chapter in a Book:

3. Kumar E, Rajan M. Microbiology of Indian desert. In: Ecology and vegetation of Indian desert. D.N.Sen (ed.), Agro Botanical Publ.: India. 1990, pp. 83-105.

To refer a publication of proceedings:

4. Rajan M, Rao BS, Anjaria KB, Unny VKP, Thyagarajan S. Radiotoxicity of sulfur-35. *Proceedings of 10th NSRP, India*, 1993, pp. 257-258.

Internet source

5. Article title. http://www.indjst.org/index.php/vision. Date accessed: 01/01/2015.

6. References

1. Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks. 2003 May; 1:293-315.
2. Sen J, Koilakonda S, Uki A. A Mechanism for Detection of Cooperative Black hole Attack in Mobile Ad Hoc Networks. Phnom Penh, Cambodia: Proceedings of the 2nd International Conference on Intelligent Systems, Modeling and Simulation (ISMS'11). 2011 Jan 25-27; p. 388-43.
3. Ullah I. Blekinge Institute of Technology: Analysis of Black Hole Attack on MANET using Different MANET Routing Protocols, Master Thesis. 2010 Jun; p.1-51, p. 1-49.
4. Paul AJ, Vishnu K. Detection and Removal of Cooperative Black/Gray hole Attack in Mobile Ad hoc Networks. International Journal of Computer Applications. 2010; 1(22):38-42.

5. Aadache AB, Belmehdi A. Avoiding Black Hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks. International Journal of Computer Science Information Security. 2010; 7(1):10-16.
6. Deng H, Li W, Agrawal D. Routing Security in Wireless Adhoc Network. IEEE Communication Magazine. 2002 Oct; 40(10):70-5.
7. Werrasinghe H, Fu H. Preventing Cooperative Black hole Attacks in Mobile and Adhoc Networks: Simulation Implementation and Evaluation. Proceedings of IEEEICC. 2007; p. 362-67.
8. Gayatri Wahane, Savita Lonare. Technique for Detection of Cooperative Black Hole Attack in MANET. Tiruchengode, India: 4th ICCCNT 2013 July 4-6. 2013.
9. Po-Chun Tsou, Jiann-Liang Chen. Developing a BDSR scheme to avoid Black hole attack based on Proactive and Reactive Architecture in MANET, ICACT 2011.
10. Jian-Ming Chang, Po-Chun Tsou, Hanchiech Chao, Jiann-Liang Chen. CBDS: A Cooperative bait Detection Scheme to prevent malicious node for MANET based Hybrid Defense Architecture, IEEE. 2011.
11. Isaac Woungang, Sanjay Kumar, Rajendu Dhuraj Peddi, Md. S. Obaidat. Detecting Black Hole Attacks on DSR based Mobile Adhoc Networks. IEEE 2012; 978-1-4673-1550-0/12.
12. Chandar Diwaker, Sunitha Choudhary. Detection of Black Hole Attack in DSR based MANET. International Journal of Software and Websciences. 2013.
13. Prache N Patil, Ashish T Bhole. Black Hole Attack Prevention in Mobile Adhoc Network using Route Caching. IEEE 2013; 978-1-4673-5999-3/13.
14. Jian-Ming Chang, Po-Chun Tsou, Hanchiech Chao, Ching-Feng Lai. Defending Against Collaborative Attacks by Malicious Nodes in MANET: A Cooperative Bait Detection Approach. IEEE Systems Journal. 2015.
15. Johnson D and Maltz D. Kluwer: Dynamic Source Routing in Adhoc Wireless Networks. Mobile Computing. T. Imielinski and H. Korthi. 1996; p. 153-81.
16. Christee Joseph, Kishoreraja PC, Radhika Baskar, Reji M. Performance Evaluation of MANETS under Black Hole Attack Under Different Network Scenarios. Indian Journal of Science & Technology. 2015 November.
17. Haripriya Y, Bhavani KVB, Lavanya S. A framework for detecting malicious nodes in mobile Adhoc Network. Indian Journal of Science & Technology. 2015 January.
18. The Network Simulator-ns-2. Available from: http://www.isi.Eduo/nsnam/ns/